NetScaler VPX 13.1

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

支持矩阵和使用指南 26

XenServer 上的 VPX 实例 26

VMware ESXi 虚拟机管理程序上的 VPX 实例 26

Microsoft Hyper-V 上的 VPX 实例 29

Azure Local 上的 VPX 实例 29

Nutanix AHV 上的 VPX 实例 29

通用 KVM 上的 VPX 实例 30

公共云上的 VPX 实例 30

虚拟机管理程序上支持的 VPX 功能 31

公共云上支持的 VPX 功能 32

支持的浏览器 33

NetScaler VPX™ 支持的处理器 34

NetScaler VPX 支持的 NIC 34

使用指南 35

控制数据包引擎 CPU 使用率的命令 36

其他参考 37

优化 NetScaler VPX 在 VMware ESX、Linux KVM 和 Citrix Hypervisors 上的性能 38

VMware ESX 管理程序上的 NetScaler VPX 实例 38

ESX 主机上的推荐配置 38

使用 E1000 网络接口的 NetScaler VPX 39

每个 pNIC 部署两个 vNIC 39

带有 VMXNET3 网络接口的 NetScaler VPX 41

为 VMXNET3 设备在 VMware ESX 上配置多队列和 RSS 支持 42

具有 SR-IOV 和 PCI 直通网络接口的 NetScaler VPX 43

Linux-KVM 平台上的 NetScaler VPX 实例 43

KVM 的性能设置 43

© 1997–2026 Citrix Systems, Inc. All rights reserved.

带有 PV 网络接口的 NetScaler VPX 49
具有 SR-IOV 和 Fortville PCIe 直通网络接口的 NetScaler VPX 51
Citrix Hypervisors 上的 NetScaler VPX 实例 52
适用于 Citrix Hypervisors 的性能设置 53
具有 SR-IOV 网络接口的 NetScaler VPX 53
具有半虚拟化接口的 NetScaler VPX 53
支持增加 NetScaler VPX 磁盘空间 55
在 NetScaler VPX 上动态增加主磁盘大小 55
添加辅助磁盘 55
手动增加 NetScaler VPX 上的主磁盘大小 56
在云中首次启动 NetScaler 设备时应用 NetScaler VPX 配置 58
什么是用户数据 58
如何在云实例中提供预启动用户数据 58
使用 AWS 控制台提供预启动用户数据 58
使用 AWS CLI 提供预启动用户数据 59
使用 Azure 控制台提供预启动用户数据 60
使用 Azure CLI 提供预启动用户数据 61
使用 GCP 控制台提供预启动用户数据 62
使用 gcloud CLI 提供预启动用户数据 63
预启动用户数据格式 64
NetScaler 配置 65
用户脚本 67
许可 72
引导 73
默认引导配置 73
自定义引导配置 74
方法 1：通过仅指定接口详细信息进行自定义启动 74
AWS 的自定义引导示例 74

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure 的自定义引导示例 76
GCP 的自定义引导示例 78
方法 2：通过指定接口、IP 地址和子网掩码进行自定义引导 79
适用于 AWS 的自定义引导示例 79
适用于 Azure 的自定义引导示例 80
GCP 的自定义引导示例 80
方法 3：通过在 `<NS-CONFIG>` 部分提供引导相关命令进行自定义引导 81
AWS 的自定义引导示例 81
Azure 的自定义引导示例 85
GCP 的自定义引导示例 88
在 AWS 和 Azure 中连接和分离 NIC 的影响 90
提高公有云平台上的 SSL-TPS 性能 92
使用 NetScaler CLI 配置 PE 模式 92
在云中首次启动 NetScaler 设备时应用 PE 模式配置 93
在公有云上为 NetScaler VPX 配置同步多线程 94
SMT 支持矩阵 95
限制 95
配置 SMT 95
故障排除 97
在裸机服务器上安装 NetScaler VPX 实例 99
在裸机服务器上安装 NetScaler VPX 实例的先决条件 99
在裸机服务器上安装 NetScaler VPX 实例 99
在 Citrix Hypervisor/XenServer 上安装 NetScaler VPX 实例 100
在 Hypervisor 上安装 NetScaler VPX 实例的先决条件 100
Hypervisor 硬件要求 100
XenCenter 系统要求 102
使用 XenCenter 在 Hypervisor 上安装 NetScaler VPX 实例 102
配置 VPX 实例以使用单根 I/O 虚拟化 (SR-IOV) 网络接口 103

© 1997–2026 Citrix Systems, Inc. All rights reserved.

限制 103
英特尔 82599 网卡的限制 103
Intel X710 10G 和 Intel XL710 40G 网卡的限制 104
Intel 82599 NIC 的先决条件 104
通过使用 Citrix Hypervisor 主机将 Intel 82599 SR-IOV VF 分配给 NetScaler VPX 实例 105
使用 Citrix Hypervisor 主机将 Intel 82599 SR-IOV VF 从 NetScaler VPX 实例中取消分配 105
使用 Citrix Hypervisor 主机将 Intel X710/XL710 SR-IOV VF 分配给 NetScaler VPX 实例 106
使用 Citrix Hypervisor 主机从 NetScaler 实例中移除 Intel X710/XL710 SR-IOV VF 108
在 SR-IOV 接口上配置链路聚合 108
在 SR-IOV 接口上配置 VLAN 109
其他参考 109
在 VMware ESX 上安装 NetScaler VPX 实例 110
先决条件 110
VMware ESX 硬件要求 110
VMware vSphere 客户端系统要求 112
OVF Tool 1.0 系统要求 112
下载 NetScaler VPX 安装文件 113
在 VMware ESX 上安装 NetScaler VPX 实例 113
使用 VMware vMotion 迁移 NetScaler VPX 实例 114
配置 NetScaler VPX 实例以使用 VMXNET3 网络接口 115
配置 NetScaler VPX 实例以使用 SR-IOV 网络接口 126
限制 126
先决条件 127
将 NetScaler VPX 从 E1000 迁移到 SR-IOV 或 VMXNET3 网络接口 145
配置 NetScaler VPX 实例以使用 PCI 直通网络接口 145
概述 145
先决条件 145
在主机上配置直通设备 146

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 NetScaler VPX 实例上配置直通设备 146
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 148
如何在 ESX 虚拟机管理程序上提供预启动用户数据 150
使用 CD/DVD ISO 提供用户数据 150
使用 ESX Web 客户端的 OVF 属性提供用户数据 153
使用 ESX vSphere 客户端的 OVF 属性提供用户数据 157
在 AWS 上的 VMware Cloud 上安装 NetScaler VPX 实例 162
先决条件 162
VMware Cloud 硬件要求 162
OVF Tool 1.0 系统要求 163
下载 NetScaler VPX 安装文件 163
在 VMware 云上安装 NetScaler VPX 实例 164
在 Microsoft Hyper-V 服务器上安装 NetScaler VPX 实例 165
在 Microsoft 服务器上安装 NetScaler VPX 实例的先决条件 165
Microsoft 服务器硬件要求 165
下载 NetScaler VPX 安装文件 166
在 Microsoft 服务器上安装 NetScaler VPX 实例 167
在 Hyper-V 上自动预配 NetScaler VPX 实例 168
在 Linux-KVM 平台上安装 NetScaler VPX 实例 172
限制和使用指南 172
一般建议 172
限制 172
在 Linux-KVM 平台上安装 NetScaler VPX 实例的先决条件 172
软件要求 173
客户机虚拟机硬件要求 173
网络要求 173
源接口和模式 173
源接口的属性 174

© 1997–2026 Citrix Systems, Inc. All rights reserved.

混杂模式 177

所需模块 178

使用 OpenStack 预置 NetScaler VPX 实例 178

用户数据文件 179

网络配置 182

客户脚本 183

SSH 密钥对身份验证 183

开始之前 183

预置 VPX 实例 184

使用 OpenStack 控制面板预置 VPX 实例 184

使用 OpenStack CLI 预置 VPX 实例 187

使用虚拟机管理器配置 NetScaler VPX 实例 189

检查自动置备 NetScaler VPX 实例的先决条件 190

使用 RAW 镜像配置 NetScaler VPX 实例 192

使用QCOW2镜像配置NetScaler VPX实例 197

通过连接 CDROM 驱动器启用自动预配 198

使用虚拟机管理器向 NetScaler VPX 实例添加更多接口 200

配置 NetScaler VPX 实例以使用 SR-IOV 网络接口 204

限制 205

先决条件 206

配置 NetScaler VPX 实例以使用 SR-IOV 网络接口 208

在 SR-IOV 接口上配置静态 LA/LACP 211

在 SR-IOV 接口上配置 VLAN 212

配置 NetScaler VPX 实例以使用 PCI 直通网络接口 212

先决条件 212

使用 `virsh` 程序预配 NetScaler VPX 实例 214

使用 `virsh` 程序向 NetScaler VPX 实例添加更多接口 217

© 1997–2026 Citrix Systems, Inc. All rights reserved.

管理 NetScaler VPX 访客虚拟机 219
使用虚拟机管理器管理 VPX 访客虚拟机 219
使用 `virsh` 程序管理 NetScaler VPX 访客虚拟机 220
在 OpenStack 上使用 SR-IOV 预置 NetScaler VPX 实例 222
先决条件 222
在主机上启用 SR-IOV VF 222
配置 VF 并使其可用于 OpenStack 223
在 OpenStack 上预配 NetScaler VPX 实例 223
通过 CLI 在 OpenStack 上预置 NetScaler VPX 实例 224
其他支持的配置：从主机创建和删除 SR-IOV VF 上的 VLAN 227
在 KVM 上配置 NetScaler VPX 实例以使用基于 OVS DPDK 的主机接口 228
先决条件 229
安装 DPDK 229
构建并安装 OVS 229
创建 OVS 网桥 229
将物理接口连接到 OVS 网桥 230
将 `vhost-user` 端口连接到 OVS 数据路径 230
预配具有基于 OVS-DPDK 的 `vhost-user` 端口的 KVM-VPX 231
注意事项 247
在 KVM 虚拟机管理程序上首次启动 NetScaler 设备时应用 NetScaler VPX 配置 248
如何在 KVM 虚拟机管理程序上提供预启动用户数据 250
使用 CDROM ISO 文件提供用户数据 250
AWS 上的 NetScaler VPX 252
入门 252
在 AWS 上部署 NetScaler VPX 实例 252
混合部署 253
许可 253

© 1997–2026 Citrix Systems, Inc. All rights reserved.

自动化 253
博客 253
视频 254
客户案例研究 254
解决方案 254
支持 254
其他参考资料 254
AWS 术语 255
AWS-VPX 支持矩阵 256
限制和使用指南 260
先决条件 262
在 NetScaler VPX 实例上配置 AWS IAM 角色 266
创建 IAM 角色 269
使用 IAM 策略模拟器测试 IAM 策略 276
其他参考 277
NetScaler VPX 实例在 AWS 上如何工作 278
在 AWS 上部署 NetScaler VPX 独立实例 279
使用 AWS Web 控制台在 AWS 上部署 NetScaler VPX 实例 280
使用 Citrix CloudFormation 模板配置 NetScaler VPX 实例 283
使用 AWS CLI 配置 NetScaler VPX 实例 284
场景：独立实例 284
下载 NetScaler VPX 许可证 292
如何将 AWS 订阅迁移到 BYOL 292
限制 297
在不同可用区中对服务器进行负载均衡 297
AWS 上高可用性如何工作 298
同一区域内的高可用性 298
跨不同区域的高可用性 300

© 1997–2026 Citrix Systems, Inc. All rights reserved.

开始部署之前 300
故障排除 300
在同一 AWS 可用区中部署 VPX HA 对 300
如何在同一区域中部署 VPX HA 对 301
步骤 1. 使用相同的 VPC 创建两个 VPX 实例（主节点和辅助节点），每个实例有三个 NIC（以太网 0、以太网 1、以太网 2） 302
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）分配私有 IP 地址 302
步骤 3. 在主节点上配置 VIP 和 SNIP，使用辅助私有 IP 地址 303
步骤 4：在两个实例上配置 HA 303
部署 VPX HA 对的旧方法 304
注意事项 305
使用 Citrix CloudFormation 模板部署高可用性对 306
使用 Amazon CloudWatch 监控您的实例 309
注意事项 309
如何查看 CloudWatch 指标 309
在高可用性设置中配置 SR-IOV 311
相关资源 311
跨不同 AWS 可用区的高可用性 311
注意事项 311
其他参考 312
在不同 AWS 区域部署具有弹性 IP 地址的 VPX 高可用性对 312
具有跨不同 AWS 区域的 EIP 地址的 HA 如何工作 312
如何在不同 AWS 区域部署具有弹性 IP 地址的 VPX 高可用性对 312
使用 CLI 配置高可用性 313
使用 GUI 配置高可用性 314
场景 315
在不同 AWS 区域部署具有私有 IP 地址的 VPX 高可用性对 317

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 AWS 非共享 VPC 的具有私有 IP 地址的高可用性对 317

先决条件 317

使用 AWS 非共享 VPC 部署具有私有 IP 地址的 VPX HA 对 318

使用 CLI 配置高可用性 320

使用 GUI 配置高可用性 321

使用 AWS 共享 VPC 部署具有私有 IP 地址的 VPX 高可用性对 321

先决条件 322

创建跨账户 IAM 角色 324

使用 NetScaler CLI 设置跨账户 IAM 角色 324

使用 NetScaler GUI 设置跨账户 IAM 角色 324

场景 325

用于 HA 私有 IP 解决方案的 AWS Transit Gateway 配置 328

故障排除 328

在 AWS Outposts 上部署 NetScaler VPX 实例 329

AWS Outposts 的工作原理 329

先决条件 329

使用 AWS Web 控制台在 AWS Outposts 上部署 NetScaler VPX 实例 329

在包含 AWS Outposts 的混合云上部署 NetScaler VPX 实例 330

参考 331

使用 NetScaler Web App Firewall 保护 AWS API Gateway 331

在 AWS API 网关前部署 NetScaler 设备 332

配置启用 WAF 的 NetScaler 设备 333

NetScaler 功能和特性 334

添加后端 AWS 自动扩缩服务 335

开始之前 336

将 AWS 自动扩缩服务添加到 NetScaler VPX 实例 337

在 AWS 上部署 NetScaler GSLB 342

DBS 概述 343

© 1997–2026 Citrix Systems, Inc. All rights reserved.

基于域名的服务 (DBS) 与 ELB 343

配置 AWS 组件 343

安全组 343

配置基于域名的全局服务器负载均衡服务 345

部署类型 345

CFT 部署 345

部署步骤 346

用于混合云和多云部署的 NetScaler 全局负载平衡 347

NetScaler 混合云和多云 GSLB 解决方案 347

安全组配置 348

NetScaler 混合云和多云 GSLB 解决方案的功能 348

与其他负载平衡解决方案的兼容性 348

GSLB 方法 348

GSLB 拓扑 349

IPv6 支持 349

监控 349

持久性 349

使用 NetScaler ADM StyleBook 进行配置 350

NetScaler 混合云和多云 GSLB 解决方案配置工作流 350

使用 StyleBooks 在 NetScaler LB 节点上配置 GSLB 352

使用用于 LB 节点的 Multi-cloud GSLB StyleBook 在父子拓扑中配置子站点 352

CloudFormation 模板部署 354

CFT 三网卡部署 354

先决条件 355

GSLB 先决条件 357

其他资源 357

配置 NetScaler VPX 实例以使用 SR-IOV 网络接口 357

将接口类型更改为 SR-IOV 357

© 1997–2026 Citrix Systems, Inc. All rights reserved.

更改接口类型为 SR-IOV 358

在高可用性设置上配置 SR-IOV 359

配置 NetScaler VPX 实例以使用 AWS ENA 增强网络 360

在 AWS 上升级 NetScaler VPX 实例 360

更改 AWS 上 NetScaler VPX 实例的 EC2 实例类型 361

升级 AWS 上 NetScaler VPX 实例的吞吐量或软件版本 361

使用客户许可证（自带许可证） 361

使用实用程序许可证（按小时计费的实用程序许可证） 361

升级 AWS 上的 NetScaler VPX 实例的系统软件 362

通过使用 NetScaler 高可用性配置升级到新的 NetScaler AMI 实例 362

先决条件和注意事项 362

在 AWS 上排查 VPX 实例故障 366

AWS 常见问题 366

在 Microsoft Azure 上部署 NetScaler VPX 实例 370

先决条件 370

NetScaler VPX 实例在 Azure 上的工作原理 371

多 NIC 多 IP 架构 371

单 NIC 多 IP 架构 372

单 NIC 单 IP 372

NetScaler VPX 许可 372

VPX 性能和推荐的 Azure 实例类型 373

注意事项 373

Azure 中 NetScaler VPX 实例的 IPv6 支持 374

限制 374

Azure 术语 375

Microsoft Azure 上 NetScaler VPX 实例的网络架构 378

通过网络地址转换的流量流 379

端口使用指南 380

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置 NetScaler VPX 独立实例 381
开始之前 381
配置步骤摘要 381
配置资源组 382
配置网络安全组 382
配置虚拟网络和子网 383
配置第二个子网 385
配置存储帐户 387
配置可用性集 388
配置 NetScaler VPX 实例 389
为 NetScaler VPX 独立实例配置多个 IP 地址 393
用例 393
开始之前 394
步骤 2：配置 NetScaler 拥有的 IP 地址 397
配置具有多个 IP 地址和网卡的高可用性设置 397
使用可用性集实现高可用性 398
使用 NetScaler® 高可用性模板配置 HA-INC 节点 399
使用可用性区域实现高可用性 401
使用 Azure Monitor 中的指标监视实例 403
注意事项 403
如何在 Azure 监视器中查看指标 403
使用 PowerShell 命令配置具有多个 IP 地址和 NIC 的高可用性设置 404
使用 PowerShell 命令配置 HA-INC 节点 405
场景：HA-INC PowerShell 部署 405
参数设置 406
在 Azure 上部署处于浮动 IP 禁用模式的 ALB 的 NetScaler 高可用性对 424
处于浮动 IP 禁用模式的 ALB 的 HA 部署架构 424
先决条件 425

© 1997–2026 Citrix Systems, Inc. All rights reserved.

如何在 Azure 上部署禁用 ALB 浮动 IP 的 VPX HA 对 425
配置 NetScaler VPX 实例以使用 Azure 加速网络 444
先决条件 445
限制 445
支持加速网络的网卡 445
如何使用 Azure 控制台在 NetScaler VPX 实例上启用加速网络 445
使用 Azure PowerShell 启用加速网络 451
使用 NetScaler 的 FreeBSD Shell 验证接口上的加速网络 453
使用 ADC CLI 验证接口上的加速网络 455
NetScaler 中的注意事项 457
将 VLAN 配置到 PV 接口 457
使用 NetScaler® 高可用性模板和 Azure ILB 配置 HA-INC 节点 458
示例配置 468
使用 NetScaler® 高可用性模板为面向 Internet 的应用程序配置 HA-INC 节点 469
示例配置 479
同时配置带有 Azure 外部和内部负载均衡器的高可用性设置 480
在 Azure VMware Solution 上安装 NetScaler VPX 实例 484
先决条件 485
VMware 云硬件要求 485
OVF Tool 1.0 系统要求 486
下载 NetScaler VPX 安装文件 487
部署 Azure VMware 解决方案 487
连接到运行 Windows 的 Azure 虚拟机 488
访问您的私有云 vCenter 门户 491
在 Azure 门户中创建 NSX-T 段 493
在 VMware 云上安装 NetScaler VPX 实例 494
在 Azure VMware 解决方案上配置 NetScaler VPX 独立实例 496
先决条件 497

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 NetScaler 负载均衡器在 AVS 上配置 NetScaler VPX 独立实例 497
使用 Azure 负载均衡器在 AVS 上配置 NetScaler VPX 独立实例 498
在 Azure VMware 解决方案上配置 NetScaler VPX 高可用性设置 499
先决条件 500
配置步骤 500
配置 Azure 路由服务器与 NetScaler VPX HA 对 501
先决条件 502
如何配置 Azure 路由服务器与 NetScaler VPX HA 对 502
添加 Azure Autoscale™ 设置 506
开始之前 507
将 VMSS 添加到 NetScaler VPX 实例 507
创建云配置文件时需要注意的事项 510
在 Azure 中从非托管磁盘迁移到托管磁盘 512
参考 512
用于 NetScaler VPX 部署的 Azure 标签 512
Azure 标签如何用于 VPX 部署 512
开始之前 513
如何通过使用 VPX GUI 添加 Azure 标签设置 514
如何使用 VPX CLI 添加 Azure 标签设置 516
故障排除 517
在 NetScaler VPX 实例上配置 GSLB 518
场景 519
参数 519
创建 VM 522
创建资源组 523
创建存储帐户 523
创建可用性集 523
创建虚拟网络 523

© 1997–2026 Citrix Systems, Inc. All rights reserved.

创建公共 IP 地址 524

创建 NIC 524

创建 VM 配置对象 525

获取凭据并设置操作系统属性 525

添加 NIC 525

指定操作系统磁盘并创建 VM 526

IP 配置详细信息 526

配置 GSLB 站点和其他设置 528

灾难恢复 529

用于灾难恢复的多网卡多 IP（三网卡）部署 529

用于灾难恢复的单网卡多 IP（一网卡）部署 529

在主动-备用高可用性设置上配置 GSLB 530

方案 530

参数设置 531

使用前端 IP 地址和规则配置 ALB 以允许 GSLB 和 DNS 流量 532

在每个高可用性对上启用 GSLB 534

在 Azure 上部署 NetScaler GSLB 535

DBS 概述 535

使用 Azure 负载均衡器 (ALB) 的基于域名的服务 536

Azure GSLB 先决条件 536

配置 Azure 组件 537

配置 NetScaler GSLB 基于域的服务 538

流量管理配置 538

GSLB 配置 538

其他资源 543

在 Azure Local 上部署 NetScaler VPX 实例 543

在 Azure Local 上部署 NetScaler VPX 实例的先决条件 543

如何使用 Windows Admin Center 中的 VHD 在 Azure Local 上部署 NetScaler VPX 实例 543

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 Azure 上部署 NetScaler® Web App Firewall 545
NetScaler Web App Firewall 部署策略 545
配置 Web 应用程序防火墙 546
SQL 注入 547
跨站点脚本 547
缓冲区溢出检查 547
虚拟补丁/签名 547
应用程序安全分析 547
ADM 上的集中式学习 548
StyleBooks 549
安全洞察分析 549
获取有关安全漏洞的详细信息 549
查看日志表达式详细信息 550
安全违规 552
查看应用程序安全违规详情 552
违规类别 552
设置 552
启用高级安全分析 552
启用 Web 事务设置 553
安全违规仪表板 554
Bot 洞察 554
查看 Bot 554
查看 CAPTCHA 机器人 556
查看机器人陷阱 556
查看机器人详细信息 557
高级搜索 557
异常高的请求速率 558
僵尸程序检测 559

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IP 信誉 559
NetScaler Web App Firewall 和 OWASP 十大安全风险 – 2021 560
A1:2021 访问控制失效 560
NetScaler Web 应用防火墙 保护 561
A2:2021 - 加密故障 561
NetScaler Web 应用防火墙防护 561
A3:2021- 注入 561
NetScaler Web 应用防火墙 保护 561
A5:2021 - 安全配置错误 562
NetScaler Web 应用防火墙 保护 562
A6:2021 - 易受攻击和过时的组件 563
NetScaler Web 应用防火墙防护 563
A7:2021–身份验证失效 563
NetScaler Web App Firewall 保护措施 563
A8:2021 - 软件和数据完整性故障 563
NetScaler Web App Firewall 保护措施 563
A9:2021 - 安全日志记录和监控故障 564
NetScaler Web App Firewall 保护措施 564
参考 564
为 NetScaler Gateway 设备配置地址池内网 IP 564
在 Azure 门户中注册私有 IP 地址 565
在 NetScaler Gateway 设备中配置地址池 566
使用 PowerShell 命令为 NetScaler VPX 独立实例配置多个 IP 地址 567
用例 567
脚本 569
参数 569
1. 创建资源组 572
2. 创建存储帐户 572

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 创建可用性集 572

4. 创建网络安全组 572

5. 创建虚拟网络 572

6. 创建公共 IP 地址 573

7. 分配 IP 配置 573

8. 创建 NIC 574

9. 创建 NetScaler VPX 实例 574

10. 检查网卡配置 575

11. 检查 VPX 端配置 575

用于 Azure 部署的其他 PowerShell 脚本 575

预配 NetScaler VPX 独立实例 575

在具有 Azure 外部负载均衡器的高可用性设置中预配 NetScaler VPX 对 581

在具有 Azure 内部负载均衡器的高可用性设置中预配 NetScaler VPX 对 591

Azure 常见问题 599

在 Google Cloud Platform 上部署 NetScaler VPX 实例 600

支持的功能 600

限制 600

硬件要求 600

注意事项 600

场景：部署多网卡、多 IP 的独立 VPX 实例 600

部署步骤摘要 601

场景：部署单 NIC 独立 VPX 实例 606

部署步骤摘要 606

在 GCP 上部署 VPX 实例后需要注意的事项 613

NetScaler VPX 许可 613

GCP 上支持的 NetScaler VPX 产品 614

支持的 GCP 机器类型系列 614

用于部署 NetScaler VPX 实例的 GDM 模板 614

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Marketplace 映像 614
资源 615
相关信息 615
在 Google Cloud Platform 上部署 VPX 高可用性对 615
用于在 GCP 上部署 VPX 高可用性对的 GDM 模板 616
GCP 上 VPX 高可用性对的转发规则支持 616
先决条件 616
限制 616
在 Google Cloud Platform 上部署具有外部静态 IP 地址的 VPX 高可用性对 617
开始之前 617
如何在 Google Cloud Platform 上部署 VPX HA 对 618
步骤 1. 创建 VPC 网络 619
步骤 2. 创建两个 VPX 实例 619
步骤 3. 配置高可用性 620
在 Google Cloud Platform 上部署具有私有 IP 地址的单 NIC VPX 高可用性对 627
开始之前 627
如何在 Google Cloud Platform 上部署 VPX 高可用性对 629
步骤 1. 创建 VPC 网络 630
步骤 2. 创建两个 VPX 实例 630
步骤 3. 配置高可用性 632
使用 GUI 配置高可用性 632
使用 CLI 配置高可用性 634
在 Google Cloud Platform 上部署具有私有 IP 地址的 VPX 高可用性对 636
开始之前 636
如何在 Google Cloud Platform 上部署 VPX 高可用性对 639
步骤 1. 创建 VPC 网络 640
步骤 2. 创建两个 VPX 实例 640
步骤 3. 配置高可用性 642

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 GUI 配置高可用性 642

使用 CLI 配置高可用性 645

在 Google Cloud VMware Engine 上安装 NetScaler VPX 实例 647

先决条件 648

VMware 云硬件要求 649

OVF Tool 1.0 系统要求 649

下载 NetScaler VPX 安装文件 650

部署 谷歌云 VMware 引擎 650

访问您的私有云 vCenter 门户 654

在 GCVE NSX-T 门户中创建 NSX-T 段 656

在 VMware 云上安装 NetScaler VPX 实例 662

在 VMware 云上为 NetScaler VPX 实例分配公共 IP 地址 665

添加后端 GCP 自动扩缩服务 666

开始之前 667

将 GCP 自动扩缩服务添加到 NetScaler VPX 实例 668

GCP 上的 NetScaler VPX 实例的 VIP 扩展支持 671

注意事项 672

开始之前 672

在 NetScaler VPX 实例上为 VIP 扩展配置外部 IP 地址 674

在 NetScaler VPX 实例上设置具有外部 IP 地址的负载平衡虚拟服务器 677

在 GCP 上排查 VPX 实例故障 680

NetScaler VPX 实例上的巨型帧 681

为在 VMware ESX 上运行的 VPX 实例配置巨型帧 681

为在 Linux-KVM 服务器上运行的 VPX 实例配置巨型帧 681

为在 Citrix XenServer 上运行的 VPX 实例配置巨型帧 682

为在 AWS 上运行的 VPX 实例配置巨型帧 682

常见问题 683

功能和特性 683

© 1997–2026 Citrix Systems, Inc. All rights reserved.

什么是 NetScaler VPX? 683

NetScaler VPX 是否包含 ADC 设备的所有 Web 应用程序优化功能? 683

在 NetScaler VPX 上使用 Citrix Application Firewall 时是否存在任何限制? 683

NetScaler VPX 上的 NetScaler Gateway 与 NetScaler 设备上的 NetScaler Gateway 之间是否存在任何差异? 683

除了能够在虚拟机监控程序上运行这一明显差异之外，NetScaler VPX 与 NetScaler 物理设备有何不同? 684

NetScaler VPX 在应用交付市场中扮演着怎样的角色? 684

NetScaler VPX 如何融入我们的 Citrix 交付中心战略? 684

加密 684

NetScaler VPX 是否支持 SSL 卸载? 684

安装在托管 NetScaler VPX 的服务器上的第三方 SSL 卡是否能加速 SSL 加密或解密? 685

NetScaler VPX 是否支持与物理 NetScaler 设备相同的加密密码? 685

NetScaler VPX 的 SSL 事务吞吐量是多少? 685

定价和打包 685

NetScaler VPX 如何打包? 685

NetScaler VPX 在所有虚拟机管理程序上的定价都相同? 685

所有虚拟机管理程序上的 VPX 都使用相同的 NetScaler SKU? 685

NetScaler VPX 许可证可以从一个虚拟机管理程序移动到另一个（例如从 VMware 到 Hyper-V）? 685

NetScaler VPX 实例可以升级? 685

如果我想以高可用性对的形式部署 NetScaler VPX，我需要多少许可证? 686

NetScaler VPX Express 和 90 天免费试用 686

NetScaler VPX Express 是否包含所有 NetScaler 标准功能 它是否包含 NetScaler Gateway 以及用于 Citrix Virtual Apps（以前称为 XenApp）Web Interface 和 XML 代理的负载均衡? 686

NetScaler VPX Express 是否包含所有 NetScaler 标准功能？它是否包含 NetScaler Gateway 以及用于 Citrix Virtual Apps Web Interface 和 XML 代理的负载均衡? 686

NetScaler VPX Express 需要许可证吗? 686

NetScaler VPX Express 许可证会过期吗? 686

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler VPX Express 是否包含五个免费的 NetScaler Gateway 并发许可证? 686
客户可以下载的 NetScaler VPX Express 数量是否有限制? 686
NetScaler VPX Express 是否支持与 NetScaler MPX 设备相同的加密密码? 687
我可以为 NetScaler VPX Express 提交技术支持案例? 687
NetScaler VPX Express 可以升级到零售版本吗? 687
虚拟机管理程序 687
NetScaler VPX 支持哪些 VMware 版本? 687
对于 VMware，您可以为 VPX 分配多少个虚拟网络接口? 687
如何从 vSphere 访问 NetScaler VPX 命令行? 687
如何访问 NetScaler VPX GUI? 687
安装在同一 VMware ESX 上的两个 NetScaler VPX 实例能否配置为高可用性设置? 687
运行在两个不同 VMware ESX 系统上的两个 NetScaler VPX 实例能否配置为高可用性设置? 688
对于 VMware，NetScaler VPX 是否支持接口相关事件? 688
对于 VMware，NetScaler VPX 是否支持标记 VLAN? 688
对于 VMware，NetScaler VPX 是否支持链路聚合和 LACP? 688
如何访问 NetScaler VPX 文档? 688
容量规划或大小调整 688
NetScaler VPX 的预期性能如何? 688
鉴于服务器 CPU 功率各不相同，我们如何估算 NetScaler 实例的最大性能? 688
NetScaler VPX 带宽或吞吐量限制：仅入站流量，还是入站和出站流量? 688
同一服务器上是否可以运行多个 NetScaler VPX 实例? 689
如果物理服务器上运行了多个 NetScaler VPX 实例，每个 NetScaler VPX 实例的最低硬件要求是什么? 689
我可以在同一服务器上托管 NetScaler VPX 和其他应用程序吗? 689
CPU 核心增加对单个 NetScaler VPX 实例性能的影响? 689
NetScaler VPX 在空闲时 CPU 占用率超过 90% 的原因? 689
系统要求 690
NetScaler VPX 的最低硬件要求是什么? 690

© 1997–2026 Citrix Systems, Inc. All rights reserved.

什么是 Intel VT-x? 690

VT-x 有多常见? 691

NetScaler VPX 是否有硬件兼容性列表 (HCL)? 691

NetScaler VPX 基于哪个版本的 NetScaler OS? 691

既然 NetScaler VPX 在 BSD 上运行，它能否在安装了 BSD Unix 的服务器上原生运行? 691

其他技术常见问题 691

具有多个网卡的物理服务器上的链路聚合是否有效? 691

VPX 是否支持基于 MAC 的转发 (MBF)？与 NetScaler 设备实现相比是否有任何变化? 691

NetScaler VPX 升级过程如何执行? 691

闪存和磁盘空间如何分配 我们可以更改它吗? 691

我们能否添加新的硬盘以增加 NetScaler VPX 实例上的空间? 692

NetScaler VPX 的版本编号以及与其他版本的互操作性如何? 693

NetScaler VPX 可以与 NetScaler 设备一起构成高可用性设置? 693

NetScaler VPX 中可见的所有接口是否与 Hypervisor 上的接口数量直接相关? 693

为什么 NetScaler VPX 上的半虚拟化 (PV) 接口显示为 1G 接口 (`1/x`)，即使底层物理接口是 10G？这是否意味着最大吞吐量限制为 1 Gbps? 693

Citrix Hypervisor XenMotion、VMware VMotion 或 Hyper-V 实时迁移能否用于移动 NetScaler VPX 的活动实例? 693

fix 694

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持矩阵和使用指南

本文档列出了 NetScaler VPX 和 VPX FIPS 实例上支持的不同虚拟机管理程序和功能，除非特别声明某个虚拟机管理程序在 VPX FIPS 上不受支持。本文档还描述了其使用指南和已知限制。

XenServer 上的 VPX 实例

XENSERVER 版本	系统 ID	性能范围
支持 8.2（13.0 64.x 及更高版本）、8.0、7.6、7.1	450000	10 兆位/秒 到 40 吉位/秒

VMware ESXi 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
ESXi 9.0.2	2026/01/20	25148076	13.1-61.x 及更高版本	10 Mbps 到 100 Gbps
ESXi 8.0 更新 3k	2026/07/29	25595708	13.1-64.x 及更高版本	
ESXi 8.0 更新 3j	2026/05/27	25429389	13.1-63.x 及更高版本	
ESXi 8.0 更新 3g	2025/07/29	24859861	13.1-58.x 及更高版本	
ESXi 8.0 更新 3f	2025/07/15	24784735	13.1-58.x 及更高版本	
ESXi 8.0 更新 3e	2025/04/10	24674464	13.1-58.x 及更高版本	
ESXi 8.0 更新 3d	2025/03/04	24585383	13.1-56.x 及更高构建版本	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
ESXi 8.0 更新 3c	2025/01/23	24414501	13.1-55.x 及更高构建版本	
ESXi 8.0 更新 3b	2024/09/17	24280767	13.1-53.x 及更高构建版本	
ESXi 8.0 更新 3	2024/06/25	24022510	13.1-53.x 及更高版本	
ESXi 8.0 更新 2c	2024/05/21	23825572	13.1-53.x 及更高版本	
ESXi 8.0 更新 2b	2024/02/29	23305546	13.1–49.15，以及 13.1-52.x 及更高版本	
ESXi 8.0 更新 2	2023/09/21	22380479	13.1-52.x 及更高版本	
ESXi 8.0 更新 1	2023/04/18	21495797	13.1-45.x 及更高版本	
ESXi 8.0c	2023/03/30	21493926	13.1-45.x 及更高版本	
ESXi 8.0	2022/10/11	20513097	13.1-42.x 及更高版本	
ESXi 7.0 更新 3w	2025/07/15	24784741	13.1-58.x 及更高版本	
ESXi 7.0 更新 3s	2025/03/04	24585291	13.1-55.x 及更高版本	
ESXi 7.0 更新 3r	2024/12/12	24411414	13.1-55.x 及更高版本	
ESXi 7.0 更新 3q	2024/05/21	23794027	13.1-53.x 及更高版本	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
ESXi 7.0 更新 3p	2024/03/05	23307199	13.1-52.x 及更高版本	
ESXi 7.0 更新 3o	2023/09/28	22348816	13.1-51.x 及更高版本	
ESXi 7.0 更新 3n	2023/07/06	21930508	13.1-49.x 及更高版本	
ESXi 7.0 更新 3m	2023/05/03	21686933	13.1-48.x 及更高版本	
ESXi 7.0 更新 3i	2022/12/08	20842708	13.1-37.x 及更高构建版本	
ESXi 7.0 更新 3f	2022/07/12	20036589	13.1-33.x 及更高构建版本	
ESXi 7.0 更新 3d	2022/03/29	19482537	13.1-27.x 及更高构建版本	
ESXi 7.0 更新 3c	2022/01/27	19193900	13.1-21.x 及更高版本	
ESX 7.0 更新 2d	2021/09/14	18538813	13.1-9.x 及更高版本	
ESX 7.0 更新 2a	2021/04/29	17867351	13.1-4.x 及更高版本	

注意：

每个 ESXi 补丁支持都在前面表格中指定的 NetScaler VPX 版本上进行了验证，并适用于 NetScaler VPX 13.1 版本的所有更高版本。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Hyper-V 上的 VPX 实例

HYPER-V 版本	SYSID	NETSCALER VPX 版本	性能范围
2016, 2019	450020	13.1-4.x 及更高版本	10 兆比特每秒 到 3 吉比特每秒
2022	同上	13.1-58.x 及更高版本	同上
2025		13.1-60.x 及更高版本	

Azure Local 上的 VPX 实例

组件	支持的版本/内部版本	SYSID
NetScaler VPX	13.1-61.x 及更高版本	450020
Azure 本地操作系统内部版本	25398.1965、26100.7171 和 20349.3692	

有关 Azure 本地版本发布的更多信息，请参阅 Microsoft 文档。

Nutanix AHV 上的 VPX 实例

NetScaler VPX 通过 Citrix Ready 合作伙伴关系 在 Nutanix AHV 上受支持。Citrix Ready 是一项技术合作伙伴计划，旨在帮助软件和硬件供应商开发其产品并将其与 NetScaler 技术集成，以用于数字工作区、网络和分析。

有关在 Nutanix AHV 上部署 NetScaler VPX 实例的分步方法，请参阅 在 Nutanix AHV 上部署 NetScaler VPX。

第三方支持：

如果您在 NetScaler® 环境中遇到特定第三方 (Nutanix AHV) 集成的任何问题，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，则合作伙伴可以联系 NetScaler 支持以获得进一步帮助。来自合作伙伴的专门技术资源将与 NetScaler 支持团队协作，直到问题解决。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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	450070	10 兆比特每秒 至 100 吉比特每秒
乌班图 16.04、乌班图 18.04、乌班图 22.04		

注意事项：

在使用 KVM 虚拟机管理程序时，请注意以下几点。

- VPX 实例适用于表 1-4 中提及的虚拟机管理程序发布版本，而非版本内的补丁发布。但是，VPX 实例应能与受支持版本的补丁发布无缝协作。如果未能正常工作，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：
  a. 编辑 /etc/default/grub 并将 `"kvm_intel.preemption_timer=0"` 附加到 `GRUB_CMDLINE_LINUX` 变量。
  b. 使用 `"# grub2-mkconfig -o /boot/grub2/grub.cfg"` 命令重新生成 grub.cfg。
  c. 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：
  a. 编辑 /etc/default/grub 并将 `"kvm_intel.preemption_timer=0"` 附加到 `GRUB_CMDLINE_LINUX` 变量。
  b. 使用 `"# grub-mkconfig -o /boot/grub/grub.cfg “` 命令重新生成 grub.cfg。
  c. 重新启动主机。

公共云上的 VPX 实例

公共云	SYSID	性能范围
AWS	450040	从 10 Mbps 到 30 Gbps
艾祖尔	450020	从10 Mbps到10 Gbps
GCP	450070	从10 Mbps到10 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

虚拟机管理程序上支持的 VPX 功能

虚拟机管理程序 → 功能 ↓	XEN SERVER 上的 VPX		VMWARE ESX 上的 VPX			微软 HYPER-V 上的 VPX		通用 KVM 上的 VPX		
接口 →	PV	SR-IOV	PV	SR-IOV	模拟	PCI 直通	PV	PV	SR-IOV	PCI 直通
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/HA Mon	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]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

虚拟机管理程序 → 功能 ↓	XEN SERVER 上的 VPX	VMWARE ESX 上的 VPX	微软 HYPER-V 上的 VPX	通用 KVM 上的 VPX						
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

公共云上支持的 VPX 功能

公共云 → 功能 ↓	AWS 上的 VPX	AZURE 上的 VPX	GCP 上的 VPX
多 PE 支持	是	是	是
集群支持	是	否	是
VLAN 标记	否	否	否
检测链路事件/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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

公共云 → 功能 ↓	AWS 上的 VPX	AZURE 上的 VPX	GCP 上的 VPX
热插拔	是	否	否

前面两个表格中使用的上标数字（1、2、3）指的是以下对应编号的要点：

1. SRIOV 上支持客户端和服务器端接口的集群，但不支持背板。
2. NetScaler VPX 实例中不记录接口 DOWN 事件。
3. 对于静态 LA，流量可能仍会发送到物理状态为 DOWN 的接口上。

以下几点适用于前面两个表格中列出的各项功能：

- 对于 LACP，对等设备根据 LACP 超时机制了解接口 DOWN 事件。
  - 短超时：3 秒
  - 长超时：90 秒
- 对于 LACP，请勿在虚拟机之间共享接口。
- 对于动态路由，收敛时间取决于路由协议，因为未检测到链路事件。
- 如果未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 状态取决于链路状态。
- 如果发生链路故障，高可用性中不会发生部分故障检测。如果发生链路故障，可能会出现高可用性裂脑情况。
  - 当 VPX 实例生成任何链路事件（禁用、启用、重置）时，链路的物理状态不会改变。对于静态 LA，对等方发起的任何流量都会在该实例上丢弃。
  - 要在 VMware ESX 上使用 VLAN 标记功能，请将 VMware ESX 服务器的 vSwitch 上的端口组 VLAN ID 设置为 1–4095。
- 不支持带有 ENA 接口的 VPX 实例的热插拔，如果尝试热插拔，实例的行为可能无法预测。热添加仅支持在 AWS 上使用 NetScaler 的 PV 和 SRIOV 接口。
- 通过 AWS Web 控制台或 AWS CLI 接口热移除 NetScaler 的 PV、SRIOV 和 ENA 接口不受支持。如果尝试热移除，实例的行为可能无法预测。

支持的浏览器

有关访问 NetScaler GUI 14.1 和 13.1 版本所支持的浏览器的信息，请参阅 兼容的浏览器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler VPX™ 支持的处理器

平台	INTEL 处理器	AMD 处理器
思杰虚拟机监控程序	是	否
ESXi 虚拟机监控程序	是	是
超V	是	否
KVM	是	否
AWS	是	是
微软 Azure	是	是
GCP	是	是

NetScaler VPX 支持的 NIC

下表列出了 VPX 平台或云上支持的 NIC。

NIC → 平台 ↓	迈络思 CX-3	迈络思 CX-4	迈络思 CX-5	英特尔 82599 SRIOV VF	英特尔 X710/ X722/ XL710 SRIOV VF	INTEL X710/ XL710/ XXV710 PCI 直通模式
Citrix 虚拟机监控程序	不适用	不适用	不适用	是	是	否
ESXi 管理程序	否	是	否	是	否	是
Hyper-V 虚拟化	不适用	不适用	不适用	否	否	否
KVM	否	是	是	是	是	否
AWS	不适用	不适用	不适用	是	不适用	不适用

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NIC → 平台 ↓	迈络思 CX-3	迈络思 CX-4	迈络思 CX-5	英特尔 82599 SRIOV VF	英特尔 X710/ X722/ XL710 SRIOV VF	INTEL X710/ XL710/ XXV710 PCI 直通模式
阿祖尔	是	是	是	不适用	不适用	不适用
GCP	不适用	不适用	不适用	不适用	不适用	不适用

使用指南

请遵循以下使用指南：

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

请参阅 Performance Best Practices for VMware vSphere 6.5 文档中的“**VMware ESXi CPU 考量**”部分。以下是摘录：

- 不建议将具有高 CPU/内存需求的虚拟机放置在过度承诺的主机或群集上。
- 在大多数环境中，ESXi 允许在不影响虚拟机性能的情况下进行显著级别的 CPU 过度承诺。在主机上，您可以运行比该主机中物理处理器核心总数更多的 vCPU。
- 如果 ESXi 主机 CPU 饱和，即虚拟机和主机上的其他负载需要主机拥有的所有 CPU 资源，则对延迟敏感的工作负载可能无法良好运行。在这种情况下，您可能需要减少 CPU 负载，例如通过关闭一些虚拟机或将其迁移到不同的主机（或允许 DRS 自动迁移它们）。
- Citrix 建议使用最新的硬件兼容性版本，以利用 ESXi 虚拟机管理程序为虚拟机提供的最新功能集。有关硬件和 ESXi 版本兼容性的更多信息，请参阅 VMware 文档。
- NetScaler VPX 是一种对延迟敏感的高性能虚拟设备。为了提供其预期的性能，该设备需要 vCPU 预留、内存预留和主机上的 vCPU 绑定。此外，必须在主机上禁用超线程。如果主机不满足这些要求，则会出现高可用性故障转移、VPX 实例内的 CPU 峰值、访问 VPX CLI 迟钝、pit boss 守护程序崩溃、数据包丢失和低吞吐量等问题。

如果满足以下两个条件之一，则虚拟机管理程序被视为过度配置：

- 主机上配置的虚拟核心 (vCPU) 总数大于物理核心 (pCPU) 总数。
- 配置的虚拟机总数消耗的 vCPU 数量多于 pCPU 总数。

  如果实例过度配置，虚拟机管理程序可能无法保证为该实例预留的资源（例如 CPU、内存等），这可能是由于虚拟机管理程序调度开销、错误或虚拟机管理程序限制所致。此行为可能导

© 1997–2026 Citrix Systems, Inc. All rights reserved.

致 NetScaler 缺少 CPU 资源，并可能导致“**使用指南**”下第一点中提到的问题。作为管理员，建议您减少主机上的租用，以便主机上配置的 vCPU 总数小于或等于 pCPU 总数。

示例：

对于 ESX 虚拟机管理程序，如果在 `esxtop` 命令输出中，VPX vCPU 的 `%RDY%` 参数大于 0，则表示 ESX 主机存在调度开销，这可能导致 VPX 实例出现与延迟相关的问题。

在这种情况下，请减少主机上的租用，以便 `%RDY%` 始终返回 0。或者，联系虚拟机管理程序供应商以排查未兑现资源预留的原因。

- 热添加仅支持在 AWS 上使用 NetScaler 的 PV 和 SRIOV 接口。具有 ENA 接口的 VPX 实例不支持热插拔，如果尝试热插拔，实例的行为可能无法预测。
- 通过 AWS Web 控制台或 AWS CLI 接口进行热移除，NetScaler 不支持 PV、SRIOV 和 ENA 接口。如果尝试热移除，实例的行为可能无法预测。

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)]`

  允许每个虚拟机使用已分配给其他虚拟机但未被使用的 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**：允许已分配但未使用的 CPU 资源被其他虚拟机使用。
  - **NO**：为已分配的虚拟机保留所有 CPU 资源。此选项在虚拟机管理程序和云环境中显示 VPX CPU 使用率的百分比更高。
  - **DEFAULT**：否。

  注意：

  在所有 NetScaler VPX 平台上，主机系统上的 vCPU 使用率为 100%。键入 `set ns vpxparam –cpuyield YES` 命令可覆盖此使用率。

  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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 如果形成群集，所有节点都将以“yield=DEFAULT”启动。
- 如果使用已设置为“yield=YES”的节点形成集群，则这些节点将使用“DEFAULT”yield添加到集群中。

> **注意：**
>
> 如果要将集群节点设置为“yield=YES”，则只能在形成集群后进行配置，而不能在形成集群之前进行配置。

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

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

- `show ns vpxparam`

  显示当前的 `vpxparam` 设置。

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 Citrix Ready 合作伙伴页面。
- 有关 VMware ESX 硬件版本，请参阅 升级 VMware Tools。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

优化 NetScaler VPX 在 VMware ESX、Linux KVM 和 Citrix Hypervisors 上的性能

NetScaler VPX 的性能因管理程序、分配的系统资源和主机配置而异。为了达到所需的性能，请首先遵循 VPX 数据表中的建议，然后使用本文档中提供的最佳实践进一步优化它。

VMware ESX 管理程序上的 NetScaler VPX 实例

本节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 管理程序上实现 NetScaler VPX 实例最佳性能的建议。

- ESX 主机上的推荐配置
- 使用 E1000 网络接口的 NetScaler VPX
- 使用 VMXNET3 网络接口的 NetScaler VPX
- 使用 SR-IOV 和 PCI 直通网络接口的 NetScaler VPX

ESX 主机上的推荐配置

为了使使用 E1000、VMXNET3、SR-IOV 和 PCI 直通网络接口的 VPX 达到高性能，请遵循以下建议：

- ESX 主机上配置的虚拟 CPU (vCPU) 总数必须小于或等于 ESX 主机上的物理 CPU (pCPU) 总数。
- 必须为 ESX 主机设置非统一内存访问 (NUMA) 亲和性和 CPU 亲和性，以获得良好结果。

  – 要查找 Vmnic 的 NUMA 亲和性，请本地或远程登录到主机，然后键入：

  ```
  #vsish -e get /net/pNics/vmnic7/properties | grep NUMA

  Device NUMA Node: 0
  ```

  - 要为 VM 设置 NUMA 和 vCPU 亲和性，请参阅 VMware 文档。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 E1000 网络接口的 NetScaler VPX

在 VMware ESX 主机上执行以下设置：

- 在 VMware ESX 主机上，从一个 pNIC vSwitch 创建两个 vNIC。多个 vNIC 会在 ESX 主机中创建多个 Rx 线程。这会增加 pNIC 接口的 Rx 吞吐量。
- 为您创建的每个 vNIC 在 vSwitch 端口组级别启用 VLAN。
- 为了提高 vNIC 传输 (Tx) 吞吐量，请在 ESX 主机中为每个 vNIC 使用单独的 Tx 线程。使用以下 ESX 命令：
  - 对于 ESX 5.5 版本：

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

  - 对于 ESX 6.0 及更高版本：

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

- 为了进一步提高 vNIC Tx 吞吐量，请为每个设备 (NIC) 队列使用单独的 Tx 完成线程和 Rx 线程。使用以下 ESX 命令：

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

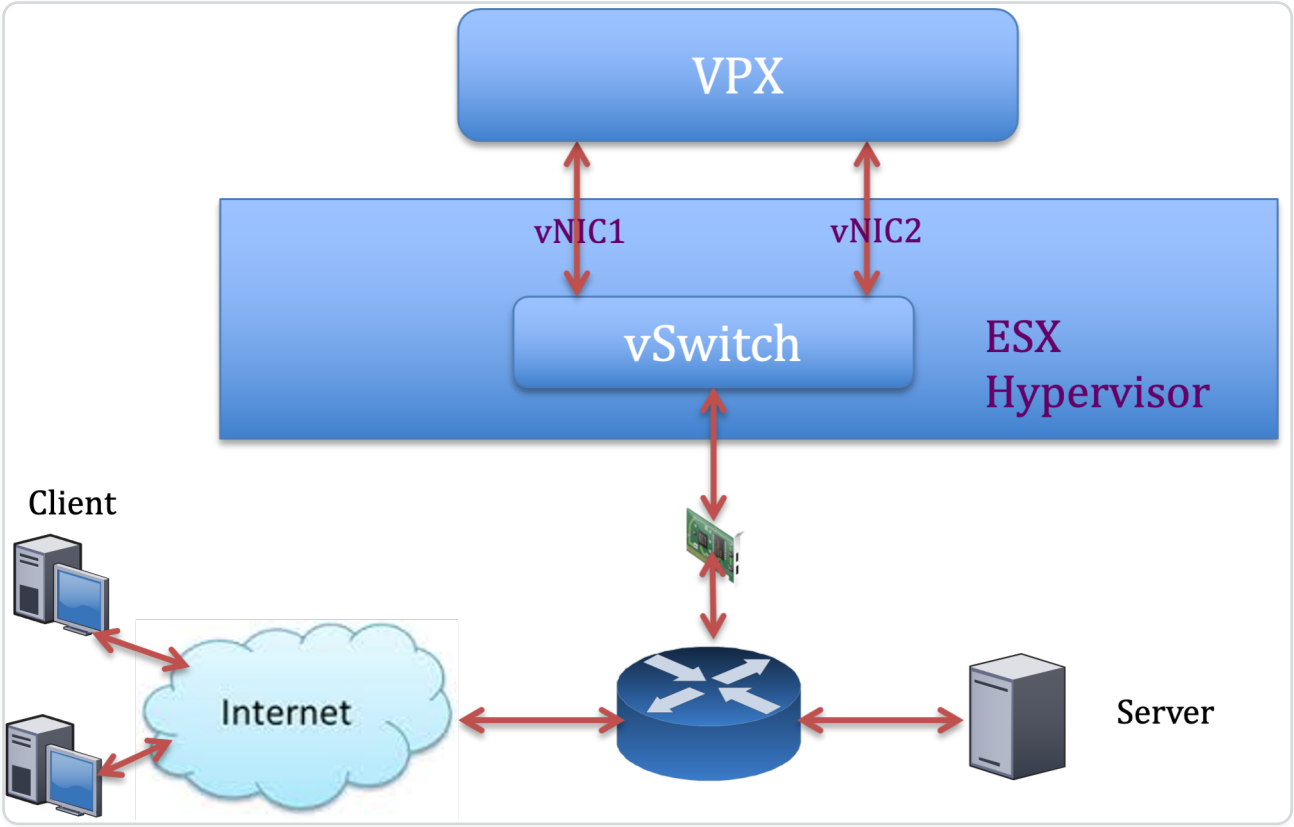
注意：

确保重新启动 VMware ESX 主机以应用更新的设置。

每个 pNIC 部署两个 vNIC

以下是 **每个 pNIC 两个 vNIC** 部署模型的示例拓扑和配置命令，该模型可提供更好的网络性能。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler VPX 示例配置：

为了实现前面示例拓扑中所示的部署，请在 NetScaler VPX 实例上执行以下配置：

- 在客户端，将 SNIP (1.1.1.2) 绑定到网络接口 1/1 并启用 VLAN 标记模式。

```
bind vlan 2 -ifnum 1/1 –tagged

bind vlan 2 -IPAddress 1.1.1.2 255.255.255.0
```

- 在服务器端，将 SNIP (2.2.2.2) 绑定到网络接口 1/1 并启用 VLAN 标记模式。

```
bind vlan 3 -ifnum 1/2 –tagged

bind vlan 3 -IPAddress 2.2.2.2 255.255.255.0
```

- 添加一个 HTTP 虚拟服务器 (1.1.1.100) 并将其绑定到服务 (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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
360 -CKA NO -TCPB NO -CMP NO

bind lb vserver v1 s1
```

注意：

确保在路由表中包含以下两个条目：

- 1.1.1.0/24 子网，网关指向 SNIP 1.1.1.2
- 2.2.2.0/24 子网，网关指向 SNIP 2.2.2.2

带有 VMXNET3 网络接口的 NetScaler VPX

为了使带有 VMXNET3 网络接口的 VPX 达到高性能，请在 VMware ESX 主机上执行以下设置：

- 从一个 pNIC vSwitch 创建两个 vNIC。多个 vNIC 会在 ESX 主机中创建多个 Rx 线程。这会增加 pNIC 接口的 Rx 吞吐量。
- 对于您创建的每个 vNIC，在 vSwitch 端口组级别启用 VLAN。
- 为了提高 vNIC 传输 (Tx) 吞吐量，为每个 vNIC 在 ESX 主机中使用单独的 Tx 线程。使用以下 ESX 命令：
  - 对于 ESX 5.5 版本：

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

  - 对于 ESX 6.0 及更高版本：

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

在 VMware ESX 主机上，执行以下配置：

- 在 VMware ESX 主机上，从 1 个 pNIC vSwitch 创建两个 vNIC。多个 vNIC 会在 ESX 主机中创建多个 Tx 和 Rx 线程。这会增加 pNIC 接口的 Tx 和 Rx 吞吐量。
- 为您创建的每个 vNIC 在 vSwitch 端口组级别启用 VLAN。
- 要提高 vNIC 的 Tx 吞吐量，请为每个设备 (NIC) 队列使用单独的 Tx 完成线程和 Rx 线程。使用以下命令：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

- 通过将以下设置添加到 VM 的配置中，将 VM 配置为每个 vNIC 使用一个传输线程：

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

- 通过将以下设置添加到 VM 的配置中，将 VM 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 ESX 主机上更多的 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：

请务必重新启动 VMware ESX 主机以应用更新的设置。

您可以将 VMXNET3 配置为**每个 pNIC 两个 vNIC**部署。有关更多信息，请参阅每个 pNIC 两个 vNIC 部署。

为 VMXNET3 设备在 VMware ESX 上配置多队列和 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，为 VMXNET3 接口配置的 Rx 和 Tx 队列数量默认切换为 1。您可以通过更改 ESX 上的某些配置，为 VMXNET3 设备配置多达 19 个 Rx 和 Tx 队列。此选项可提高性能并使数据包在 VPX 实例的 vCPU 之间均匀分布。

注意：

从 NetScaler 13.1 build 48.x 版本开始，NetScaler VPX 在 ESX 上为 VMXNET3 设备支持多达 19 个 Rx 和 Tx 队列。

先决条件：

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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler VPX 版本为 13.1 build 48.X 及更高版本。
- NetScaler VPX 配置为硬件版本 17 及更高版本的虚拟机，该虚拟机受 VMware ESX 7.0 及更高版本支持。

配置 VMXNET3 接口以支持超过 8 个 Rx 和 Tx 队列：

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

> **注意：**
>
> 增加队列数量也会增加 ESX 主机上的处理器开销。因此，在增加队列之前，请确保 ESX 主机中有足够的 CPU 资源。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量。在这种情况下，我们建议逐步增加队列数量。例如，从 8 增加到 12，然后到 16，再到 20，依此类推。在每个设置下评估性能，而不是直接增加到最大限制。

具有 SR-IOV 和 PCI 直通网络接口的 NetScaler VPX

要实现具有 SR-IOV 和 PCI 直通网络接口的 VPX 的高性能，请参阅 ESX 主机上的推荐配置。

Linux-KVM 平台上的 NetScaler VPX 实例

本节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 实例最佳性能的建议。

- KVM 的性能设置
- 具有 PV 网络接口的 NetScaler VPX
- 具有 SR-IOV 和 Fortville PCIe 直通网络接口的 NetScaler VPX

KVM 的性能设置

在 KVM 主机上执行以下设置：

使用 `lstopo` 命令查找网卡的 NUMA 域：

确保 VPX 和 CPU 的内存固定在同一位置。 在以下输出中，10G 网卡“ens2”绑定到 NUMA 域 #1。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
[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
```

从 NUMA 域分配 VPX 内存。

`numactl` 命令指示分配内存的 NUMA 域。在以下输出中，大约 10 GB RAM 从 NUMA 节点 #0 分配。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

要更改 NUMA 节点映射，请按照以下步骤操作。

1. 编辑主机上 VPX 的 .xml 文件。

```
/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. 启动 VPX。然后检查主机上的 `numactl -hardware` 命令输出，查看 VPX 的更新内存分配。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
[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 ~]#
```

将 VPX 的虚拟 CPU 绑定到物理核心。

- 要查看 VPX 的虚拟 CPU 到物理 CPU 的映射，请输入以下命令

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

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

虚拟 CPU 0–4 映射到物理核心 8–11。

- 要查看当前物理 CPU 使用情况，请输入以下命令：

```
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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 要更改虚拟 CPU 到物理 CPU 的绑定，有两种选择。
  - 在 VPX 启动后，使用以下命令在运行时更改它：

```
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，请像以前一样编辑 `.xml` 文件，并使用以下标签：

    a. 编辑主机上 VPX 的 .xml 文件

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

    b. 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>
```

    c. 关闭 VPX。

    d. 使用以下命令更新虚拟机的配置信息，其中包含 NUMA 节点映射：

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. 启动 VPX。然后检查主机上的 `virsh vcpupin <VPX name>` 命令输出，以查看更新的 CPU 绑定。

消除主机中断开销。

- 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 VPX 的 vCPU 所绑定的同一 pCPU 上。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执行的虚拟机退出，请使用 `kvm_stat` 命令。

  ```
  [root@localhost ~]# kvm_stat -1  | grep EXTERNAL

  kvm_exit(EXTERNAL_INTERRUPT)  1728349 27738

  [root@localhost ~]#
  ```

  1+M 数量级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。任何超出此范围的值都可能表明有一个或多个主机中断向量映射到同一 pCPU。

- 检测主机中断并迁移主机中断。

  当您对“/proc/interrupts”文件运行 `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 pCPU，则其对应的计数器会递增。

  将与 NetScaler VPX 的 pCPU 重叠的任何中断移动到未使用的 pCPU：

  ```
  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 平衡。

  禁用 IRQ 平衡守护程序，以便不会即时发生重新调度。

  ```
  service irqbalance stop

  service irqbalance show - To check the status
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
service irqbalance start - Enable if needed
```

确保运行 `kvm_stat` 命令以确保计数器不多。

带有 PV 网络接口的 NetScaler VPX

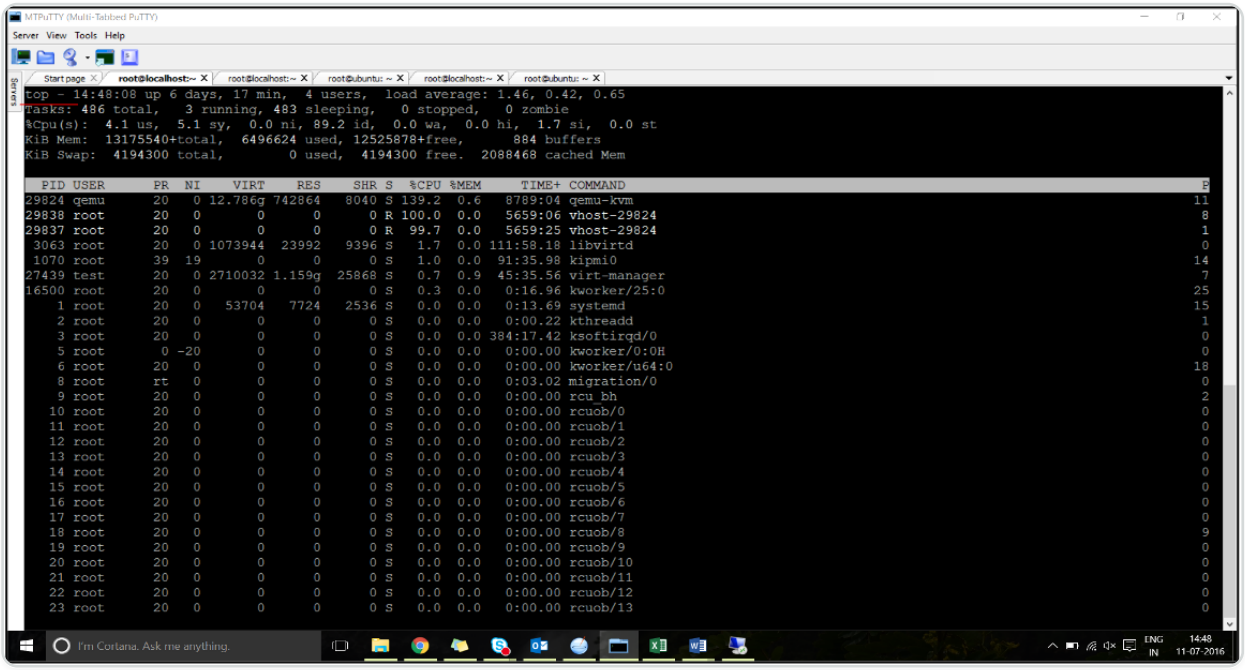
您可以将半虚拟化 (PV)、SR-IOV 和 PCIe 直通网络接口配置为**每个 pNIC 两个 vNIC** 部署。有关详细信息，请参阅 每个 pNIC 两个 vNIC 部署。

为了获得 PV (virtio) 接口的最佳性能，请执行以下步骤：

- 识别 PCIe 插槽/网卡所绑定的 NUMA 域。
- VPX 的内存和 vCPU 必须固定到同一个 NUMA 域。
- Vhost 线程必须绑定到同一 NUMA 域中的 CPU。

将虚拟主机线程绑定到相应的 CPU：

1. 流量启动后，在主机上运行 `top` 命令。



2. 识别虚拟主机进程（命名为 `vhost-<pid-of-qemu>`）的亲和性。
3. 使用以下命令将 vHost 进程绑定到前面识别的 NUMA 域中的物理核心：

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

示例：

```
taskset -pc 12 29838
```

4. 可以使用以下命令识别与 NUMA 域对应的处理器核心：

```
[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'/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        <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/>
```

将 QEMU 进程绑定到相应的物理核心：

1. 识别 QEMU 进程正在运行的物理核心。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 绑定的相同物理核心：

```
taskset –pc 8-11 29824
```

具有 SR-IOV 和 Fortville PCIe 直通网络接口的 NetScaler VPX

为了获得 SR-IOV 和 Fortville PCIe 直通网络接口的最佳性能，请遵循以下步骤：

- 识别 PCIe 插槽/网卡所绑定的 NUMA 域。
- VPX 的内存和 vCPU 必须绑定到同一个 NUMA 域。

适用于 Linux KVM 的 vCPU 和内存绑定 VPX XML 示例文件：

```
    <domain type='kvm'>

        <name>NetScaler-VPX</name>

        <uuid>138f7782-1cd3-484b-8b6d-7604f35b14f4</uuid>

        <memory unit='KiB'>8097152</memory>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        <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 Hypervisors 上的 NetScaler VPX 实例

本节包含有关可配置选项和设置，以及其他有助于您实现 Citrix Hypervisors 上 NetScaler VPX 实例最佳性能的建议。

- Citrix Hypervisors 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Citrix Hypervisors 的性能设置

使用“xl”命令查找网卡的 NUMA 域：

```
xl info -n
```

将 VPX 的 vCPU 绑定到物理核心。

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

检查 vCPU 的绑定。

```
xl vcpu-list
```

为 NetScaler VM 分配超过 8 个 vCPU。

要配置超过 8 个 vCPU，请从 Citrix Hypervisor™ 控制台运行以下命令：

```
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

为了获得 SR-IOV 网络接口的最佳性能，请执行以下步骤：

- 确定 PCIe 插槽或 NIC 所绑定的 NUMA 域。
- 将 VPX 的内存和 vCPU 固定到相同的 NUMA 域。
- 将 Domain-0 vCPU 绑定到剩余的 CPU。

具有半虚拟化接口的 NetScaler VPX

为了获得最佳性能，建议采用每个 pNIC 两个 vNIC 和每个 pNIC 一个 vNIC 的配置，这与其他 PV 环境相同。

为了实现半虚拟化 (netfront) 接口的最佳性能，请执行以下步骤：

- 确定 PCIe 插槽或 NIC 所绑定的 NUMA 域。
- 将 VPX 的内存和 vCPU 固定到相同的 NUMA 域。
- 将 Domain-0 vCPU 绑定到相同 NUMA 域的剩余 CPU。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 将 vNIC 的主机 Rx/Tx 线程固定到 Domain-0 vCPU。

将主机线程固定到 Domain-0 vCPU：

1. 在 Citrix Hypervisor 主机 shell 上使用 `xl list` 命令查找 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** - 分配给 XenCenter 中 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，依此类推。

   xl list 命令的输出(/en-us/vpx/media/xl-list-command.png)
3. 使用以下命令将线程固定到 Domain-0 vCPU：

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

   示例：

   ```
   taskset -pc 1 29189
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持增加 NetScaler VPX 磁盘空间

NetScaler VPX 支持 20 GB 的默认磁盘空间。如果您因各种原因遇到磁盘大小限制，可以使用以下选项来增加 VPX 磁盘空间：

- 动态增加主磁盘大小
- 添加辅助磁盘
- 手动增加主磁盘大小

注意：

增加 NetScaler VPX 磁盘空间的功能适用于本地 VPX 和云部署的 VPX。

在 NetScaler VPX 上动态增加主磁盘大小

从 NetScaler 14.1 版本 build 21.x 开始，管理员可以一次性将 NetScaler VPX 上的主磁盘大小从 20 GB 动态增加到 1 TB。对于后续的每次增加，您可以再次扩展到 1 TB。每次增加主磁盘大小时，请务必关闭虚拟机。这允许系统正确识别新的磁盘大小、更新分区表并保持系统稳定性。要增加磁盘空间，请在相应的云或虚拟机管理程序 UI 中将主磁盘大小至少扩展 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。因此，仅在必要时才增加磁盘大小。

添加辅助磁盘

从 NetScaler 13.1 版本 build 21.x 开始，您可以通过添加辅助磁盘来增加 NetScaler VPX 实例上的磁盘空间。当您连接辅助磁盘时，`/var/crash` 目录会自动挂载到此磁盘上。辅助磁盘用于存储核心文件和日志。核心文件和日志文件的现有目录将继续像以前一样运行。

注意：

在降级 NetScaler 设备之前进行外部备份，以避免数据丢失。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关如何在云上将新的硬盘驱动器 (HDD) 附加到 NetScaler VPX 实例的信息，请参阅以下内容：

- Azure 文档

  注意：

  要在部署在 Azure 上的 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 VM 大小。

- AWS 文档
- GCP 文档

警告：

将新的 HDD 添加到 VPX 后，在以下情况下，一些处理已移动到新 HDD 的文件的脚本可能会失败：

如果您使用“link”shell 命令为已移动到新 HDD 的文件创建硬链接。
将所有此类命令替换为“ln -s”以使用符号链接。此外，相应地修改失败的脚本。

手动增加 NetScaler VPX 上的主磁盘大小

请按照以下步骤使用虚拟机管理程序或云平台手动增加 VPX 主磁盘大小：

1. 关闭虚拟机。
2. 将默认磁盘大小从 20 GB 扩展到更高的值，例如 30 GB 或 40 GB。对于 Azure，将默认磁盘大小从 32 GB 扩展到 64 GB。
3. 启动虚拟机并进入引导提示符。
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。在以下示例中，VM 分区为 da0。
7. 使用 `gpart resize` 命令调整磁盘分区大小。

   示例： 让我们通过运行以下命令，将 da0 MBR 分区调整为包含 10 GB 的可用空间。

   `gpart resize -i 1 da0`

8. 将可用空间合并到最后一个分区。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

示例：

```
gpart resize -i 5 da0s1
```

9. 使用“growfs”命令扩展文件系统以包含新分配的可用空间。

   示例：

   ```
   growfs /dev/da0s1e
   ```

10. 重新启动 VM，并在 shell 提示符下使用“df -h”命令验证增加的磁盘空间。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

您可以在云环境中首次启动 NetScaler 设备时应用 NetScaler VPX 配置。本文档将此阶段称为**预启动**阶段。因此，在某些情况下，例如 ADC 池化许可，特定的 VPX 实例可以在更短的时间内启动。此功能在 Microsoft Azure、Google Cloud Platform 和 AWS 云中可用。

什么是用户数据

在云环境中预置 VPX 实例时，您可以选择将用户数据传递给该实例。用户数据允许您执行常见的自动化配置任务、自定义实例的启动行为，并在实例启动后运行脚本。首次启动时，NetScaler VPX 实例执行以下任务：

- 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

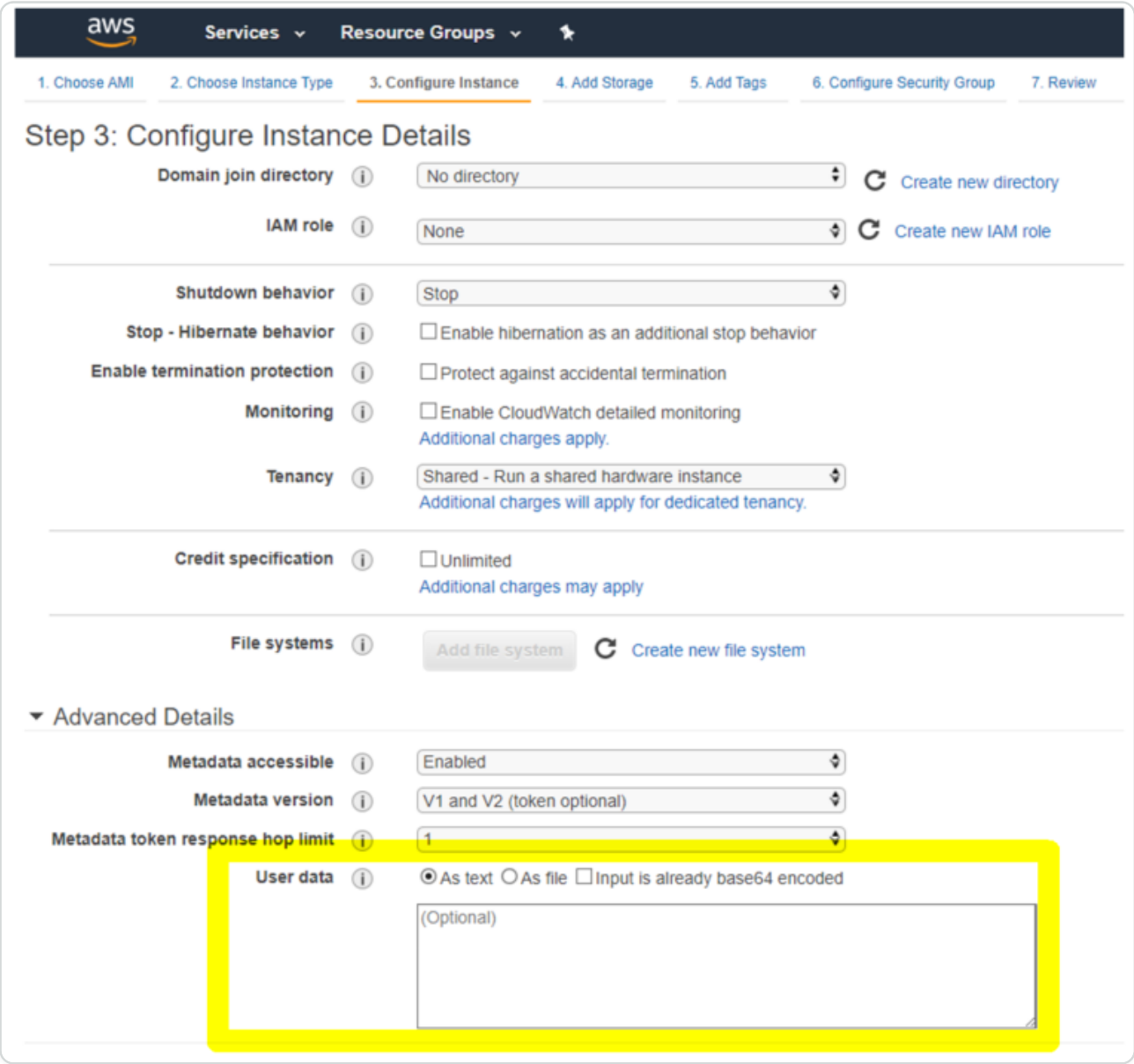
您可以以 XML 格式向云实例提供预启动用户数据。不同的云提供用户数据的接口也不同。

使用 AWS 控制台提供预启动用户数据

使用 AWS 控制台预置 NetScaler VPX 实例时，导航到 **Configure Instance Details > Advanced Details**，并在 **User data** 字段中提供预启动用户数据配置。

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 AWS 文档中的 启动实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

预启动用户数据功能的 AWS IMDSv2 仅限模式从 NetScaler VPX 13.1.48.x 及更高版本开始支持。

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 \
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    --count 1 \

    --subnet-id subnet-08fc749671b2d077c \

    --key-name MyKeyPair \

    --security-group-ids sg-0b0384b66d7d692f9 \

    --user-data file://my_script.txt
```

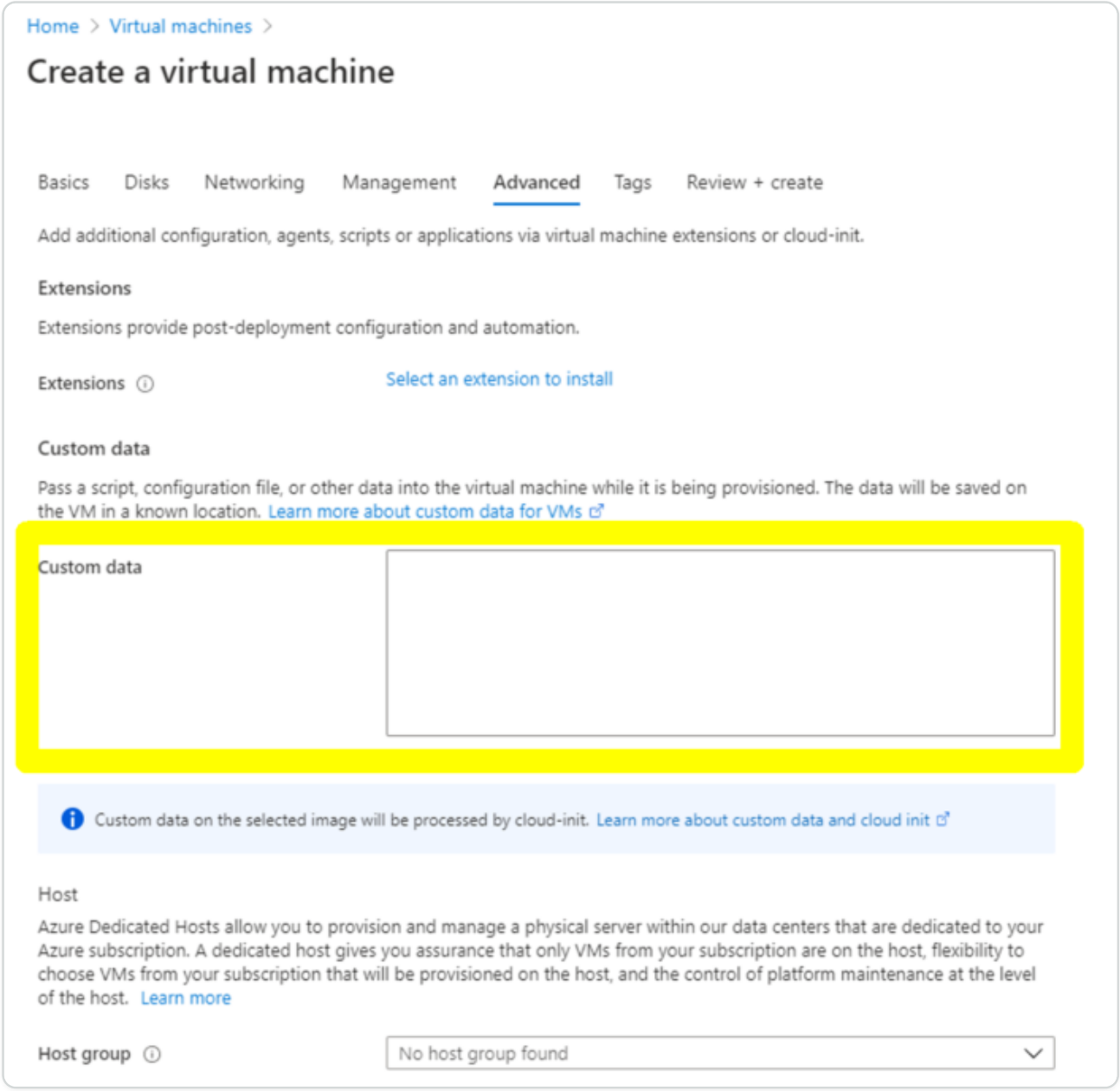
有关更多信息，请参阅 AWS 文档中的 运行实例。

有关更多信息，请参阅 AWS 文档中的 使用实例用户数据

使用 Azure 控制台提供预启动用户数据

使用 Azure 控制台预配 NetScaler VPX 实例时，导航到“**创建虚拟机 > 高级**”选项卡。在“**自定义数据**”字段中，提供预启动用户数据配置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



使用 Azure CLI 提供预启动用户数据

在 Azure CLI 中键入以下命令：

```
az vm create \

  --resource-group myResourceGroup \

  --name MyVm \

  --image debian \

  --custom-data MyCloudInitScript.txt \
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

示例：

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

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

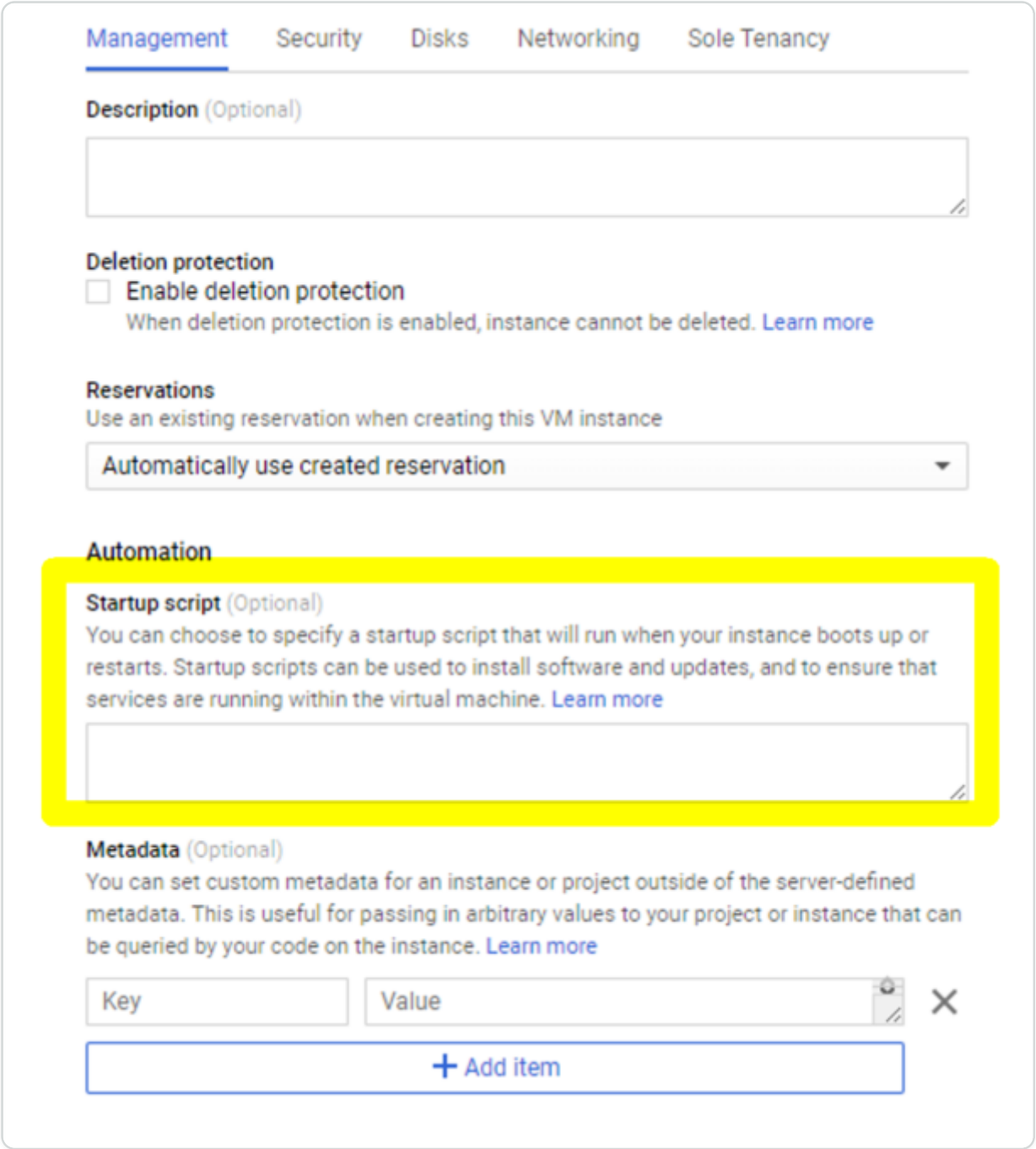
有关更多信息，请参阅 Azure CLI 文档。

使用 GCP 控制台提供预启动用户数据

使用 GCP 控制台预配 NetScaler VPX 实例时，填写实例属性。展开“**管理、安全性、磁盘、网络、独占租用**”。导航到“**管理**”选项卡。在“**自动化**”部分中，在“**启动脚本**”字段中提供预启动用户数据配置。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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
```

metadata-from-file - 从存储在 <LOCAL_FILE_PATH> 的文件中读取值或用户数据。

有关详细信息，请参阅 gcloud CLI 文档

© 1997–2026 Citrix Systems, Inc. All rights reserved.

预启动用户数据格式

预启动用户数据必须以 XML 格式提供给云实例。您在启动期间通过云基础架构提供的 NetScaler 预启动用户数据可包含以下四个部分：

- 由 `<NS-CONFIG>` 标签表示的 NetScaler 配置。
- 由 `<NS-BOOTSTRAP>` 标签表示的自定义引导 NetScaler。
- 由 `<NS-SCRIPTS>` 标签表示的在 NetScaler 中存储用户脚本。
- 由 `<NS-LICENSE-CONFIG>` 标签表示的池化许可配置。

您可以在 ADC 预启动配置中以任何顺序提供上述四个部分。 提供预启动用户数据时，请务必严格遵循以下各节中所示的格式。

注意：

整个预启动用户数据配置必须包含在 `<NS-PRE-BOOT-CONFIG>` 标签中，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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    <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>` 部分必须包含有效的 ADC CLI 命令。CLI 不会验证语法错误或格式。

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>` 部分必须包含有效的 ADC CLI 命令。CLI 不会验证语法错误或格式。

示例：

在以下示例中，`<NS-CONFIG>` 部分包含配置的详细信息。配置了 ID 为“5”的 VLAN 并将其绑定到 SNIP (5.0.0.1)。还配置了负载平衡虚拟服务器 (4.0.0.101)。

```
<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>
```

您可以从此处复制前面屏幕截图中显示的配置：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<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 实例将使用 `<NS-CONFIG>` 部分中应用的配置启动，如以下插图所示。

```
> 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> 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>` 标签提供任何必须存储并在 NetScaler VPX 实例中运行的脚本。

您可以在 `<NS-SCRIPTS>` 标签中包含多个脚本。每个脚本都必须包含在 `<SCRIPT>` 标签中。 每个 `<SCRIPT>` 部分对应一个脚本，并使用以下子标签包含脚本的所有详细信息。

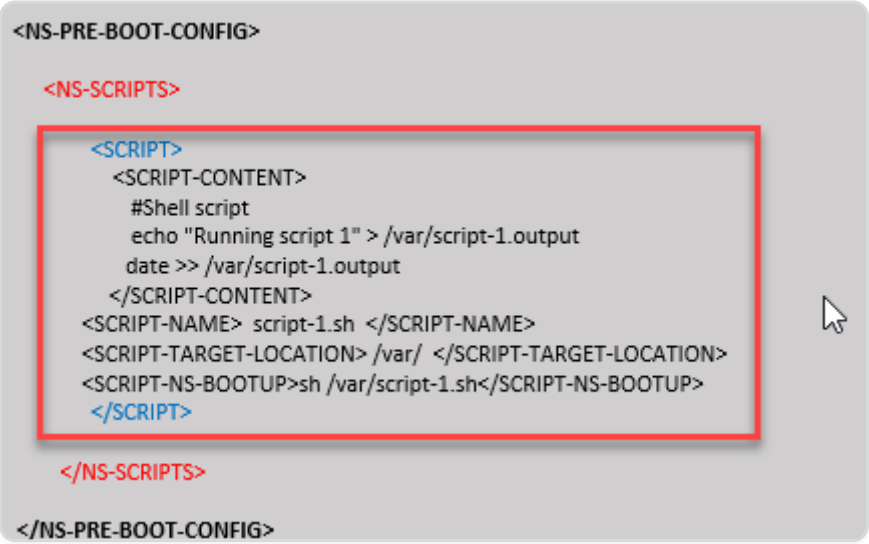
- **`<SCRIPT-NAME>:`** 指示必须存储的脚本文件的名称。
- **`<SCRIPT-CONTENT>:`** 指示必须存储的文件的内容。
- **`<SCRIPT-TARGET-LOCATION>:`** 指示必须存储此文件的指定目标位置。如果未提供目标位置，则文件或脚本默认保存到“/nsconfig”目录中。
- **`<SCRIPT-NS-BOOTUP>:`** 指定用于运行脚本的命令。
  - 如果您使用 `<SCRIPT-NS-BOOTUP>` 部分，则该部分中提供的命令将存储在“/nsconfig/nsafter.sh”中，并且这些命令将在数据包引擎启动后作为“nsafter.sh”执行的一部分运行。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 如果您不使用 `<SCRIPT-NS-BOOTUP>` 部分，则脚本文件将存储在您指定的目标位置。

示例 1：

在此示例中，`<NS-SCRIPTS>` 标签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。脚本将填充指定内容，并在数据包引擎启动后使用“sh /var/script-1.sh”命令运行。



您可以从此处复制前面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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP>

        </SCRIPT>

    </NS-SCRIPTS>

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

在以下快照中，您可以验证“script-1.sh”脚本已保存到“/var/”目录中。“Script-1.sh”脚本已运行，并已正确创建输出文件。

```
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>` 标签包含两个脚本的详细信息。

- 第一个脚本以“script-1.sh”的形式保存在“/var”目录中。该脚本填充了指定内容，并在数据包引擎启动后通过命令“sh /var/script-1.sh”运行。
- 第二个脚本以“file-2.txt”的形式保存在“/var”目录中。此文件填充了指定内容。但它不会运行，因为未提供启动执行命令 `<SCRIPT-NS-BOOTUP>`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<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
cript/file.
      </SCRIPT-CONTENT>
      <SCRIPT-NAME>file-2.txt</SCRIPT-NAME>
      <SCRIPT-TARGET-LOCATION>/var/</SCRIPT-TARGET-LOCATION>
    </SCRIPT>

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

script-1.sh

file-2.txt

您可以从此处复制前面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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            <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>
```

在以下快照中，您可以验证 script-1.sh 和 file-2.txt 已在“/var/”目录中创建。Script-1.sh 已运行，并已相应地创建了输出文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
root@ns# ls /var/
.monit.id                core                    gui                     nsinstall               pubkey
.monit.state             crash                   install                 nslog                   python
.snap                    cron                    krb                     nsproflog               run
AAA                      db                      learnt_data             nssynclog               safenet
app_catalog              dev                     log                     nstemplates             script-1.output
cloudhadaemon            download                mastools                nstmp                   script-1.sh
cloudhadaemon.tgz        empty                   netscaler               nstrace                 tmp
clusterd                 file-2.txt              ns_gui                  opt                     vpn
configdb                 gcfl                    ns_sys_backup           osr_compliance          vpns
root@ns#
root@ns# cat /var/script-1.sh
#Shell script
echo "Running script 1" > /var/script-1.output
date >> /var/script-1.output
root@ns#
root@ns# cat /var/script-1.output
Running script 1
Wed Jan  6 05:08:56 UTC 2021
root@ns#
root@ns#
root@ns# cat /var/file-2.txt
This script has no execution point.
It will just be saved at the target location
NS Consumer module should consume this script/file
root@ns#
root@ns#
```

许可

使用 `<NS-LICENSE-CONFIG>` 标签在启动 VPX 实例时应用 NetScaler 池化许可。在 `<NS-LICENSE-CONFIG>` 部分中使用 `<LICENSE-COMMANDS>` 标签提供池化许可命令。这些命令必须在语法上有效。

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

应用 `<NS-LICENSE-CONFIG>` 后，VPX 会在启动时显示请求的版本，并尝试从许可证服务器签出配置的许可证。

- 如果许可证签出成功，则会将配置的带宽应用于 VPX。
- 如果许可证签出失败，则大约在 10-12 分钟内无法从许可证服务器检索到许可证。结果，系统将重新启动并进入未授权状态。

示例：

在以下示例中，应用 `<NS-LICENSE-CONFIG>` 后，VPX 在启动时会以 Premium 版本启动，并且 VPX 会尝试从许可证服务器 (10.102.38.214) 检出配置的许可证。

```
<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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以从此处复制前面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>
```

如以下插图所示，您可以运行“show license server”命令，并验证许可证服务器 (10.102.38.214) 已添加到 VPX。

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

引导

使用 `<NS-BOOTSTRAP>` 标签提供自定义引导信息。您可以在 `<NS-BOOTSTRAP>` 部分中使用 `<SKIP-DEFAULT-BOOTSTRAP>` 和 `<NEW-BOOTSTRAP-SEQUENCE>` 标签。此部分告知 NetScaler 设备是否避免默认引导。如果避免默认引导，此部分将为您提供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** - 具有特定 NSIP 地址的管理接口。
- **Eth1** - 具有特定 VIP 地址的面向客户端的接口。
- **Eth2** - 具有特定 SNIP 地址的面向服务器的接口。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

自定义引导配置

您可以跳过默认引导序列，为 NetScaler VPX 实例提供新的引导序列。使用 `<NS-BOOTSTRAP>` 标签提供自定义引导信息。例如，您可以更改默认引导，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) 总是以特定顺序提供。

下表显示了 `<SKIP-DEFAULT-BOOTSTRAP>` 和 `<NEW-BOOTSTRAP-SEQUENCE>` 标签允许的不同值所对应的引导行为。

SKIP-DEFAULT-BOOTSTRAP	NEW-BOOTSTRAP-SEQUENCE	启动行为
是	是	跳过默认的启动行为，并运行 `<NS-BOOTSTRAP>` 部分中提供的新自定义启动序列。
是	否	跳过默认的启动行为。运行 `<NS-CONFIG>` 部分中提供的启动命令。

您可以通过以下三种方法自定义启动配置：

- 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>` 部分中提供启动相关命令

方法 1：通过仅指定接口详细信息进行自定义启动

您指定管理接口、面向客户端接口和面向服务器接口，但不指定它们的 IP 地址和子网掩码。IP 地址和子网掩码通过查询云基础设施来填充。

AWS 的自定义引导示例

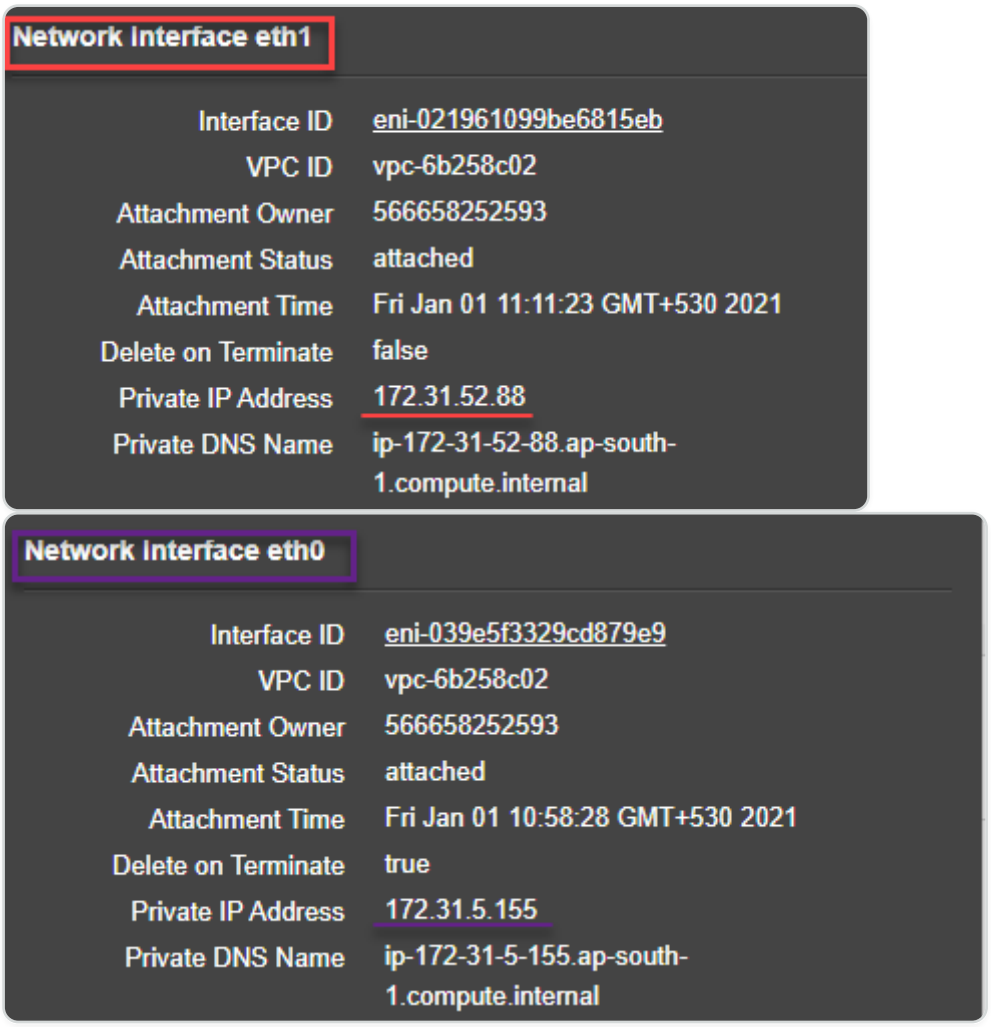
您可以提供自定义引导序列，如以下示例所示。有关详细信息，请参阅如何在云实例中提供预引导用户数据。Eth1 接口被指定为管理接口 (NSIP)，Eth0 接口被指定为客户端接口 (VIP)，Eth2 接口被指定为服务器接口 (SNIP)。`<NS-BOOTSTRAP>` 部分仅包含接口详细信息，不包含 IP 地址和子网掩码的详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

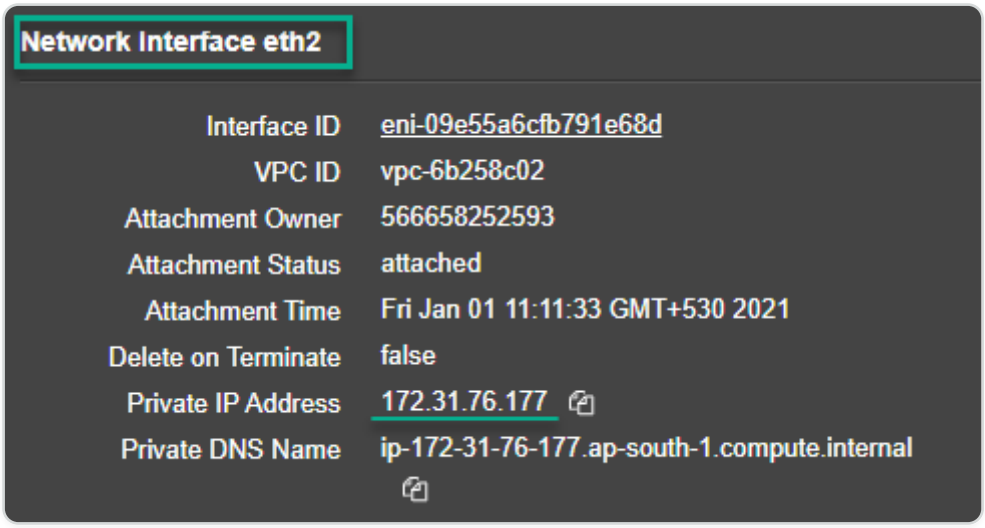
```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <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>
```

VM 实例创建后，您可以在 AWS 门户中按如下方式验证网络接口属性：

1. 导航到 **AWS 门户 > EC2 实例**，然后选择您通过提供自定义引导信息创建的实例。
2. 在**描述**选项卡中，您可以验证每个网络接口的属性，如以下插图所示。



© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以在 **ADC CLI** 中运行 `show nsip` 命令，并验证在 ADC 设备首次启动期间应用于 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
```

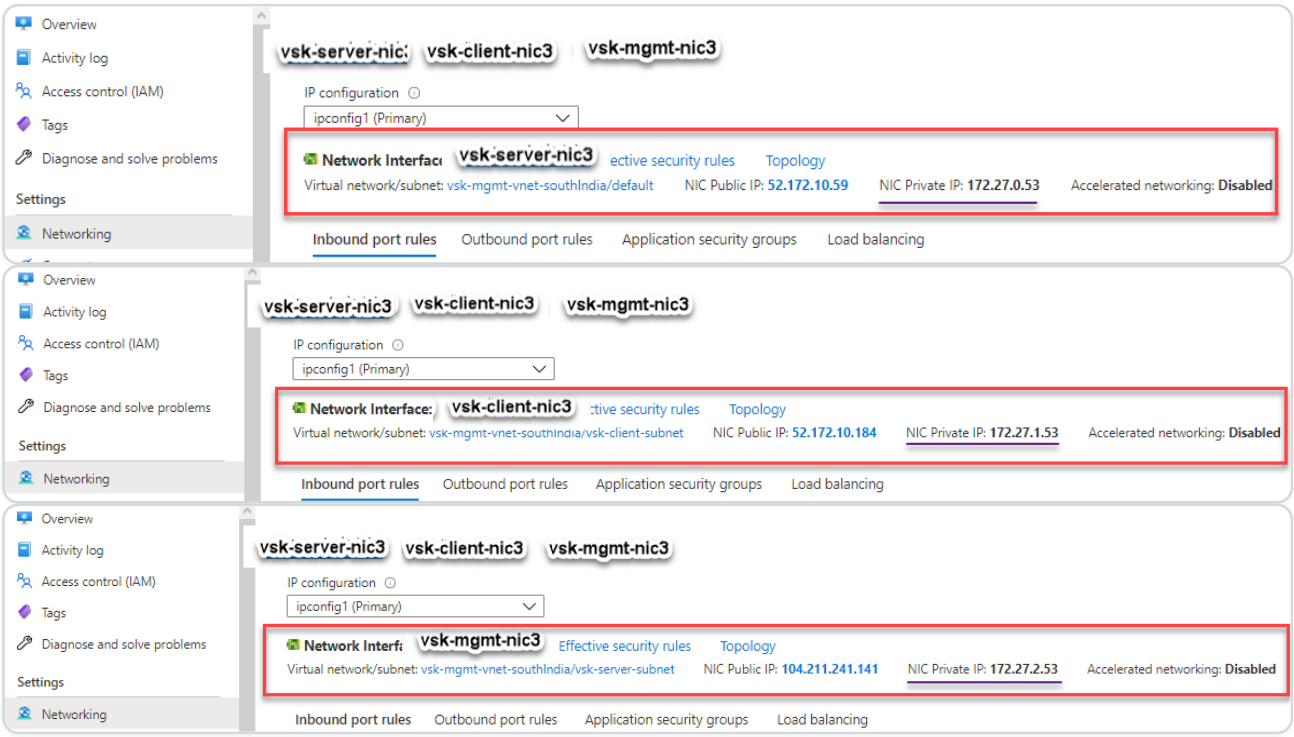
Azure 的自定义引导示例

您可以提供自定义引导序列，如以下示例所示。有关详细信息，请参阅如何在云实例中提供预引导用户数据。Eth2 接口被指定为管理接口 (NSIP)，Eth1 接口被指定为客户端接口 (VIP)，Eth0 接口被指定为服务器接口 (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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<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 实例是使用三个网络接口创建的。导航到 **Azure 门户 > VM 实例 > 网络**，并验证三个 NIC 的网络属性，如以下插图所示。



您可以在 ADC CLI 中运行 "show nsip" 命令，并验证 `<NS-BOOTSTRAP>` 部分中指定的新引导序列是否已应用。您可以运行 "show route" 命令来验证子网掩码。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> 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

您可以按照以下示例提供自定义引导序列。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 接口被指定为管理接口 (NSIP)，Eth0 接口被指定为客户端接口 (VIP)，Eth2 接口被指定为服务器接口 (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。

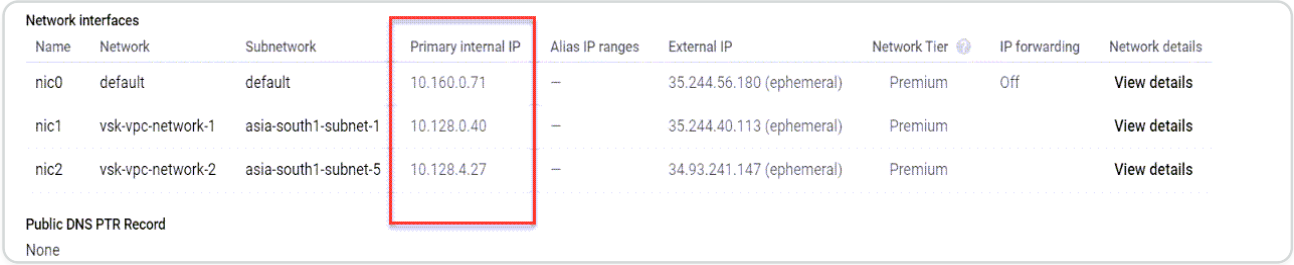
```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <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，您可以按如下方式验证网络接口属性：

1. 选择您通过提供自定义引导信息创建的实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 导航到“网络接口属性”并按如下方式验证 NIC 详细信息：



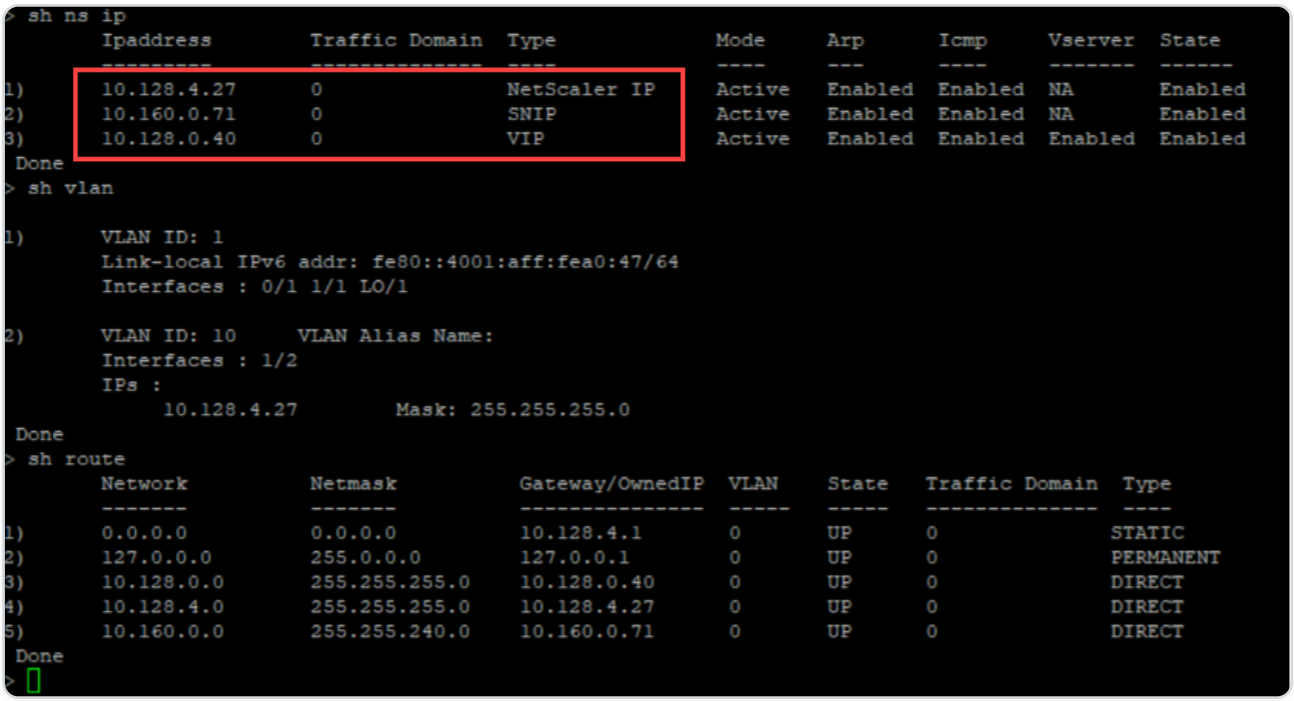
Network interfaces

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，并验证在 ADC 设备首次启动期间应用于 NetScaler VPX 实例的网络接口。



```
> sh ns ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  ------
1)      10.128.4.27      0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.160.0.71      0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.128.0.40      0               VIP             Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::4001:aff:fea0:47/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             10.128.4.27        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.128.4.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      10.128.0.0       255.255.255.0    10.128.0.40      0       UP      0               DIRECT
4)      10.128.4.0       255.255.255.0    10.128.4.27      0       UP      0               DIRECT
5)      10.160.0.0       255.255.240.0    10.160.0.71      0       UP      0               DIRECT
 Done
>
```

方法 2：通过指定接口、IP 地址和子网掩码进行自定义引导

您指定管理、面向客户端和面向服务器的接口及其 IP 地址和子网掩码。

适用于 AWS 的自定义引导示例

在以下示例中，您跳过默认引导并为 NetScaler 设备运行新的引导序列。对于新的引导序列，您指定以下详细信息：

- **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。

AWS 自定义引导方法 2(/en-us/vpx/media/aws-custom-bootstrap-method2.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

AWS 显示 NSIP 方法 2(/en-us/vpx/media/aws-show-nsip-method2.png)

适用于 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了默认引导。您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)

Azure 自定义引导方法 2(/en-us/vpx/media/azure-custom-bootstrap-method2-new.png)

您可以看到 NetScaler VPX 实例是使用三个网络接口创建的。导航到 **Azure 门户 > VM 实例 > 网络**，并验证三个 NIC 的网络属性，如以下插图所示。

Azure 管理界面方法 2(/en-us/vpx/media/azure-mgmt-method2.png)

Azure 客户端界面方法 2(/en-us/vpx/media/azure-client-method2.png)

Azure 服务器界面方法 2(/en-us/vpx/media/azure-server-method2.png)

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

Azure 显示 NSIP 方法 2(/en-us/vpx/media/azure-show-nsip-method2.png)

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，并跳过了默认引导。您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)

GCP 方法 2(/en-us/vpx/media/gcp-method2.png)

在 GCP 门户中使用自定义引导创建 VM 实例后，您可以按如下方式验证网络接口属性：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 选择您通过提供自定义引导信息创建的实例。
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

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

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      10.128.4.31      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      10.160.0.75      0               SNIP             Passive  Enabled  Enabled  NA       Enabled
3)      10.128.0.43      0               VIP              Passive  Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

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

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             10.128.4.31        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.128.4.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      10.128.0.0       255.255.255.0    10.128.0.43      0       UP      0               DIRECT
4)      10.128.4.0       255.255.255.0    10.128.4.31      0       UP      0               DIRECT
5)      10.160.0.0       255.255.255.0    10.160.0.75      0       UP      0               DIRECT
 Done
>
```

方法 3：通过在 `<NS-CONFIG>` 部分提供引导相关命令进行自定义引导

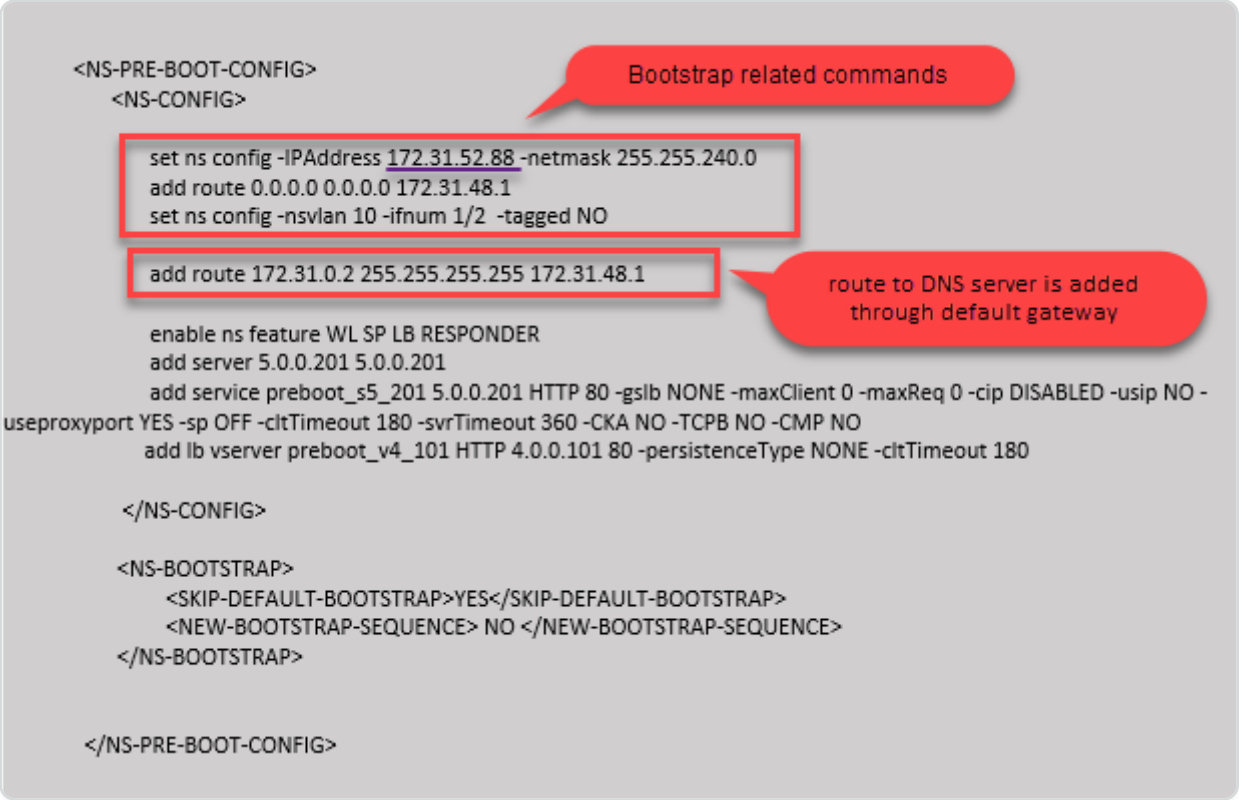
您可以在 `<NS-CONFIG>` 部分提供引导相关命令。在 `<NS-BOOTSTRAP>` 部分中，您必须将 `<NEW-BOOTSTRAP-SEQUENCE>` 指定为“否”，才能运行 `<NS-CONFIG>` 部分中的引导命令。您还必须提供用于分配 NSIP、默认路由和 NSVLAN 的命令。此外，请提供与您使用的云相关的命令。

在提供自定义引导之前，请确保您的云基础架构支持特定的接口配置。

AWS 的自定义引导示例

在此示例中，引导相关命令在 `<NS-CONFIG>` 部分中提供。`<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。您还必须提供用于创建 NSIP、添加默认路由和添加 NSVLAN 的命令。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以从此处复制前面屏幕截图中显示的配置：

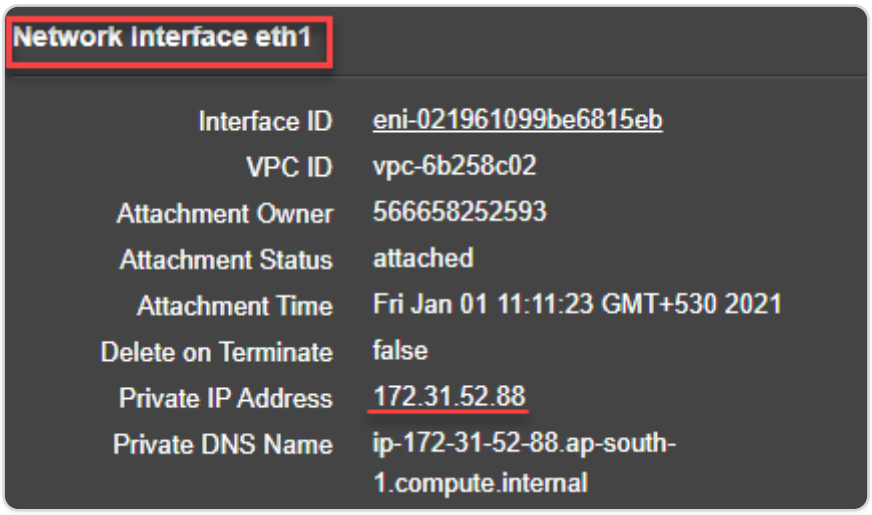
```
<NS-PRE-BOOT-CONFIG>

    <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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        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，在 AWS 门户中，您可以按如下方式验证网络接口属性：

1. 导航到 **AWS Portal > EC2 实例**，然后选择您通过提供自定义引导信息创建的实例。
2. 在“**描述**”选项卡中，您可以验证每个网络接口的属性，如以下插图所示。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Network Interface eth0

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

Network Interface eth2

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

您可以在 **ADC CLI** 中运行 `show nsip` 命令，并验证在 ADC 设备首次启动期间应用于 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
>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure 的自定义引导示例

在此示例中，引导相关命令在 `<NS-CONFIG>` 部分提供。`<NS-BOOTSTRAP>` 部分表示跳过默认引导，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 接口至少必须配置为 SNIP，IMDS 或 DNS 访问才能正常工作。还必须添加通过 Eth0 网关到 IMDS 端点 (169.254.169.254) 和 DNS 端点 (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>

    <NS-BOOTSTRAP>

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

    </NS-BOOTSTRAP>
```

Bootstrap related commands

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



    <NS-CONFIG>
```

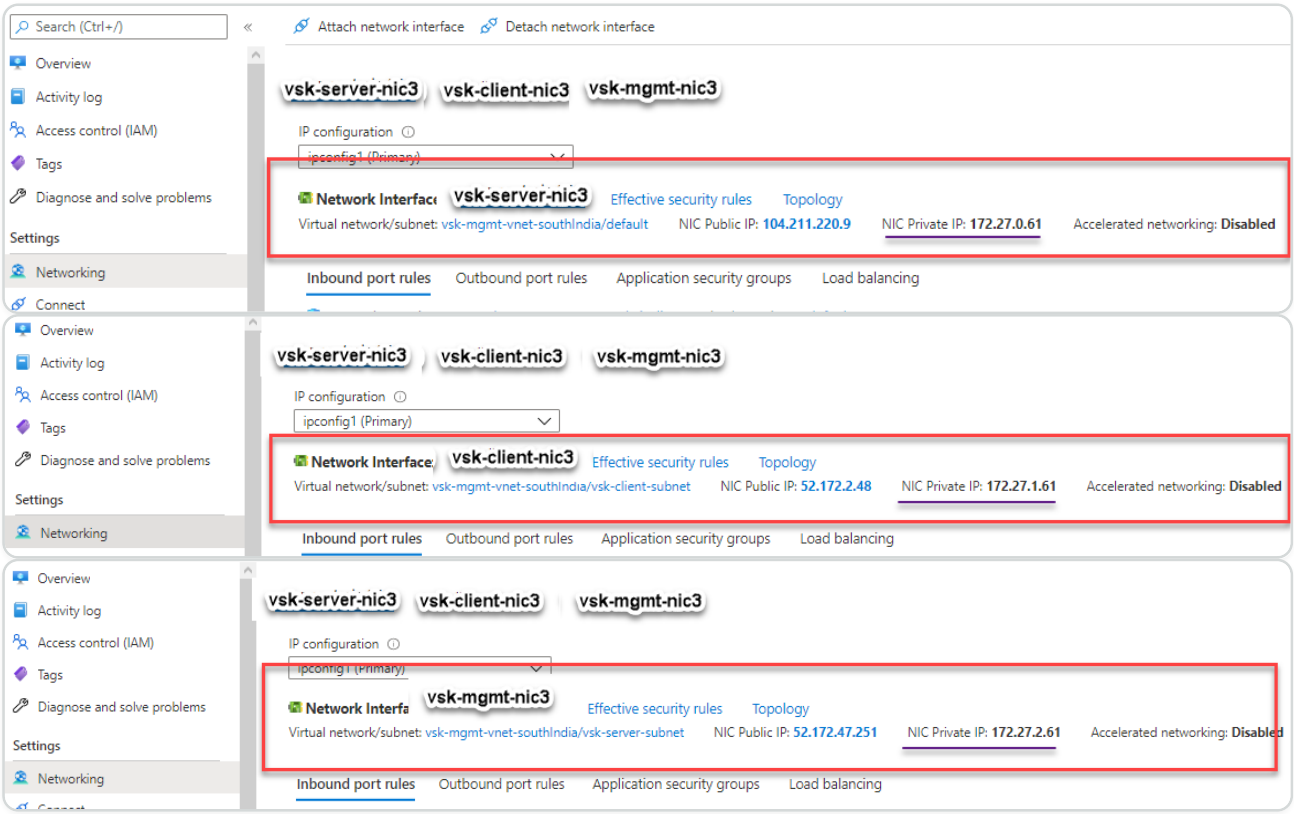
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        set ns config -IPAddress 172.27.2.61 -netmask 255.255.255.0

        add route 0.0.0.0   0.0.0.0   172.27.2.1

        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO

        add ns ip 172.27.0.61   255.255.255.0   -type SNIP

        add route 169.254.169.254 255.255.255.255 172.27.0.1

        add route 168.63.129.16 255.255.255.255 172.27.0.1



        add vlan 5

        bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0

        enable ns feature WL SP LB RESPONDER

        add server 5.0.0.201 5.0.0.201

        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -maxClient
0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout
180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -persistenceType
NONE -cltTimeout 180



    </NS-CONFIG>



    <NS-BOOTSTRAP>



    <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>

    <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    </NS-BOOTSTRAP>


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

您可以看到 NetScaler VPX 实例是使用三个网络接口创建的。导航到 **Azure 门户 > VM 实例 > 网络**，并验证三个 NIC 的网络属性，如以下插图所示。



您可以在 ADC CLI 中运行 `show nsip` 命令，并验证 `<NS-BOOTSTRAP>` 部分中指定的新引导序列是否已应用。您可以运行 "show route" 命令来验证子网掩码。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> 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，引导相关命令在 `<NS-CONFIG>` 部分提供。`<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。

```
<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>
```

bootstrap related commands

您可以从此处复制前面屏幕截图中显示的配置：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

在 GCP 门户中通过自定义引导创建 VM 实例后，您可以按如下方式验证网络接口属性：

1. 选择您通过提供自定义引导信息创建的实例。
2. 导航到“网络接口属性”并验证 NIC 详细信息，如插图所示。

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)

您可以在 **ADC CLI** 中运行 `show nsip` 命令，并验证前面 `<NS-CONFIG>` 部分中提供的配置是否已在 ADC 设备首次启动时应用。

```
> 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 中连接和分离 NIC 的影响

AWS 和 Azure 提供了将网络接口连接到实例以及从实例分离网络接口的选项。连接或分离接口可能会改变接口位置。因此，Citrix 建议您不要从 NetScaler VPX 实例分离接口。如果在配置了自定义引导时分离或连接接口，NetScaler VPX 实例会将新可用接口的主 IP 重新分配为管理接口位置的 NSIP。如果您分离的接口之后没有其他可用接口，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)。如果您从实例中分离 Eth1 接口（这是一个管理接口），ADC 会将下一个可用接口 (Eth2) 配置为管理

© 1997–2026 Citrix Systems, Inc. All rights reserved.

接口。因此，NetScaler VPX 实例仍然可以通过 Eth2 接口的主 IP 访问。如果 Eth2 也不可用，则剩余的接口 (Eth0) 将成为管理接口。因此，对 NetScaler VPX 实例的访问将继续存在。

让我们考虑以下不同的接口分配：Eth0 (SNIP)、Eth1 (VIP) 和 Eth2 (NSIP)。如果您分离 Eth2 (NSIP)，由于 Eth2 之后没有新的接口可用，则第一个接口 (Eth0) 将成为管理接口。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

提高公有云平台上的 SSL-TPS 性能

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，大约 10–12%。

在 AWS 和 GCP 云上，具有 10–16 个 vCPU 的 NetScaler VPX 实例未显示任何性能改进，因为 PE 权重默认情况下是平均分配的。

注意：

在 Azure 云中，PE 权重默认情况下是平均分配的。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 权重平均分配。 当 PE 模式设置为 DEFAULT 时，PE 权重设置为默认值。

注意：

此命令是节点特定的。在高可用性或群集设置中，您必须在每个节点上运行该命令。如果您在 CLIP 上运行该命令，则会出现以下错误： `Operation not permitted on CLIP`

要显示已配置的 PE 模式状态，请运行以下命令：

```
show cpuparam
```

示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> 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，您必须使用自定义脚本创建 `/nsconfig/.cpubound.conf` 文件。有关更多信息，请参阅 在云中首次启动 NetScaler 设备时应用 NetScaler VPX 配置。

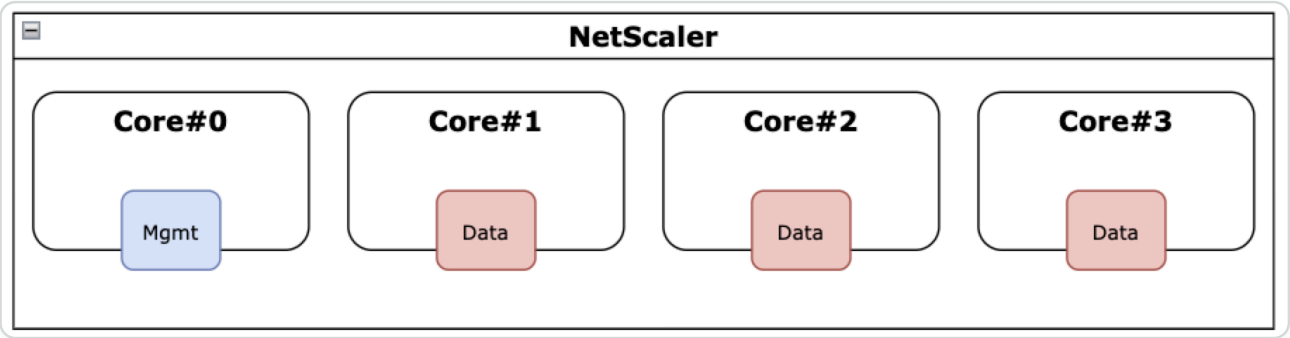
© 1997–2026 Citrix Systems, Inc. All rights reserved.

在公有云上为 NetScaler VPX 配置同步多线程

NetScaler® 使用不同的专用核心来执行其管理和数据平面功能。一个核心通常分配给管理平面功能。其余可用核心分配给数据平面功能。

下图显示了 4 核 NetScaler VPX 的简化示意图。

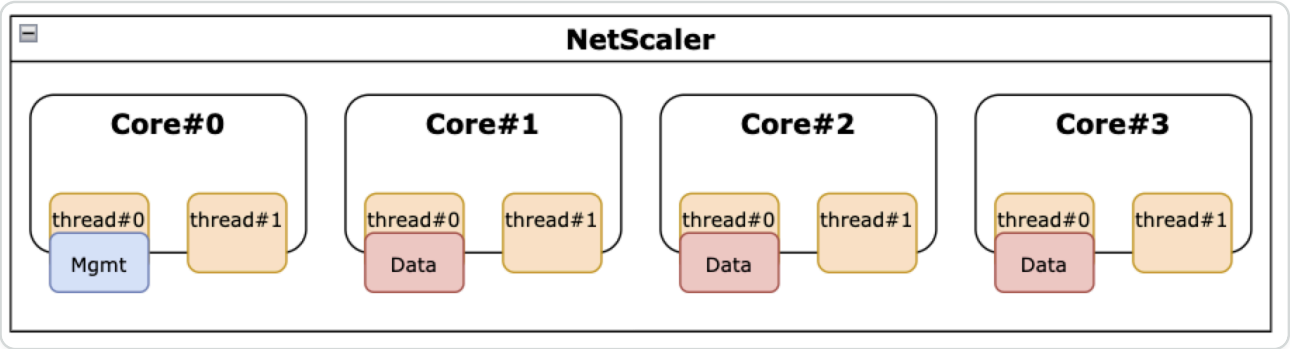
图 1. 4 核系统上的 NetScaler 管理和数据平面工作负载



虽然上图显示了 NetScaler 功能在可用核心上的分布，但这不一定是底层硬件的准确描述。大多数现代 x86 CPU 通过商业上称为 Intel 超线程 (HT) 或 AMD 同步多线程 (SMT) 的功能，为每个物理核心提供两个逻辑核心。

下图显示了在禁用 SMT 的现代 CPU 上运行的 NetScaler VPX。每个 CPU 核心被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，并与其兄弟线程竞争共享资源。

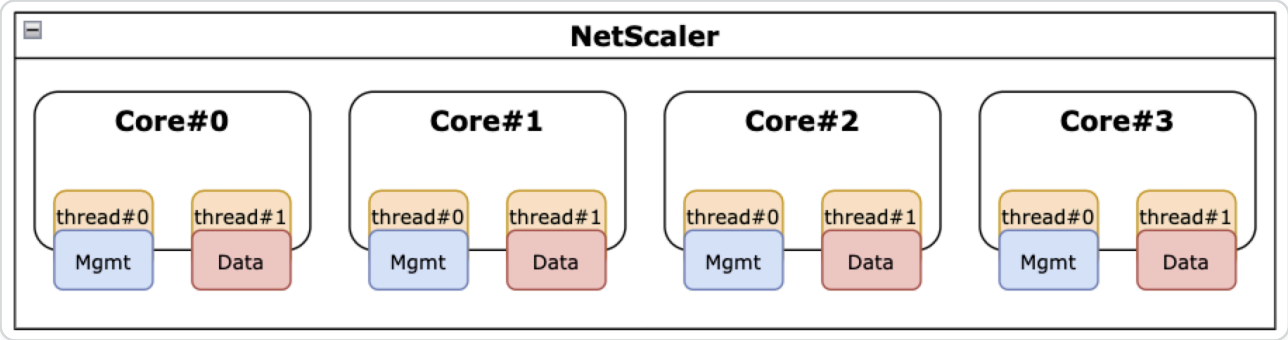
图 2. 在禁用 SMT 的 4 核/8 线程系统上的 NetScaler 管理和数据平面工作负载



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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



启用 SMT 可通过以下方式提高 NetScaler 性能：

- 在所有物理核心上运行数据平面功能。
- 将管理平面功能移动到兄弟线程。
- 引入灵活的资源限制机制，以防止管理平面功能影响数据平面功能的性能。

SMT 支持矩阵

支持 SMT 的 VPX 平台、云实例类型和 NetScaler 版本列在下表中。

VPX 平台	实例类型	NETSCALER VPX 版本
AWS	M5, m5n, c5, c5n	13.1-48.x 及更高版本

注意：

通过启用 SMT 功能，NetScaler VPX 在支持的类型上性能得到提升。

限制

SMT 功能有效地使 NetScaler 设备可用的 vCPU 数量翻倍。必须考虑许可限制，以允许 NetScaler 设备使用它们。

例如，考虑图 3 中所示的 NetScaler VPX。如果使用基于吞吐量的许可，则 SMT 功能需要 10 Gbps 或更高的许可证才能启用 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 配置为签出两倍于 vCPU 数量的许可证才能正常运行。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矩阵表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要启用 SMT 功能，请按照以下步骤操作：

1. 在“/nsconfig”目录下创建名为 `.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. 重启后，NetScaler 会指示该功能既可用又已启用。

```


smt_handling is set to “1”



> shell sysctl -a | grep smt_handling

netscaler.smt_handling_platform: 1

netscaler.smt_handling: 1
```

要禁用 SMT 功能，请按照以下步骤操作：

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

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

  Done
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
reboot



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

Done
```

3. 重启后，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
```

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。

- SMT 功能缺失。

  `sysctl` 命令不返回任何输出。

- SMT 功能不受支持。

  SMT 功能不受支持的原因如下：

  - 您的 NetScaler VPX 版本低于 13.1-48.x 或 14.1-12.x。
  - 您的云不支持 SMT。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 您的 VM 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)
```

- SMT 功能受支持但未启用。

```
> shell sysctl -a | grep smt_handling

netscaler.smt_handling_platform: 1 (available)

netscaler.smt_handling: 0 (not enabled)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在裸机服务器上安装 NetScaler VPX 实例

裸机是一种完全专用的物理服务器，可提供物理隔离，并完全集成到云环境中。它也称为单租户服务器。单租户可让您避免“吵闹的邻居”效应。使用裸机时，您不会遇到“吵闹的邻居”效应，因为您是唯一的用户。

安装了管理程序的裸机服务器为您提供管理套件，用于在该服务器上创建虚拟机。管理程序不本机运行应用程序。它的目的是将您的工作负载虚拟化为独立的虚拟机，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

必须从云供应商处获取裸机服务器，该供应商的裸机服务器必须满足相应管理程序的所有系统要求。

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，您必须首先从云供应商处获取具有足够系统资源的裸机服务器。在该裸机服务器上，必须在部署 NetScaler VPX 实例之前安装和配置任何受支持的管理程序，例如 Linux KVM、VMware ESX、Citrix Hypervisor 或 Microsoft Hyper-V。

有关 NetScaler VPX 实例支持的不同管理程序和功能的列表的更多信息，请参阅 支持矩阵和使用指南。

有关在不同管理程序上安装 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：** 请参阅 在 VMware ESX 上安装 NetScaler VPX 实例。
- **Microsoft Hyper-V：** 请参阅 在 Microsoft Hyper-V 服务器上安装 NetScaler VPX 实例。
- **Linux KVM 平台：** 请参阅 在 Linux-KVM 平台上安装 NetScaler VPX 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

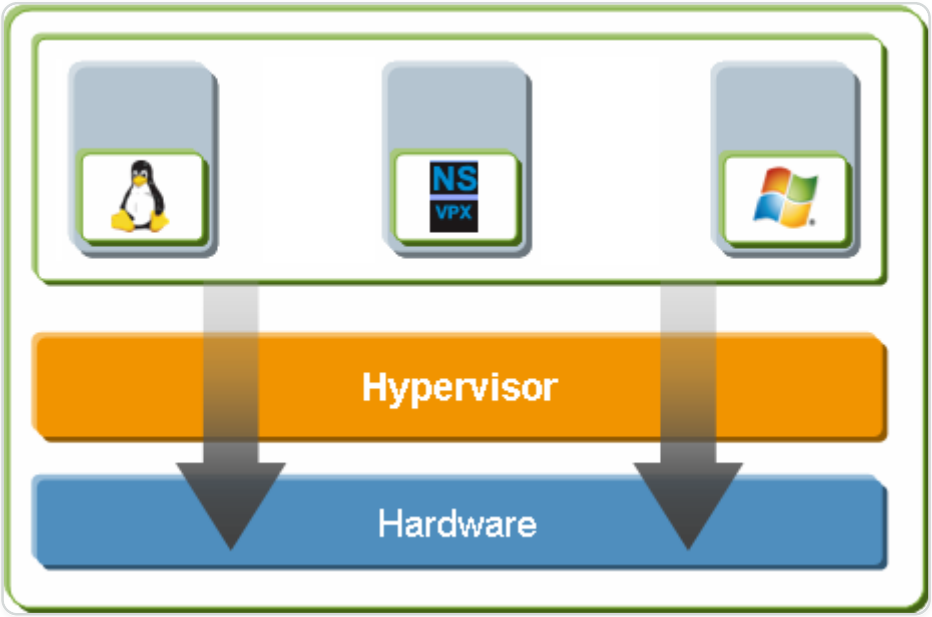
在 Citrix Hypervisor/XenServer 上安装 NetScaler VPX 实例

要在 Citrix Hypervisor/XenServer 上安装 VPX 实例，您必须首先在具有足够系统资源的计算机上安装 Hypervisor。要执行 NetScaler VPX 实例安装，您需要使用 Citrix XenCenter，它必须安装在可以通过网络连接到 Hypervisor 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 Hypervisor 上 NetScaler VPX 实例的裸机解决方案架构。

图。 Citrix Hypervisor/XenServer 上的 NetScaler VPX 实例



在 Hypervisor 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 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。

Hypervisor 硬件要求

下表描述了运行 NetScaler VPX 实例的 Hypervisor 平台的最低硬件要求。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表 1。运行 nCore VPX 实例的 Hypervisor 的最低系统要求

组件	要求
CPU	2 个或更多已启用虚拟化辅助 (Intel-VT) 的 64 位 x86 CPU。要运行 NetScaler VPX 实例，必须在 Hypervisor 主机上启用虚拟化硬件支持。确保未禁用 BIOS 中的虚拟化支持选项。有关更多详细信息，请参阅 BIOS 文档。
RAM	3 GB
磁盘空间	40 GB 磁盘空间的本地连接存储 (PATA、SATA、SCSI)。**注意：** Hypervisor 安装会为 Hypervisor 主机控制域创建 4 GB 分区。剩余空间可用于 NetScaler VPX 实例和其他虚拟机。
NIC	一个 1 Gbps NIC；建议：两个 1 Gbps NIC

有关更多信息，请参阅 XenServer 文档。

下表列出了 Hypervisor 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

对于 NetScaler VPX 实例的生产用途，Citrix 建议将 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 是一个 Windows 客户端应用程序。它不能在与 Hypervisor 主机相同的机器上运行。有关最低系统要求和安装 XenCenter 的更多信息，请参阅以下 Hypervisor 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 Hypervisor 和 XenCenter 后，您可以使用 XenCenter 在 Hypervisor 上安装虚拟设备。您可以安装的虚拟设备数量取决于运行 Hypervisor 的硬件上可用的内存量。

要在 Hypervisor 上使用 XenCenter 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**”对话框中，在主机名文本框中，键入要连接的 Hypervisor 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**”。Hypervisor 名称将显示在导航窗格中，旁边有一个绿色圆圈，表示 Hypervisor 已连接。
5. 在导航窗格中，单击要安装 NetScaler VPX 实例的 Hypervisor 名称。
6. 在“**VM**”菜单上，单击“**导入**”。
7. 在“**导入**”对话框中，在“导入文件名”中，浏览到保存 NetScaler VPX 实例 `.xva` 映像文件的位置。确保选中“导出的 VM”选项，然后单击“**下一步**”。
8. 选择要安装虚拟设备的 Hypervisor，然后单击“**下一步**”。
9. 选择用于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. 您可以根据需要添加、修改或删除虚拟网络接口。完成后，单击“**下一步**”。
11. 单击“**完成**”以完成导入过程。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

要查看导入过程的状态，请单击“**日志**”选项卡。

12. 如果要安装另一个虚拟设备，请重复步骤 5 到 11。

注意：

在VPX实例的初始配置之后，如果您想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。

配置 VPX 实例以使用单根 I/O 虚拟化 (SR-IOV) 网络接口

在 Citrix Hypervisor 上安装并配置 NetScaler VPX 实例后，您可以配置虚拟设备以使用 SR-IOV 网络接口。

支持以下网卡：

- 英特尔 82599 10G
- 英特尔 X710 10G
- 英特尔 XL710 40G

限制

Citrix Hypervisor™ 不支持 SR-IOV 接口上的某些功能。英特尔 82599、英特尔 X710 和英特尔 XL710 网卡的限制列在以下部分中。

英特尔 82599 网卡的限制

英特尔 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
- 巨型帧
- 集群环境中的 IPv6 协议

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

- 不支持 L2 模式切换。
- 不支持管理分区（共享 VLAN 模式）。
- 在集群中，当 XL710 网卡用作数据接口时，不支持巨型帧。
- 当接口断开连接并重新连接时，接口列表会重新排序。
- 不支持接口参数配置，例如速度、双工和自动协商。
- 对于 Intel X710 10G 和 Intel XL710 40G 网卡，接口显示为 40/x 接口。
- VPX 实例上最多只能支持 16 个 Intel X710/XL710 SR-IOV 接口。

注意：

为了使 Intel X710 10G 和 Intel XL710 40G 网卡支持 IPv6，请通过在 Citrix Hypervisor 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
```

示例：

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

Intel 82599 NIC 的先决条件

在 Citrix Hypervisor 主机上，请确保您：

- 将 Intel 82599 NIC (NIC) 添加到主机。
- 通过将以下条目添加到 **/etc/modprobe.d/blacklist.conf** 文件中，将 `ixgbevf` 驱动程序列入黑名单：

  禁用 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)：

  选项 ixgbe max_vfs=*\<number_of_VFs\>*

  其中 *\<number_VFs\>* 是您要创建的 SR-IOV VF 的数量。

- 验证 SR-IOV 在 BIOS 中已启用。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

建议使用 IXGBE 驱动程序版本 3.22.3。

通过使用 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 主机 UUID*\> **fn=assign_free_vf args:uuid**=*<NetScaler 虚拟机 UUID*\> **args:ethdev**=\<*接口名称*\> **args:mac=***<Mac 地址*\>

   其中：

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

   注意：

   在 args:Mac= 参数中指定您要使用的 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，如果您想在链路聚合模式下使用 SR-IOV VF，请确保将 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 从 NetScaler VPX 实例中取消分配

如果您分配了错误的 SR-IOV VF，或者您想修改已分配的 SR-IOV VF，则需要将 SR-IOV VF 从 NetScaler VPX 实例中取消分配并重新分配。

要取消分配分配给 NetScaler VPX 实例的 SR-IOV 网络接口，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 实例并重新启动 NetScaler VPX 实例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

xe host-call-plugin plugin=iovirt **host-uuid**=*<Xen 主机 UUID*\> **fn**=unassign_all **args:uuid**=*<Netscaler 虚拟机 UUID*\>

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以创建网络。

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

示例：

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

2. 确定要配置 SR-IOV 网络的 NIC 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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

示例：

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

要获取有关 SR-IOV 网络参数的更多信息，请运行以下命令：

```
[root@citrix-XS82-TOPO ~]# xe network-sriov-param-list
uuid=1629b44f-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) 并将其附加到目标 VM。

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

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

注意：

VM 的 NIC 索引号必须从 0 开始。

使用以下命令查找 VM UUID：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
[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 实例中移除 Intel X710/XL710 SR-IOV VF，请执行以下步骤：

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>
```

示例：

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

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 虚拟功能 (VF)，您需要禁用已创建的虚拟功能的欺骗检查。

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\> 是接口名称。
- \<VF_id\> 是虚拟功能 ID。

禁用所有已创建的虚拟功能的欺骗检查后，重新启动 NetScaler VPX 实例，并配置链路聚合。有关说明，请参阅配置链路聚合。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要：

将 SR-IOV VF 分配给 NetScaler VPX 实例时，请确保为 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。

重要提示：

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

其他参考

启用 SR-IOV 的网卡

添加 SR-IOV 网络

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 VMware ESX 上安装 NetScaler VPX 实例

在 VMware ESX 上安装 NetScaler VPX 实例之前，请确保 VMware ESX 服务器已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，您需要使用 VMware vSphere 客户端。该客户端或工具必须安装在可以通过网络连接到 VMware ESX 的远程计算机上。

本节包含以下主题：

- 先决条件
- 在 VMware ESX 上安装 NetScaler VPX 实例

重要提示：

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

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 VMware ESX。
- 在满足最低系统要求的管理工作站上安装 VMware Client。
- 下载 NetScaler VPX 设备安装文件。
- 创建一个虚拟交换机并将物理 NIC 连接到该虚拟交换机。
- 添加端口组并连接到虚拟交换机。
- 将端口组连接到虚拟机。
- 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. 运行 NetScaler VPX 实例的 VMware ESX 服务器的最低系统要求

© 1997–2026 Citrix Systems, Inc. All rights reserved.

组件	要求
CPU	2 个或更多已启用虚拟化辅助 (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 BIOS 中的虚拟化支持选项。有关更多信息，请参阅您的 BIOS 文档。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 处理器。
RAM	2 GB VPX。对于关键部署，我们不建议为 VPX 使用 2 GB RAM，因为系统在内存受限的环境中运行。这可能会导致扩展、性能或稳定性相关问题。建议使用 4 GB RAM 或 8 GB RAM。
磁盘空间	比 VMware 设置 ESXi 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（网卡）；建议使用两个 1-Gbps NIC

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

对于 SR-IOV 网络接口或 PCI 直通支持，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 模式支持以下网卡：

- Mellanox ConnectX-4 网卡，从 NetScaler 13.1-42.x 版本开始
- Intel 82599 网卡

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. 运行 NetScaler VPX 实例所需的最低虚拟计算资源

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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，则最多可以安装 10 个虚拟网络接口。
磁盘空间	20 GB

注意：

这不包括管理程序所需的任何磁盘要求。

对于 VPX 虚拟设备的生产用途，必须保留全部内存分配。必须保留至少等于 ESX 一个 CPU 核心速度的 CPU 周期（以 MHz 为单位）。

VMware vSphere 客户端系统要求

VMware vSphere 是一款可在 Windows 和 Linux 操作系统上运行的客户端应用程序。它不能与 VMware ESX 服务器在同一台计算机上运行。下表描述了最低系统要求。

表 3. VMware vSphere 客户端安装的最低系统要求

组件	要求
操作系统	有关 VMware 的详细要求，请在 `<http://kb.vmware.com/>` 搜索“vSphere 兼容性矩阵”PDF 文件。
CPU	750 MHz；建议 1 千兆赫 (GHz) 或更快
RAM	1 GB。建议 2 GB
NIC (网卡)	100 Mbps 或更快的 NIC

OVF Tool 1.0 系统要求

OVF Tool 是一款客户端应用程序，可在 Windows 和 Linux 系统上运行。它不能与 VMware ESX 服务器在同一台计算机上运行。下表描述了最低系统要求。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表 4. OVF 工具安装的最低系统要求

组件	要求
操作系统	有关 VMware 的详细要求，请在 `<http://kb.vmware.com/>` 处搜索“OVF Tool 用户指南”PDF 文件。
CPU	最低 750 MHz，建议 1 GHz 或更快
RAM	最少 1 GB，建议 2 GB
网卡 (NIC)	100 Mbps 或更快的网卡

有关安装 OVF 的信息，请在 `<http://kb.vmware.com/>` 搜索“OVF Tool User Guide”PDF 文件。

下载 NetScaler VPX 安装文件

适用于 VMware ESX 的 NetScaler VPX 实例安装包遵循开放式虚拟机 (OVF) 格式标准。您可以从 Citrix 网站下载文件。您需要一个 Citrix 帐户才能登录。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® 主页导航以下路径：

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

将以下文件复制到与 ESX 服务器位于同一网络的某个工作站。将所有三个文件复制到同一文件夹中。

- NSVPX-ESX-\<版本号\>-\<内部版本号\>-disk1.vmdk（例如，NSVPX-ESX-13.0-71.44_nc_64-disk1.vmdk）
- NSVPX-ESX-\<版本号\>-\<内部版本号\>.ovf（例如，NSVPX-ESX-13.0-71.44_nc_64.ovf）
- NSVPX-ESX-\<版本号\>-\<内部版本号\>.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，您可以使用 VMware vSphere 客户端在 VMware ESX 服务器上安装虚拟设备。您可以安装的虚拟设备数量取决于运行 VMware ESX 的硬件上可用的内存量。

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 在您的工作站上启动 VMware vSphere 客户端。
2. 在“**IP 地址/名称**”文本框中，键入要连接的 VMware ESX 服务器的 IP 地址。
3. 在“**用户名**”和“**密码**”文本框中，键入管理员凭据，然后单击“登录”。
4. 在“**文件**”菜单上，单击“**部署 OVF 模板**”。
5. 在“**部署 OVF 模板**”对话框中，在“**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 模板中显示的网路映射到您在 ESX 主机上配置的网路。单击“**下一步**”开始在 VMware ESX 上安装虚拟设备。安装完成后，将弹出一个窗口通知您安装成功。
7. 现在您可以启动 NetScaler VPX 实例了。在导航窗格中，选择您已安装的 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、子网掩码和网关地址。完成配置后，在控制台中选择“**保存并退出**”选项。
9. 要安装另一个虚拟设备，请重复步骤 6 到步骤 8。

注意：

默认情况下，NetScaler VPX 实例使用 E1000 网络接口。

安装后，您可以使用 vSphere 客户端或 vSphere Web Client 在 VMware ESX 上管理虚拟设备。要在 VMware ESX 上启用 VLAN 标记，请将 vSwitch 上的端口组 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。

请遵循以下使用准则：

- VMware 不支持在配置了 PCI 直通和 SR-IOV 接口的虚拟机上使用 vMotion 功能。
- 支持的接口是 E1000 和 VMXNET3。要在 VPX 实例上使用 vMotion，请确保该实例配置了受支持的接口。
- 有关如何使用 VMware vMotion 迁移实例的更多信息，请参阅 VMware 文档。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置 NetScaler VPX 实例以使用 VMXNET3 网络接口

在 VMware ESX 上安装并配置 NetScaler VPX 实例后，您可以使用 VMware vSphere Web Client 配置虚拟设备以使用 VMXNET3 网络接口。

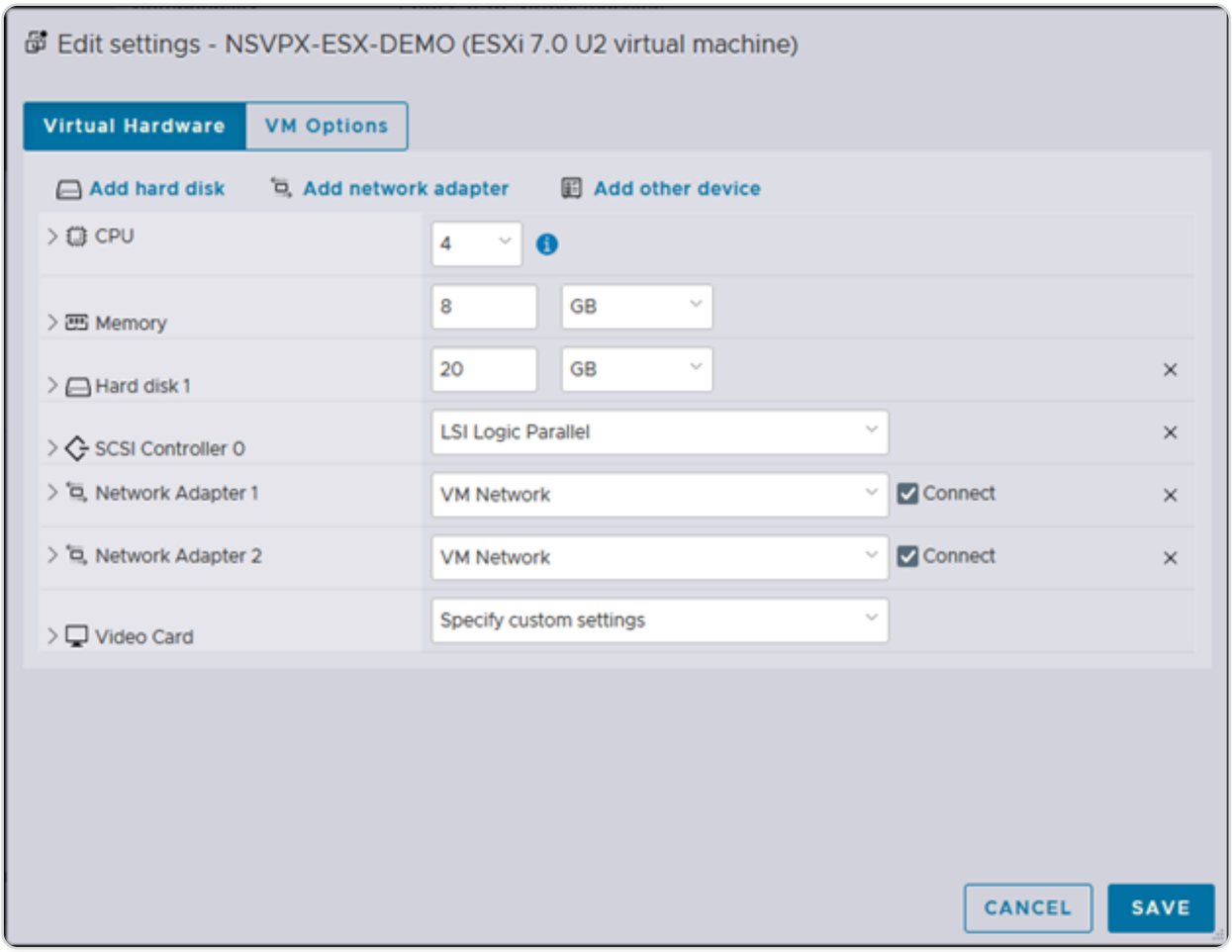
要使用 VMware vSphere Web Client 配置 NetScaler VPX 实例以使用 VMXNET3 网络接口，请执行以下操作：

1. 在 vSphere Web Client 中，选择“主机和群集”。
2. 按照以下步骤将 NetScaler VPX 实例的兼容性设置升级到 ESX：

   a. 关闭 NetScaler VPX 实例。

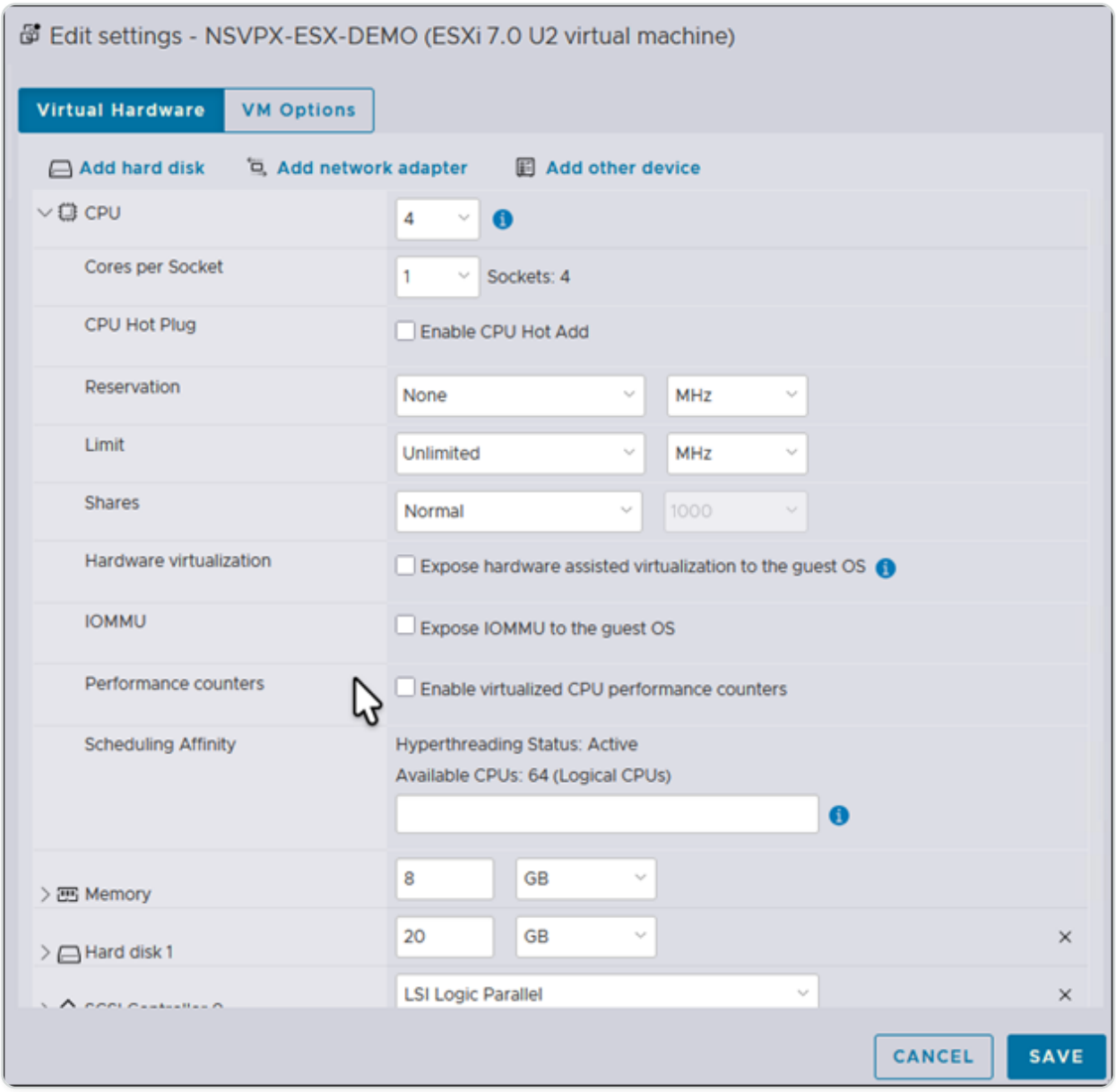
   b. 右键单击 NetScaler VPX 实例，然后选择“兼容性”>“升级 VM 兼容性”。

   c. 在“配置 VM 兼容性”对话框中，从“兼容性”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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 在“CPU”部分中，更新以下内容：

   - CPU 数量
   - 插槽数量
   - 预留
   - 限制
   - 份额

   按如下方式设置值：

   a. 在“CPU”下拉列表中，选择要分配给虚拟设备的 CPU 数量。

   b. 在“每个插槽的内核数”下拉列表中，选择插槽数量。

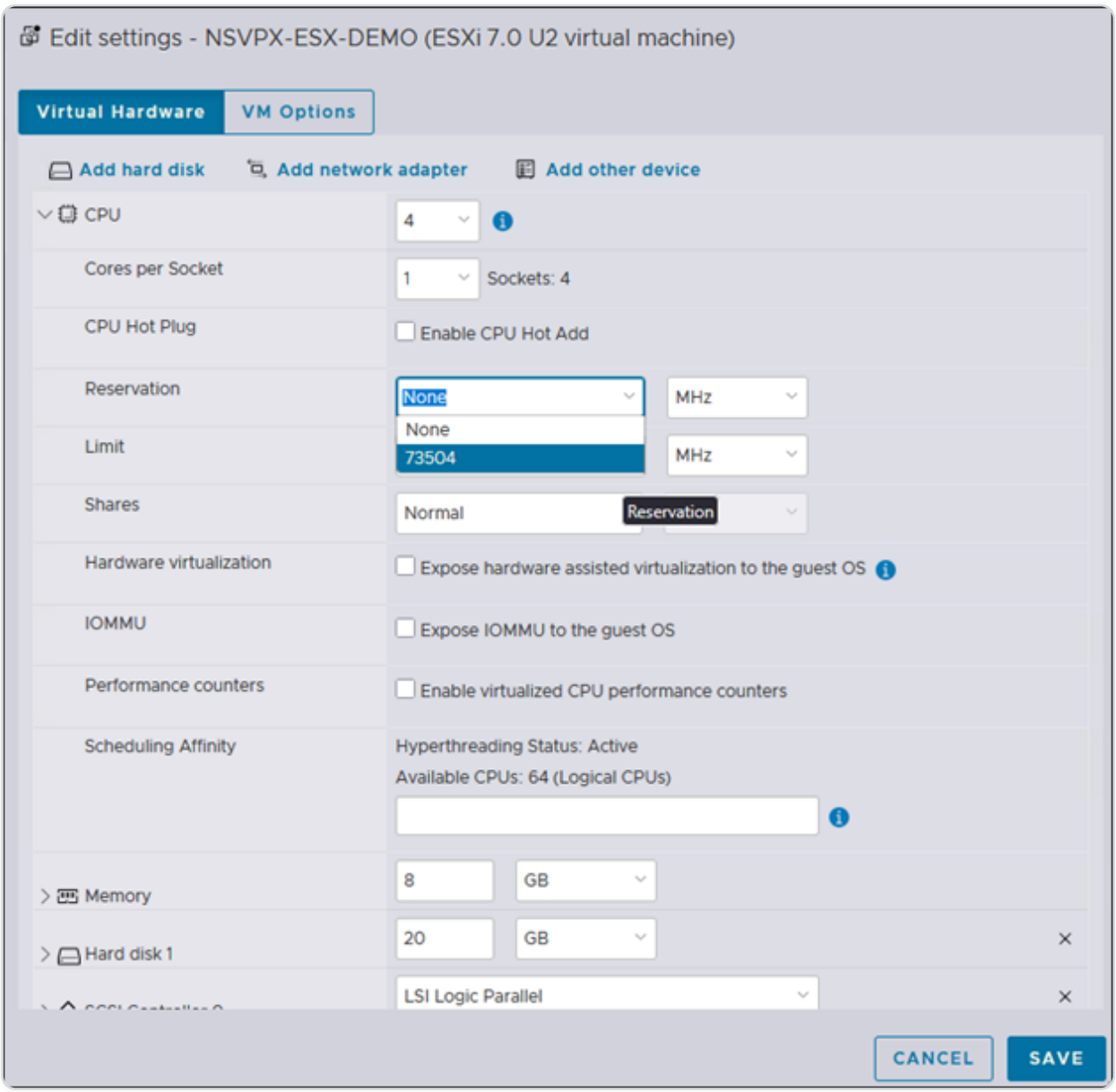
   c. （可选）在“CPU 热插拔”字段中，选中或取消选中“启用 CPU 热添加”复选框。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

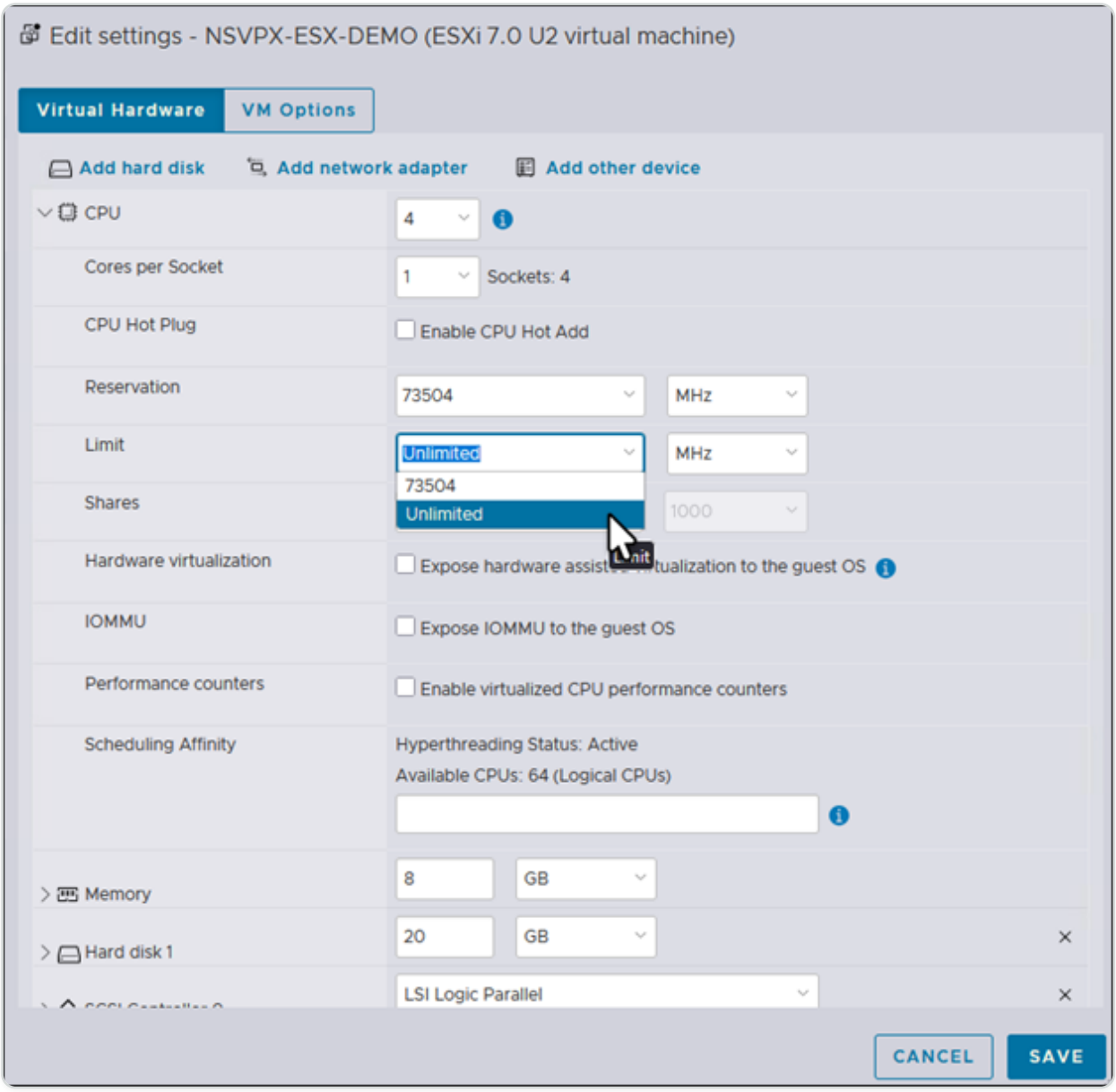
Citrix® 建议接受默认值（已禁用）。

d. 在“预留”下拉列表中，选择显示为最大值的值。



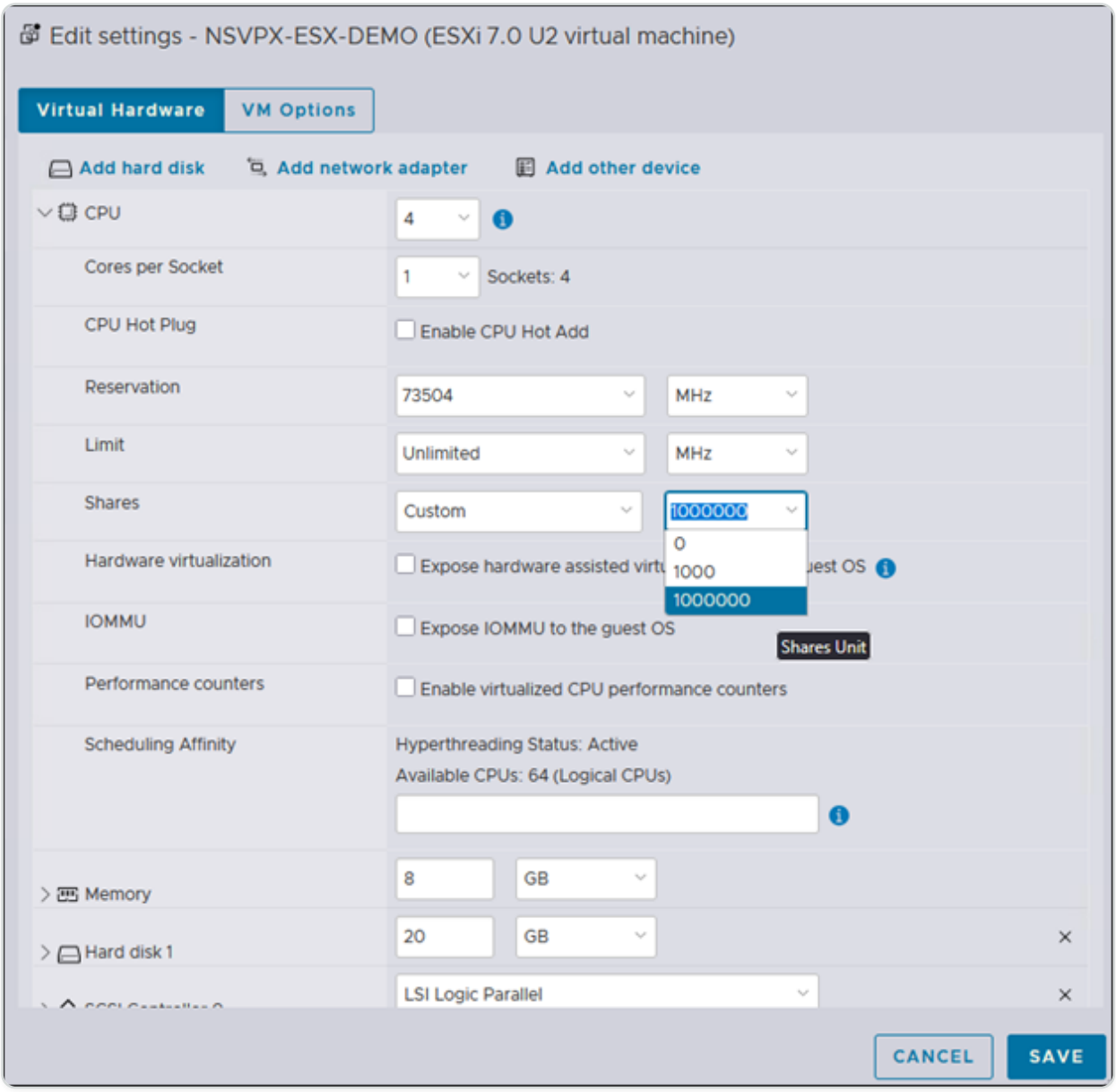
e. 在“限制”下拉列表中，选择显示为最大值的值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



f. 在“份额”下拉列表中，选择“自定义”和显示为最大值的值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 在“内存”部分，更新以下内容：

   - RAM 大小
   - 预留
   - 限制
   - 共享

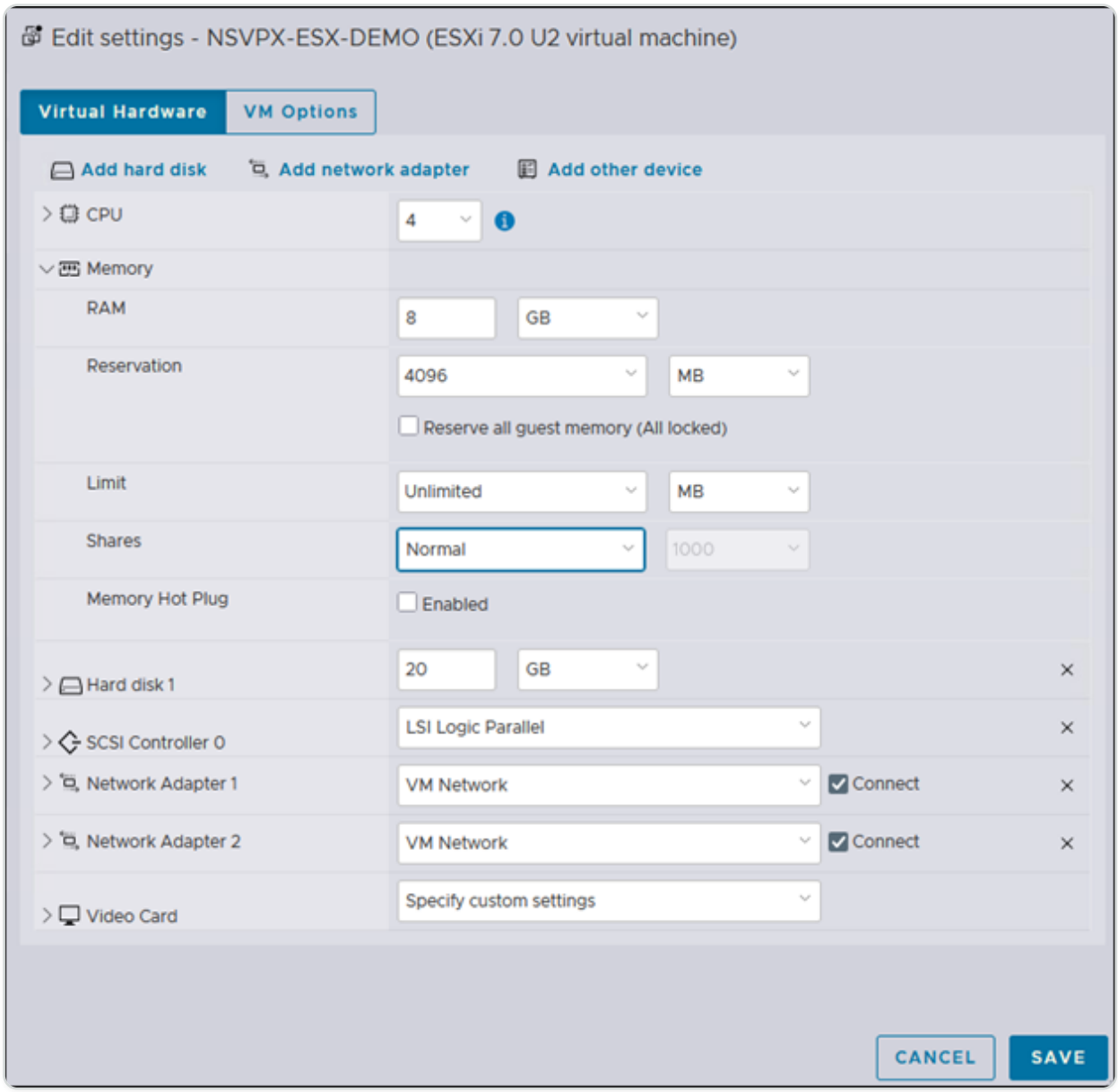
   按如下方式设置值：

   a. 在“**RAM**”下拉列表中，选择 RAM 的大小。它必须是 vCPU 数量 x 2 GB。例如，如果 vCPU 数量为 4，则 RAM 必须为 4 x 2 GB = 8 GB。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

对于 NetScaler VPX 设备的 Advanced 或 Premium 版本，请确保为每个 vCPU 分配 4 GB RAM。例如，如果 vCPU 数量为 4，则 RAM = 4 x 4 GB = 16 GB。

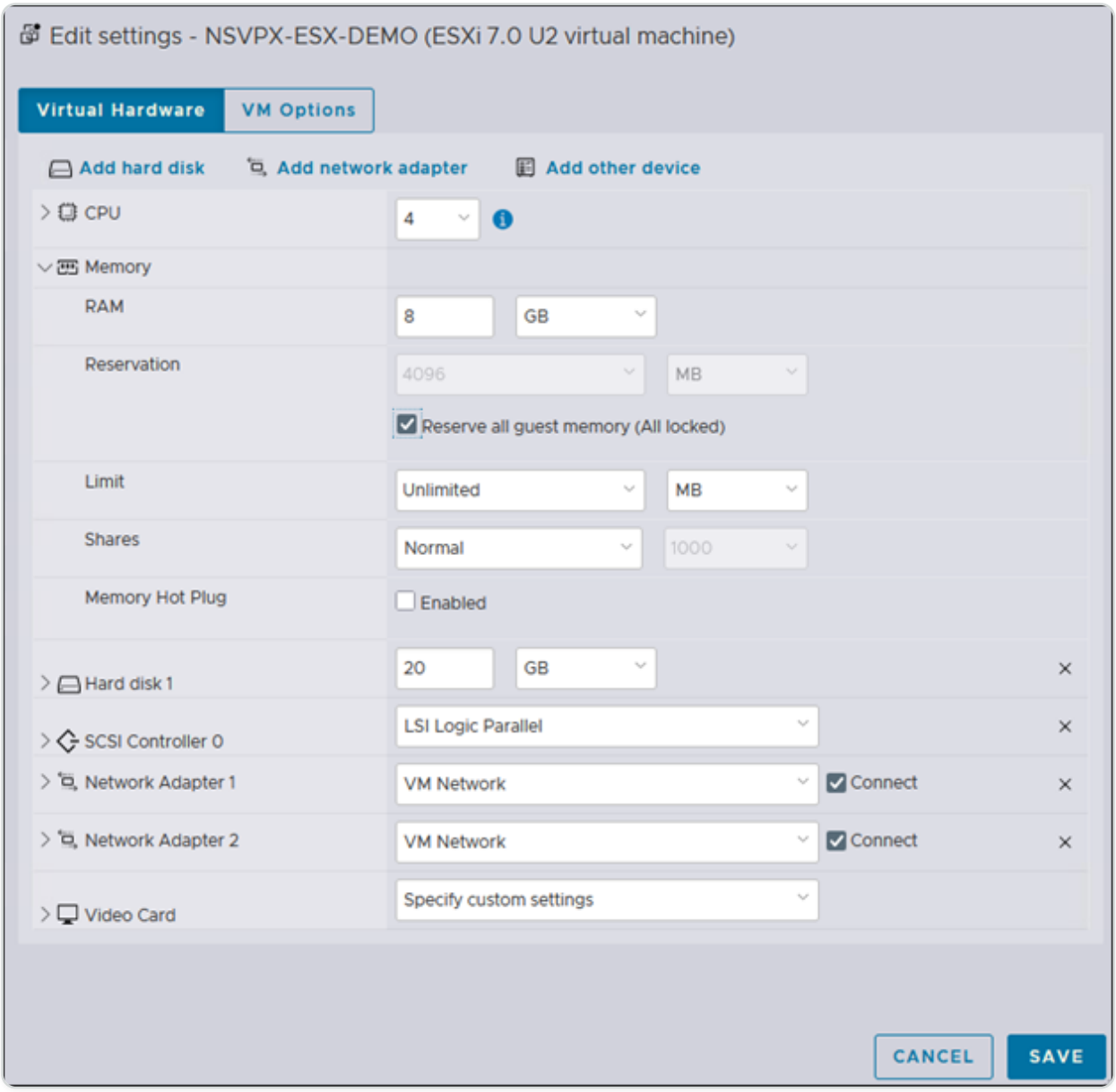


b. 在“预留”下拉列表中，输入内存预留值，然后选中“预留所有客户机内存 (全部锁定)”复选框。内存预留必须是 vCPU 数量 x 2 GB。例如，如果 vCPU 数量为 4，则内存预留必须为 4 x 2 GB = 8 GB。

注意：

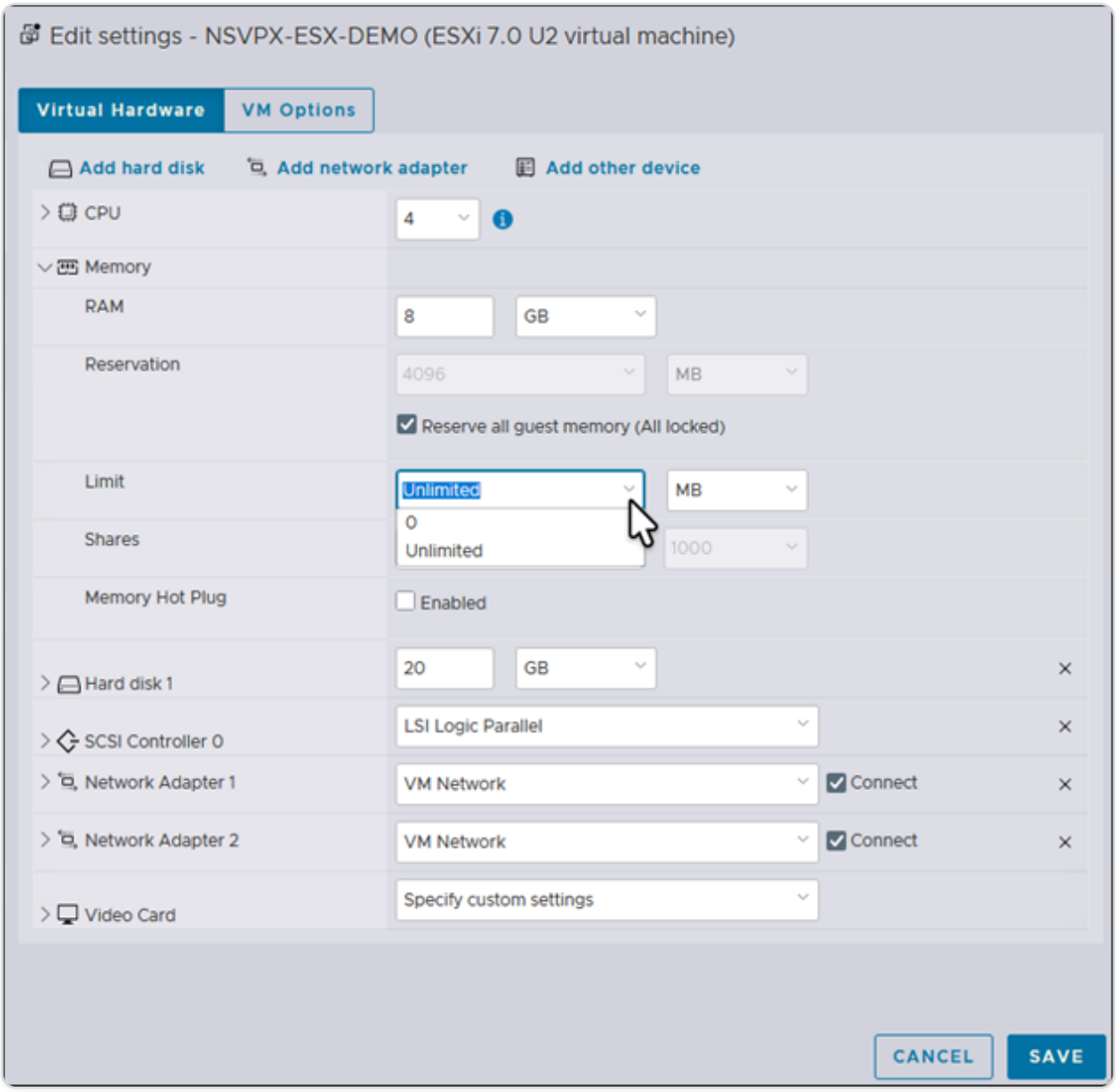
对于 NetScaler VPX 设备的 Advanced 或 Premium 版本，请确保为每个 vCPU 分配 4 GB RAM。例如，如果 vCPU 数量为 4，则 RAM = 4 x 4 GB = 16 GB。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



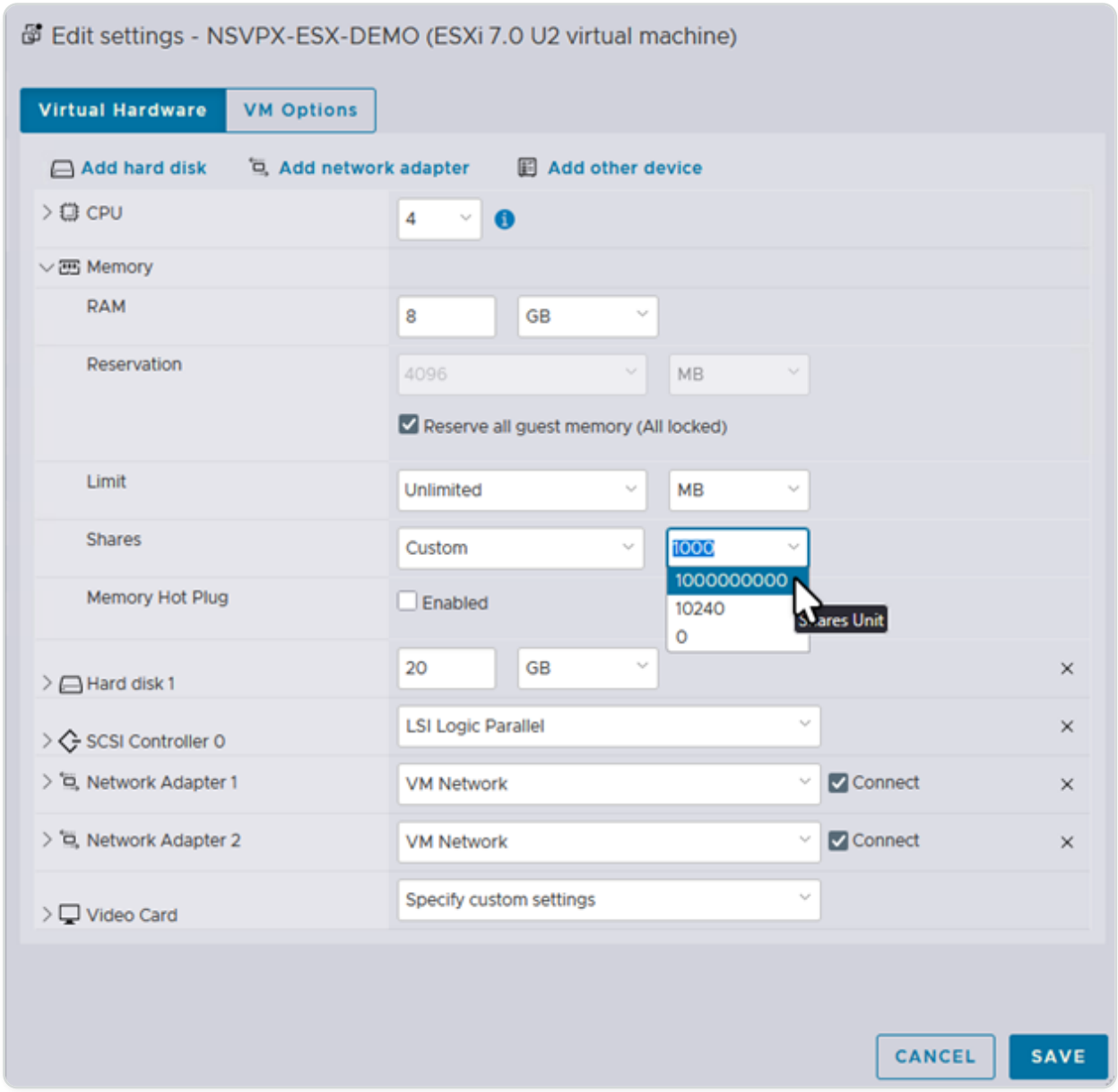
c. 在“限制”下拉列表中，选择显示的最大值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



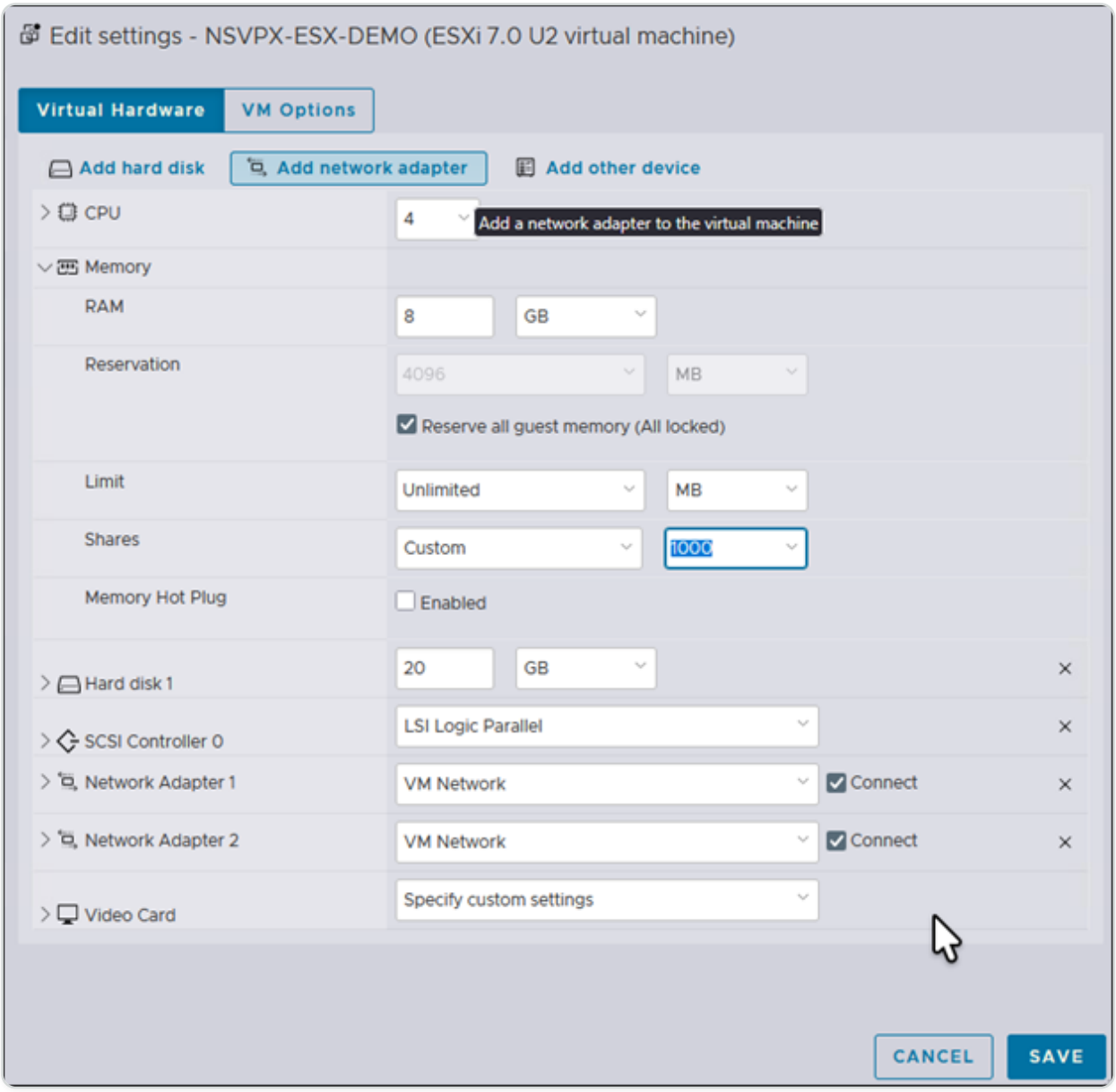
d. 在“共享”下拉列表中，选择“自定义”和显示为最大值的值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. 添加 VMXNET3 网络接口。从“新建设备”下拉列表中，选择“网络”并单击“添加”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



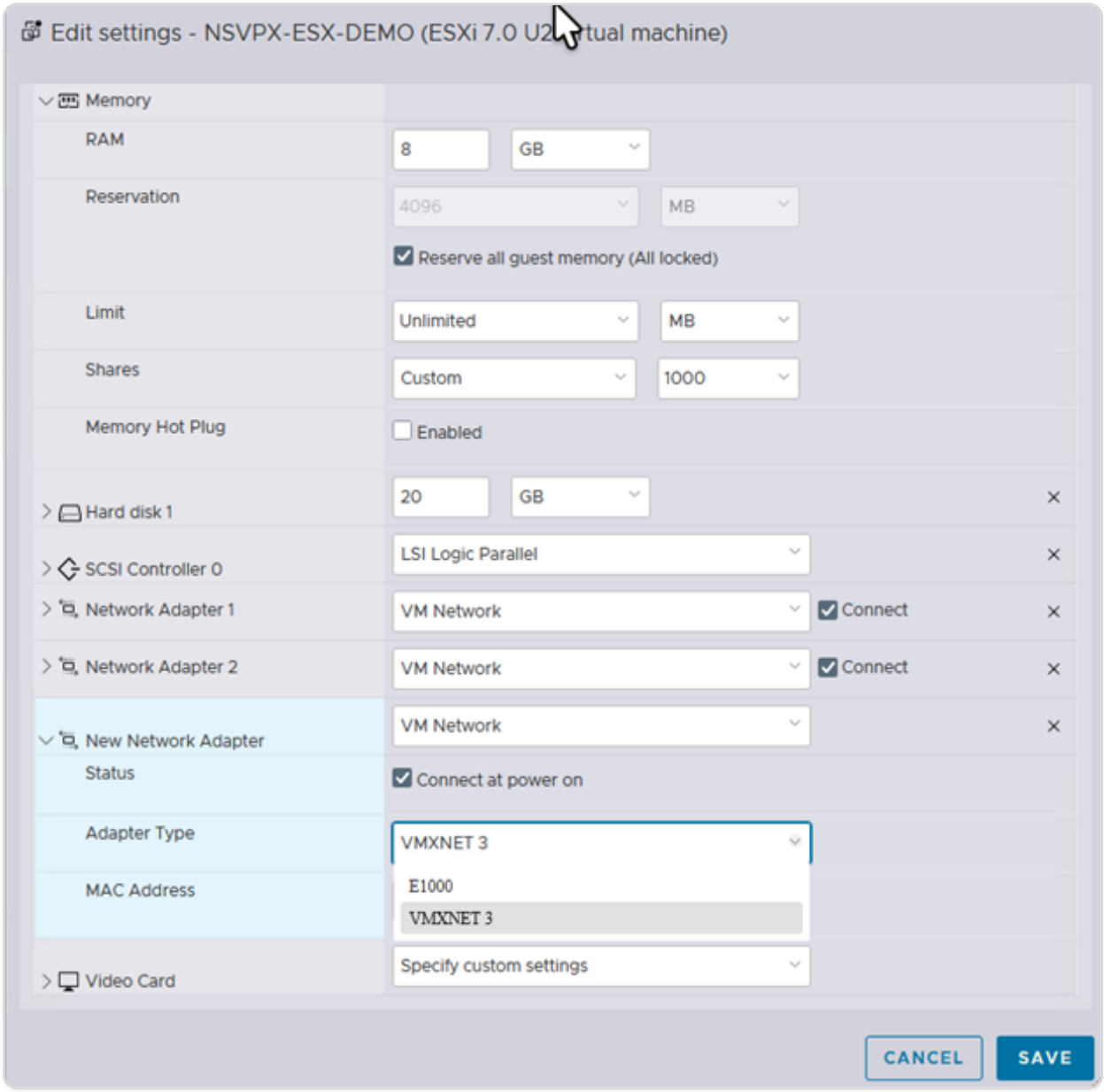
8. 在“新建网络”部分中，从下拉列表中选择网络接口，然后执行以下操作：

   a. 在“适配器类型”下拉列表中，选择 VMXNET3。

重要提示：

默认的 E1000 网络接口和 VMXNET3 不能共存，请确保删除 E1000 网络接口并使用 VMXNET3 (0/1) 作为管理接口。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. 单击“**确定**”。
10. 启动 NetScaler VPX 实例。
11. NetScaler VPX 实例启动后，您可以使用以下命令验证配置：

    显示接口摘要

输出必须显示您配置的所有接口：

```
> show interface summary

---------------------------------------------------------------------------
------

      Interface  MTU        MAC                  Suffix
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

注意：

在添加 VMXNET3 接口并重新启动 NetScaler VPX 设备后，VMware ESX 管理程序可能会更改 NIC 呈现给 VPX 设备的顺序。因此，网卡 1 可能不会始终保持为 0/1，导致与 VPX 设备的管理连接丢失。为避免此问题，请相应地更改网卡的虚拟网络。

这是 VMware ESX 管理程序的限制。

配置 NetScaler VPX 实例以使用 SR-IOV 网络接口

在 VMware ESX 上安装并配置 NetScaler VPX 实例后，您可以使用 VMware vSphere Web 客户端配置虚拟设备以使用单根 I/O 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 上使用 Intel 82599 10G 网卡 的 SR-IOV 接口不支持以下功能：
  - 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - 巨型帧
  - IPv6

- 在 KVM VPX 上使用 Intel 82599 10G 网卡 的 SR-IOV 接口不支持以下功能：
  - 静态链路聚合和 LACP
  - L2 模式切换
  - 集群
  - 管理分区 \[共享 VLAN 模式\]
  - 高可用性
  - 巨型帧
  - IPv6
  - 不支持通过 `ip link` 命令在管理程序上为 SR-IOV VF 接口配置 VLAN

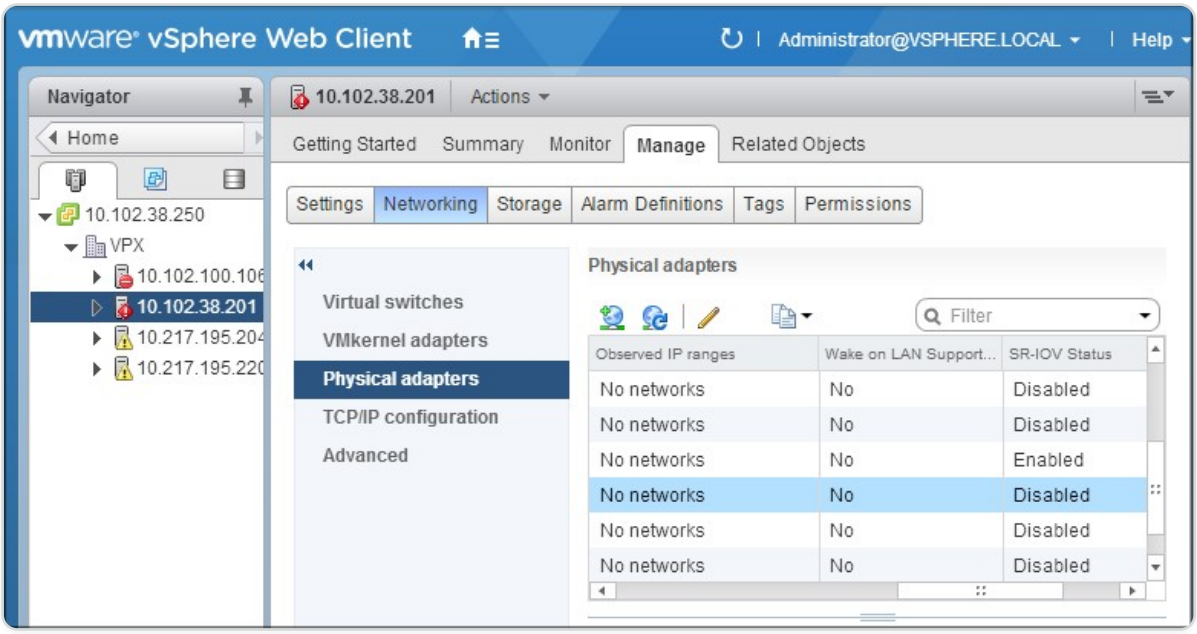
先决条件

- 确保将以下任一网卡添加到 ESX 主机：
  - 建议使用 Intel 82599 网卡，IXGBE 驱动程序版本 3.7.13.7.14iov 或更高版本。
  - Mellanox ConnectX-4 网卡
- 在主机物理适配器上启用 SR-IOV。

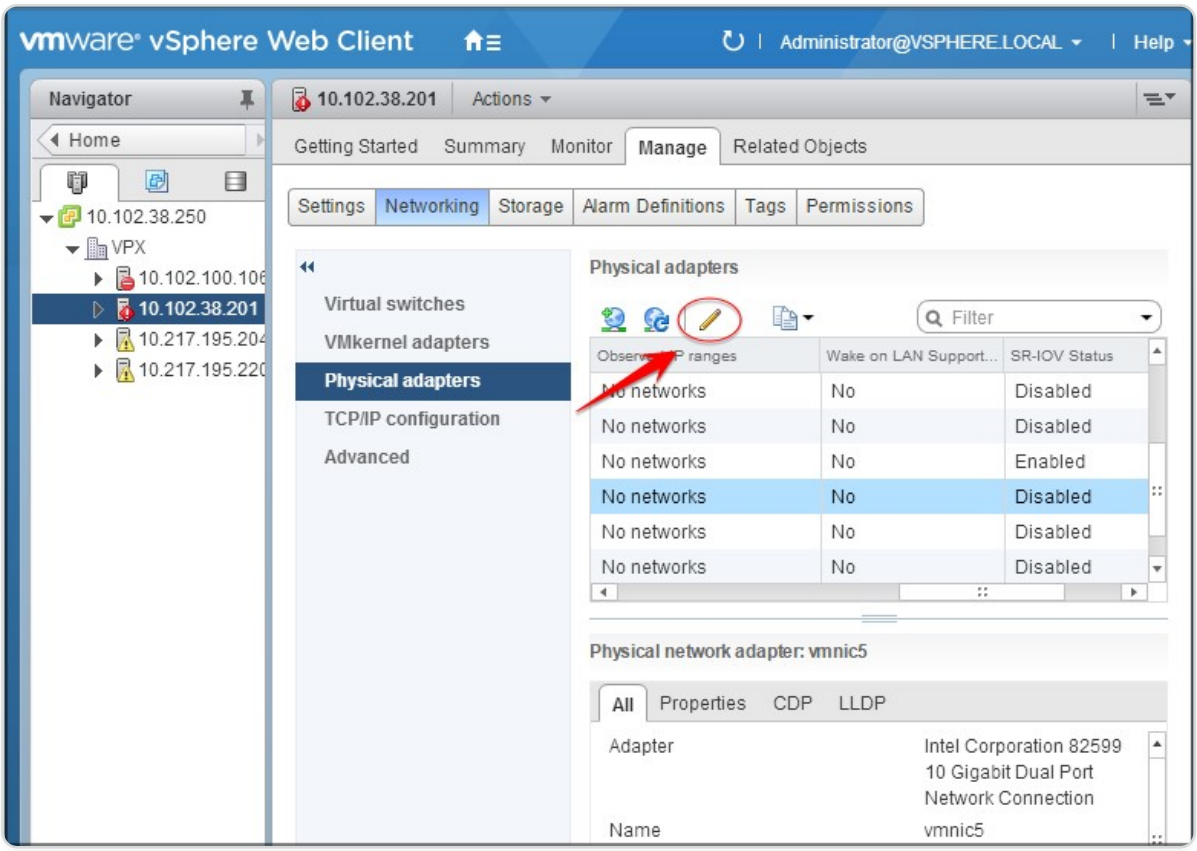
  按照以下步骤在主机物理适配器上启用 SR-IOV：

  a. 在 vSphere Web Client 中，导航到主机。
  b. 在 **管理 > 网络** 选项卡上，选择 **物理适配器**。SR-IOV 状态字段显示物理适配器是否支持 SR-IOV。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

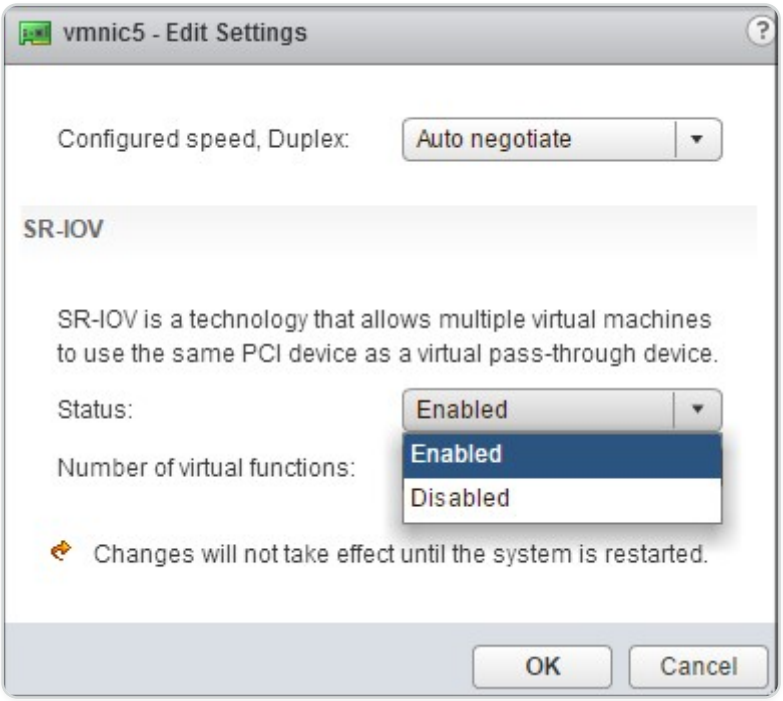


c. 选择物理适配器，然后单击铅笔图标打开“**编辑设置**”对话框。

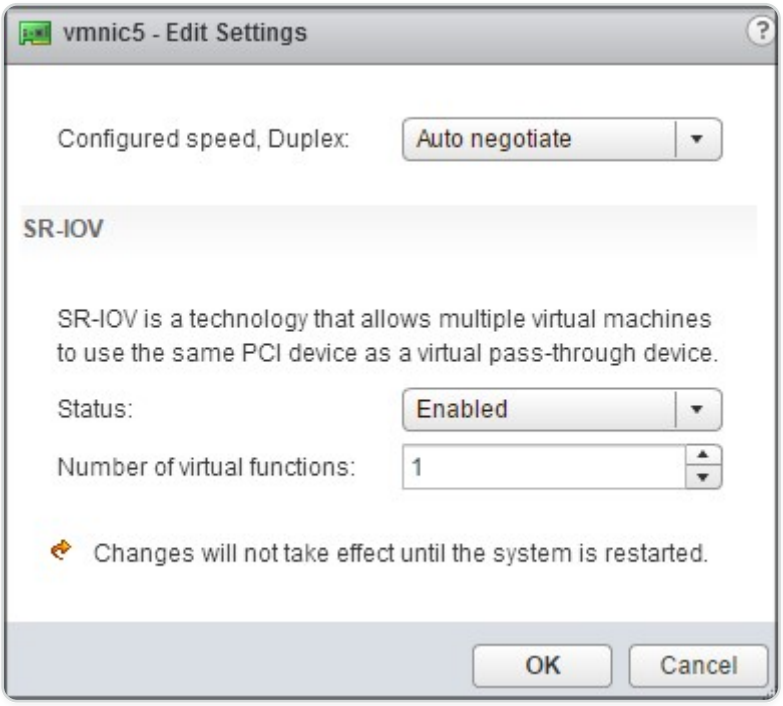


d. 在 SR-IOV 下，从“**状态**”下拉列表中选择“**已启用**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



e. 在“**虚拟功能数量**”字段中，输入您要为适配器配置的虚拟功能的数量。



f. 单击“**确定**”。

g. 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 已验证 SR-IOV 配置仅在 DVS 和 `Portgroups` 上。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

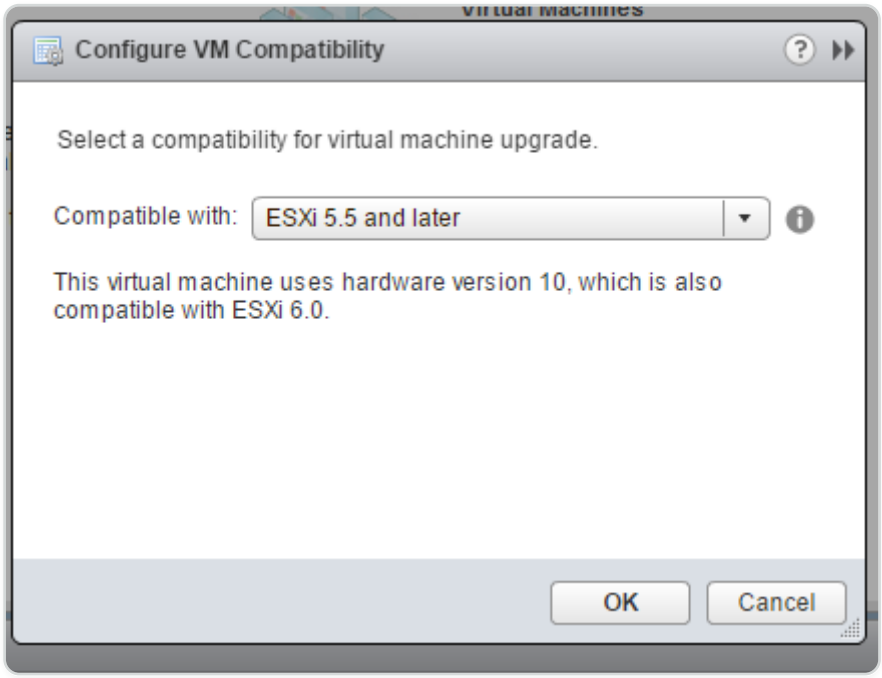
要通过使用 VMware vSphere Web Client 配置 NetScaler VPX 实例以使用 SR-IOV 网络接口：

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。

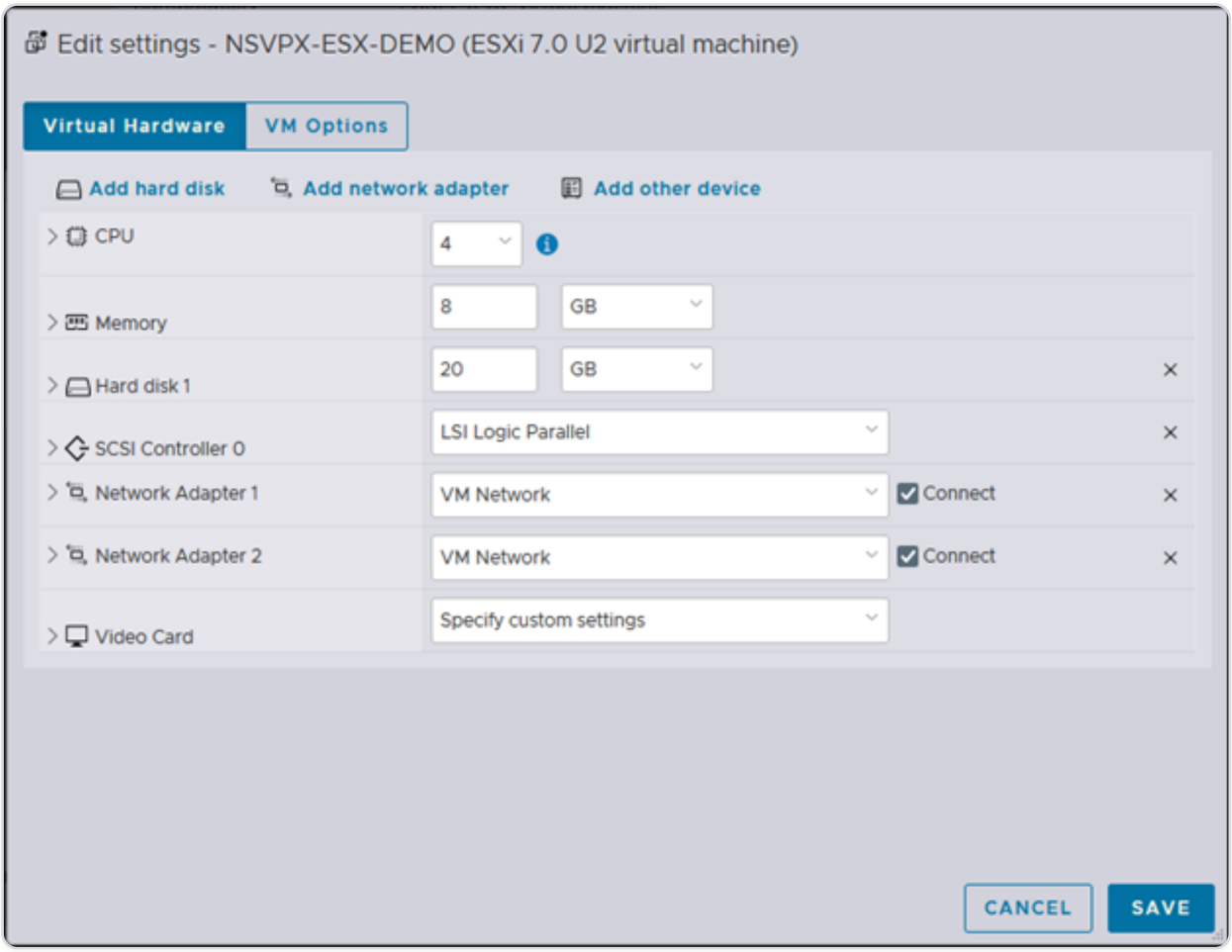
   b. 右键单击 NetScaler VPX 实例，然后选择“**兼容性 > 升级 VM 兼容性**”。

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



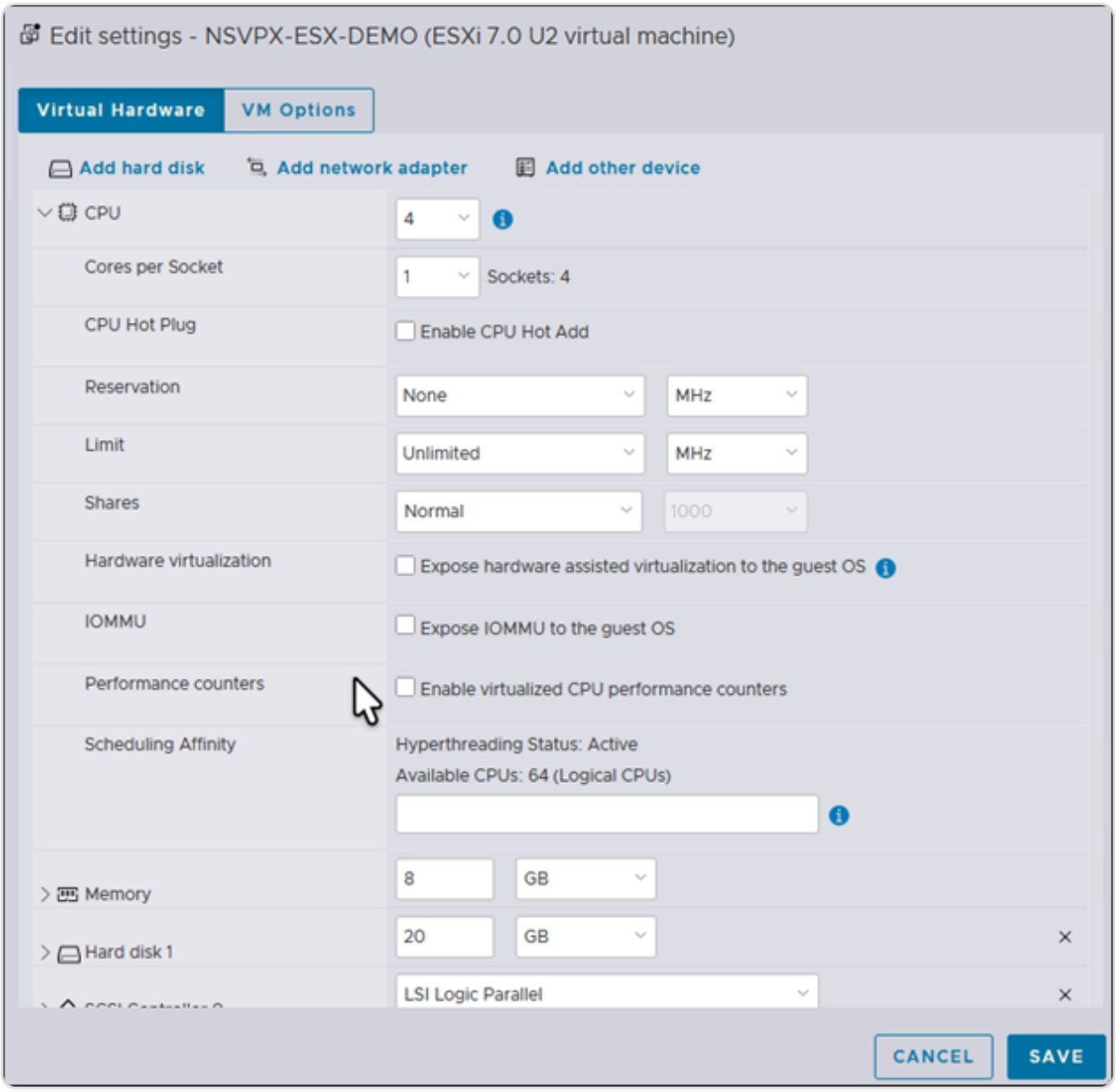
3. 右键单击 NetScaler VPX 实例，然后单击“**编辑设置**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 在“**CPU**”部分中，更新以下设置：

   - CPU 数量
   - 插槽数量
   - 预留
   - 限制
   - 份额

   如下设置值：

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

   b. 在“**每插槽核心数**”下拉列表中，选择插槽数量。

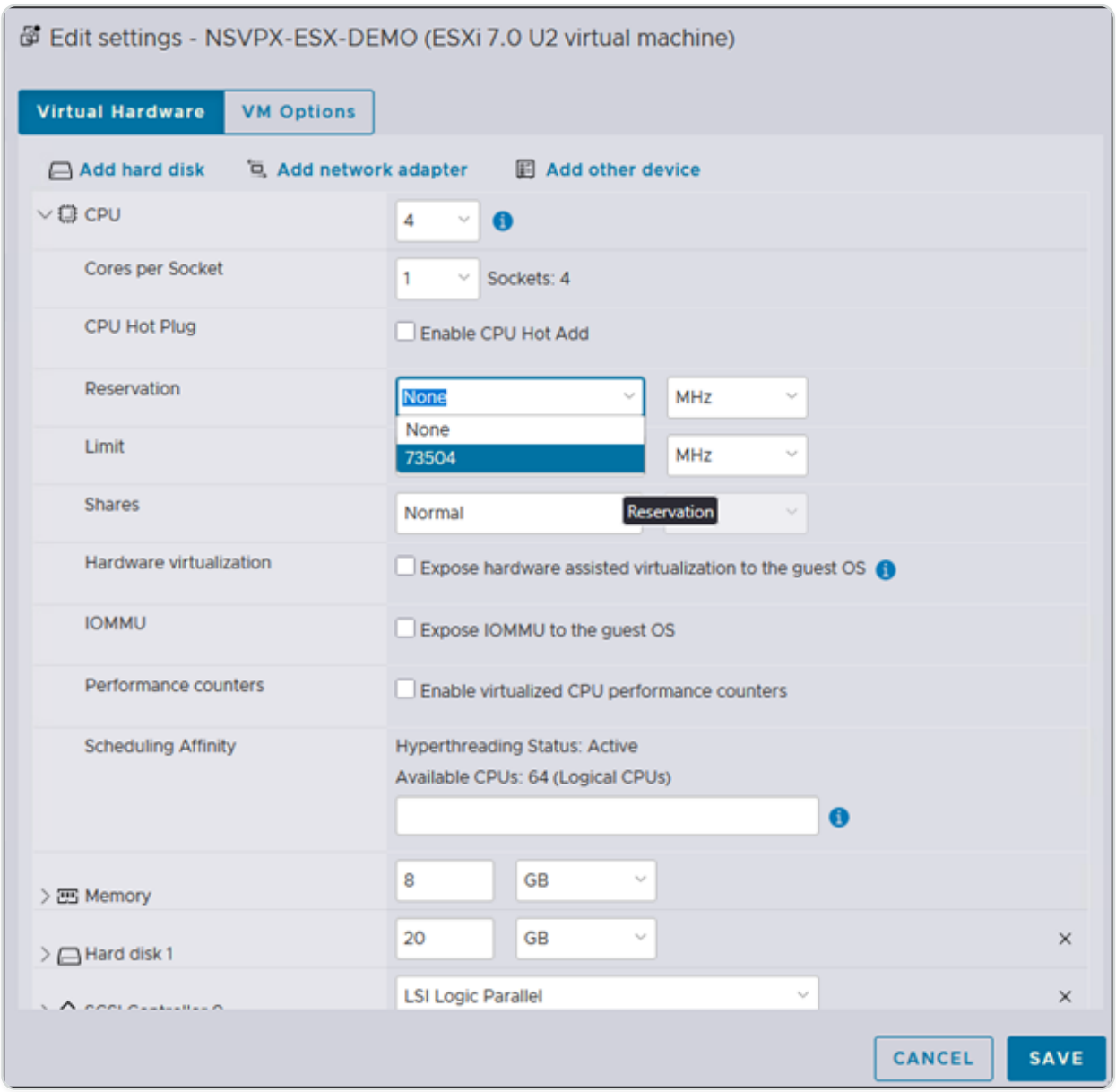
   c. (可选) 在“**CPU 热插拔**”字段中，选中或清除“**启用 CPU 热添加**”复选框。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

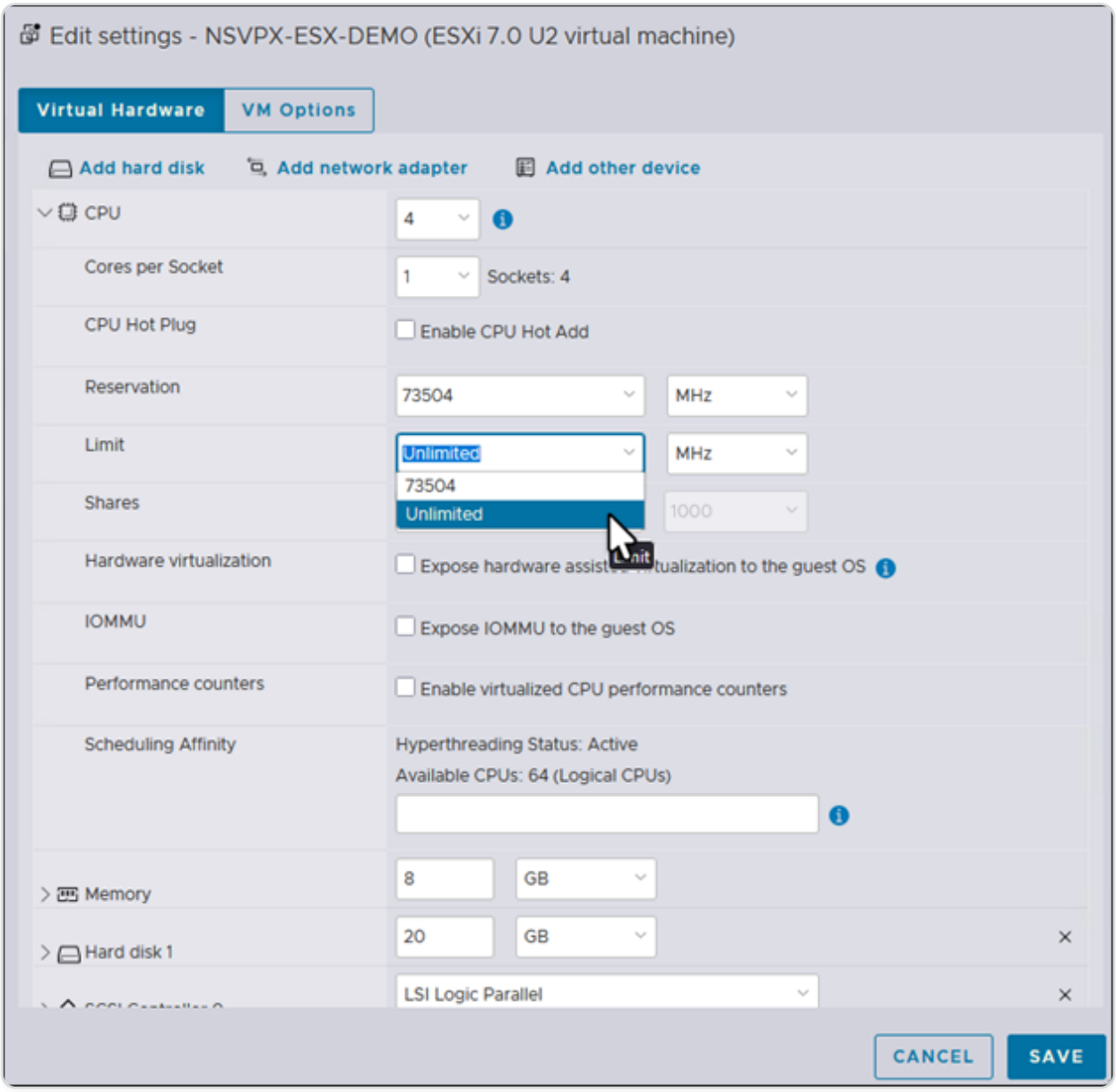
Citrix® 建议接受默认值（禁用）。

d. 在“**预留**”下拉列表中，选择显示为最大值的值。



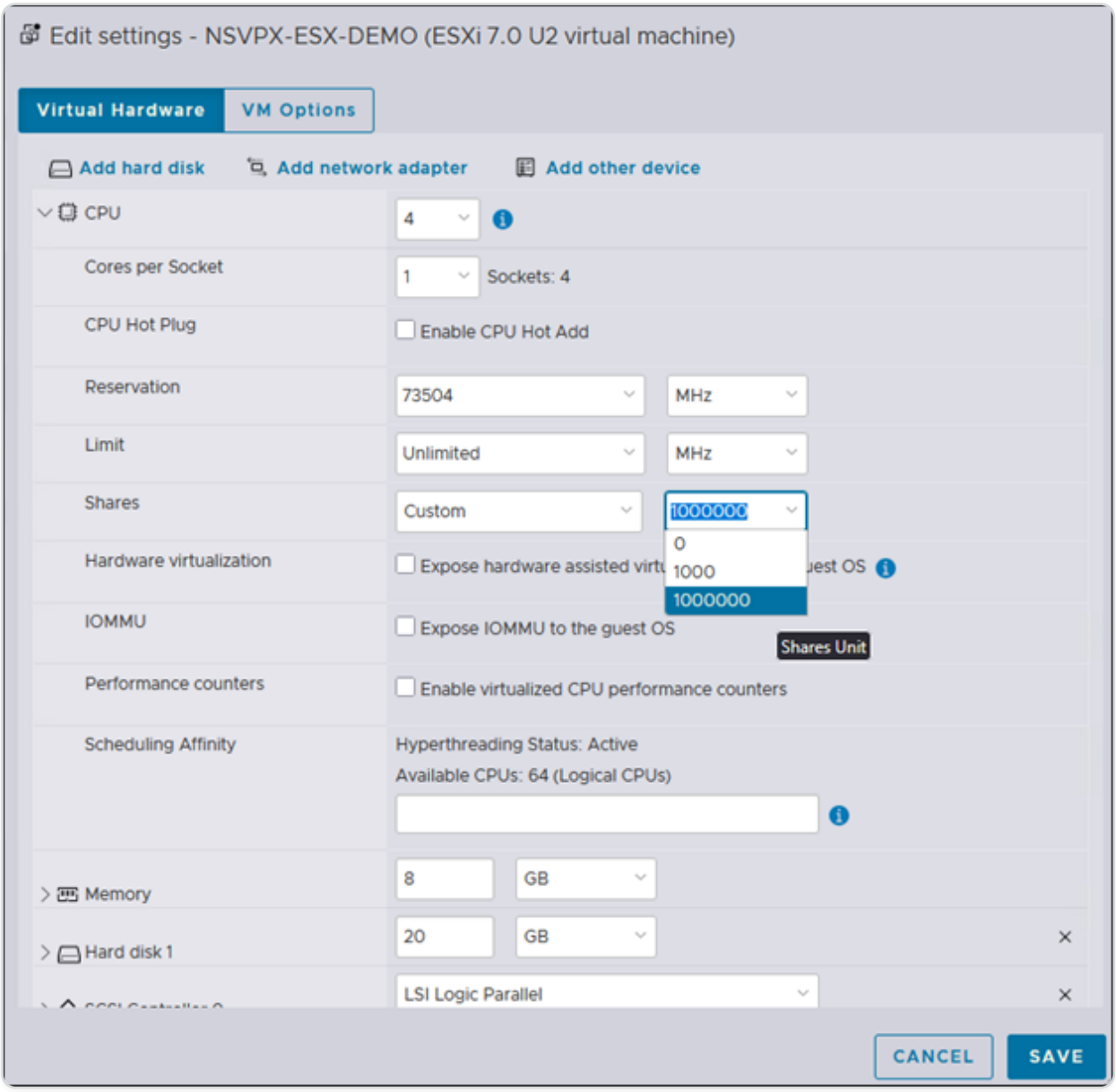
e. 在“**限制**”下拉列表中，选择显示为最大值的值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



f. 在“**份额**”下拉列表中，选择“**自定义**”以及显示为最大值的值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 在“**内存**”部分中，更新以下设置：

   - RAM 大小
   - 预留
   - 限制
   - 份额

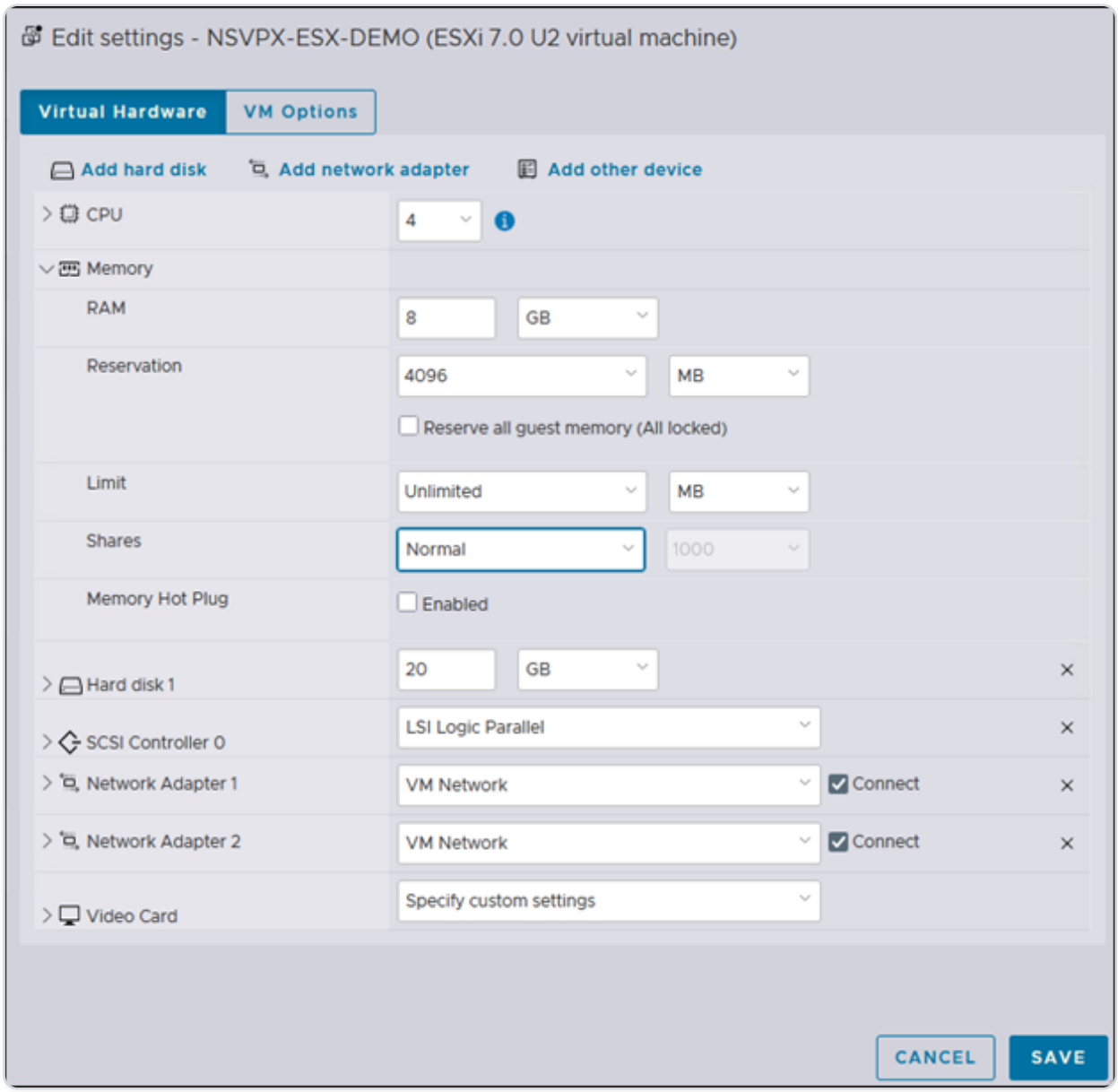
   按如下方式设置值：

   a. 在“**RAM**”下拉列表中，选择 RAM 的大小。它必须是 vCPU 数量 x 2 GB。例如，如果 vCPU 数量为 4，则 RAM = 4 x 2 GB = 8 GB。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

对于 NetScaler VPX 设备的 Advanced 或 Premium 版本，请确保为每个 vCPU 分配 4 GB RAM。例如，如果 vCPU 数量为 4，则 RAM = 4 x 4 GB = 16 GB。

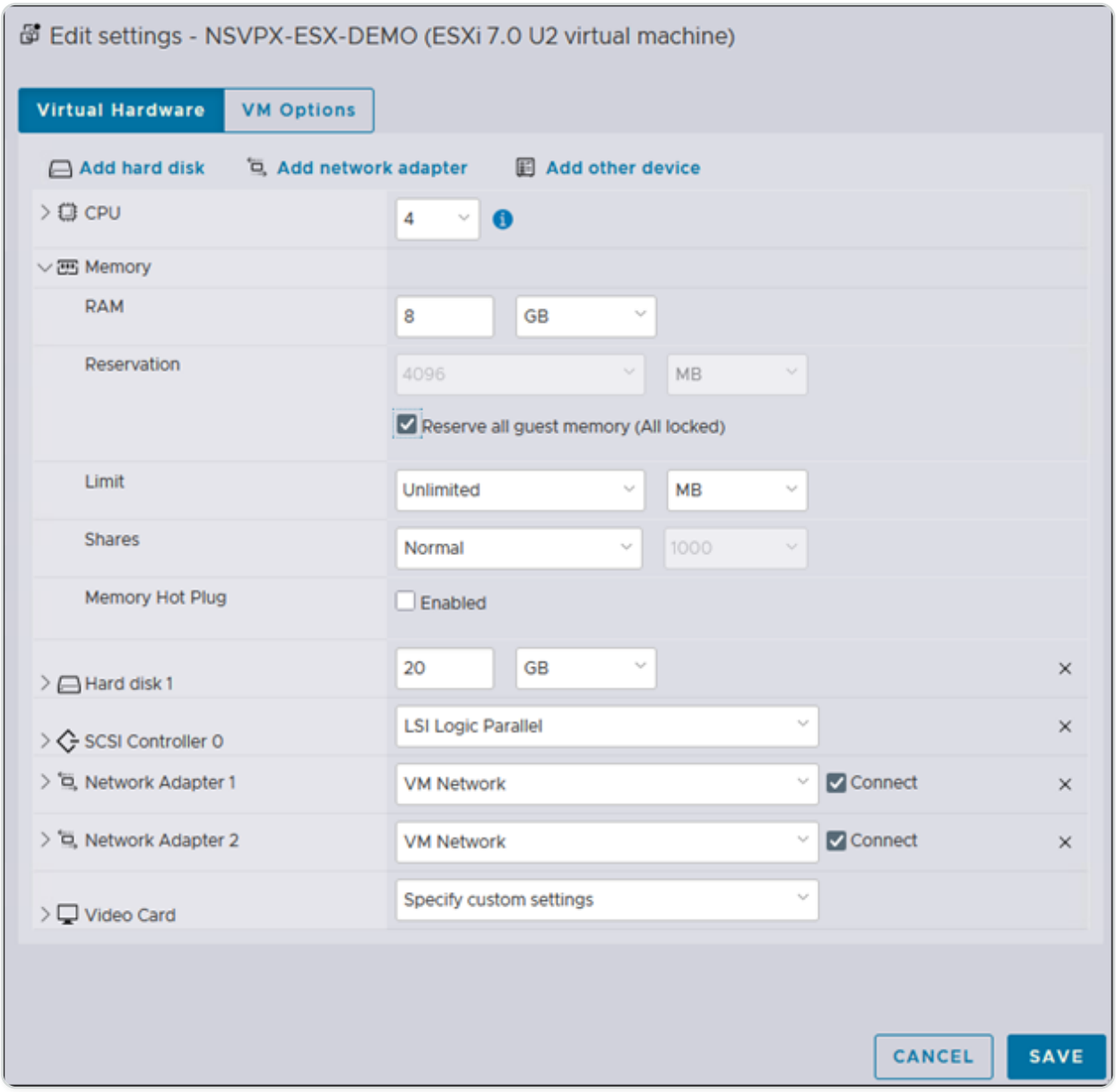


b. 在“**预留**”下拉列表中，输入内存预留的值，然后选中“**预留所有客户机内存（全部锁定）**”复选框。内存预留必须是 vCPU 数量 x 2 GB。例如，如果 vCPU 数量为 4，则内存预留必须是 4 x 2 GB = 8 GB。

注意：

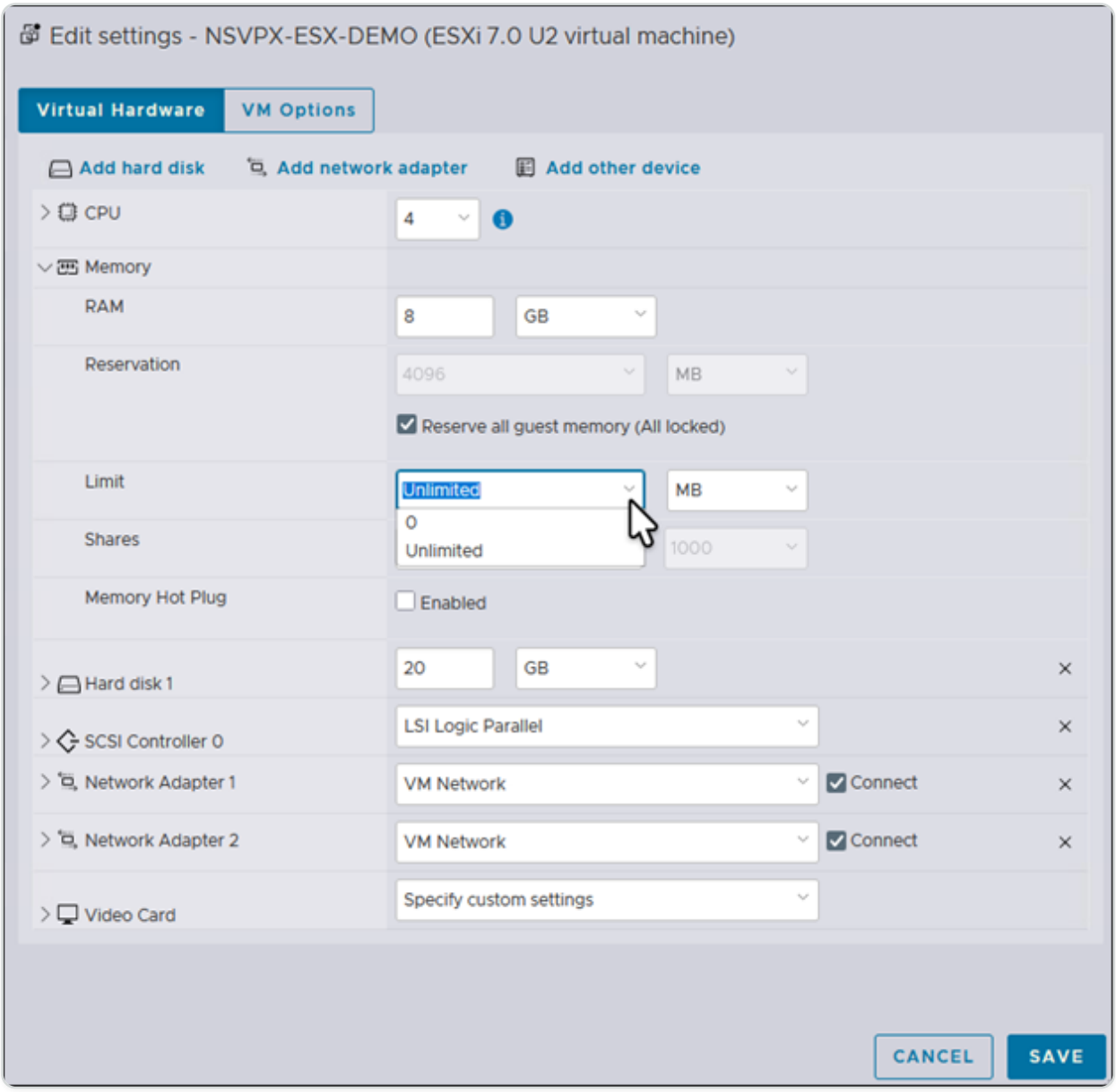
对于 NetScaler VPX 设备的 Advanced 或 Premium 版本，请确保为每个 vCPU 分配 4 GB RAM。例如，如果 vCPU 数量为 4，则 RAM = 4 x 4 GB = 16 GB。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



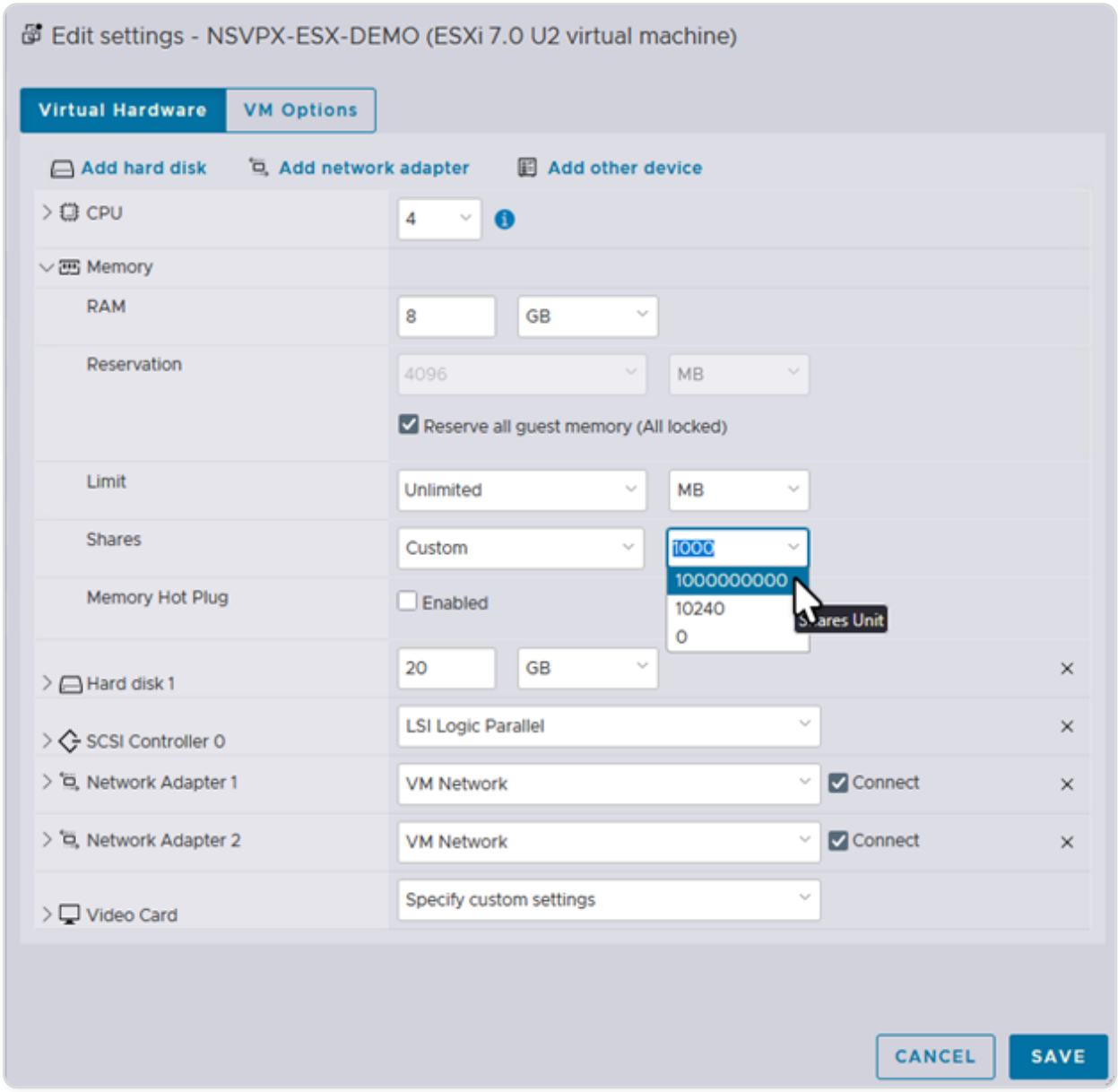
c. 在“**限制**”下拉列表中，选择显示为最大值的数字。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



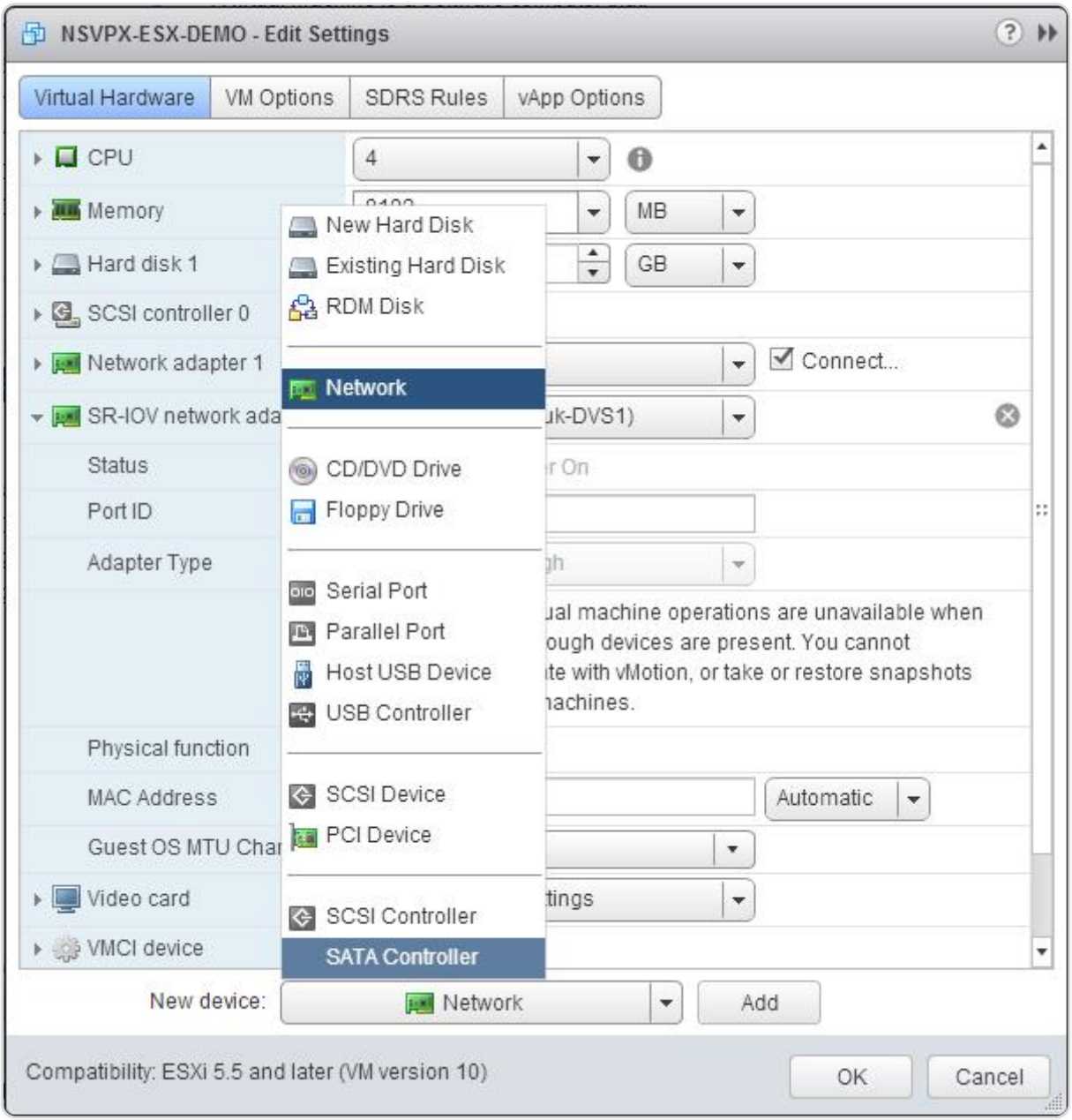
d. 在“**共享**”下拉列表中，选择“**自定义**”，然后选择显示为最大值的数字。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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**”。

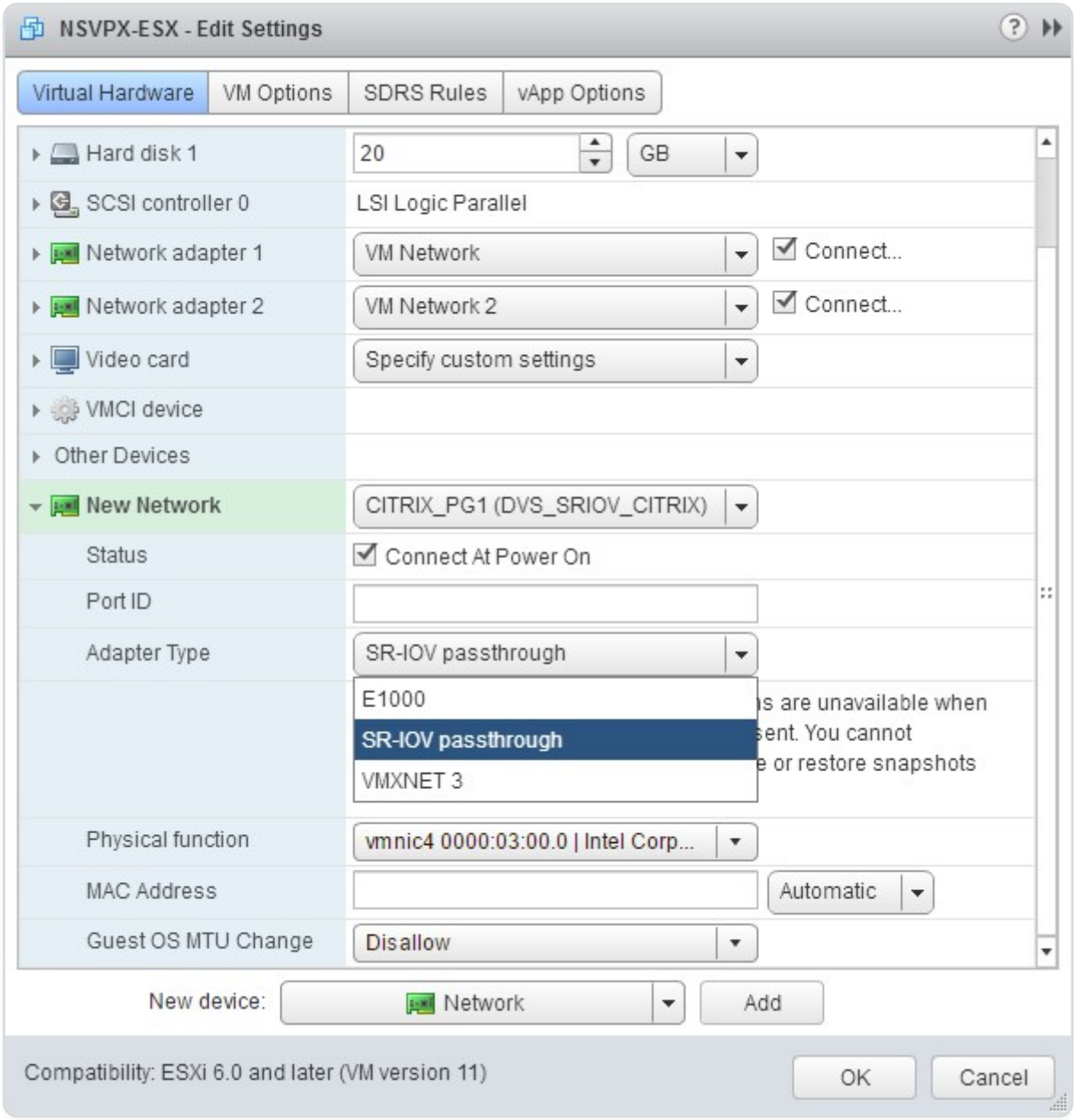
© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. 在“**新建网络**”部分。从下拉列表中，选择您创建的 `Portgroup`，然后执行以下操作：

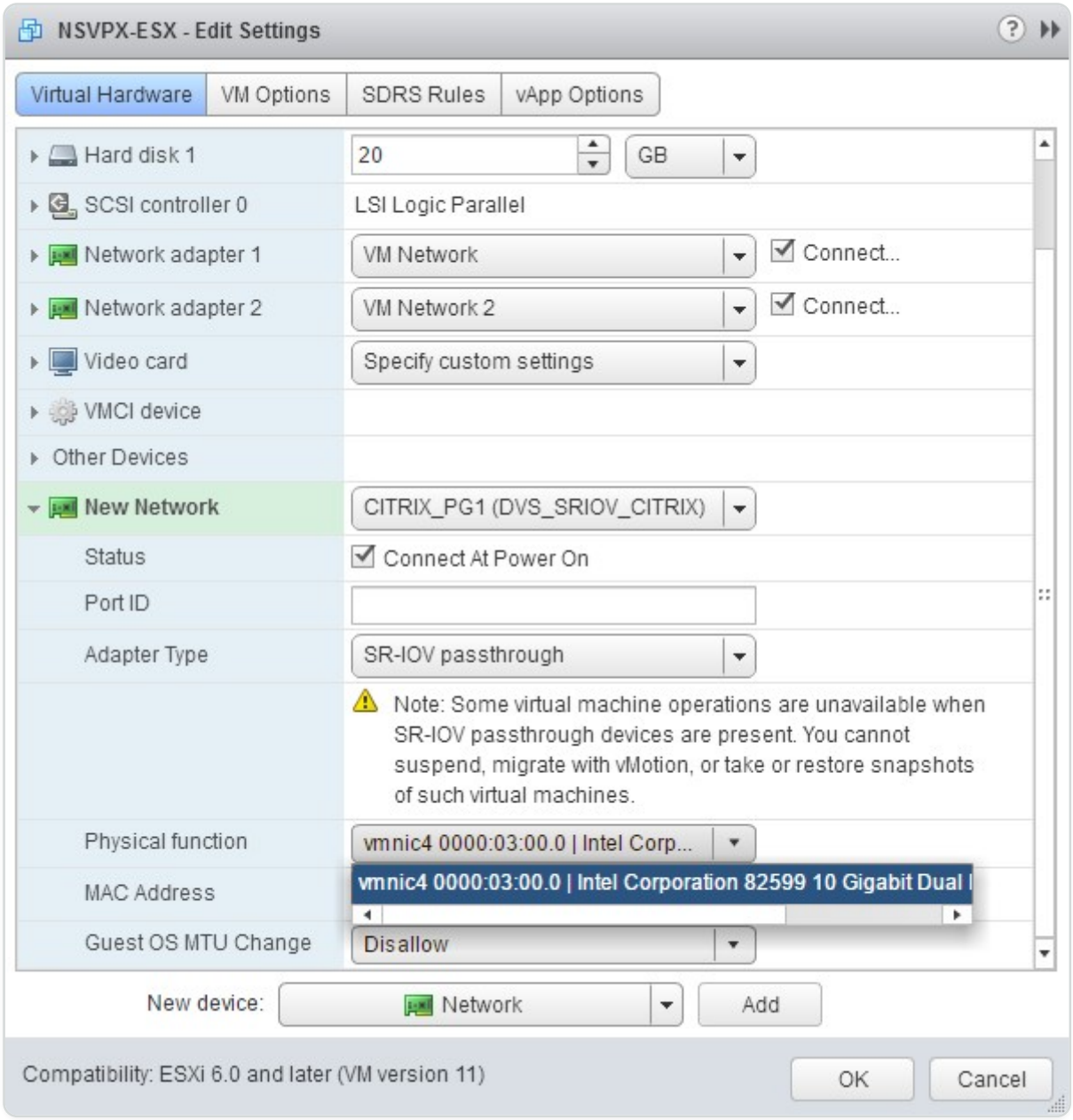
   a. 在“**适配器类型**”下拉列表中，选择“**SR-IOV 直通**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



b. 在“**物理功能**”下拉列表中，选择与 `Portgroup` 映射的物理适配器。

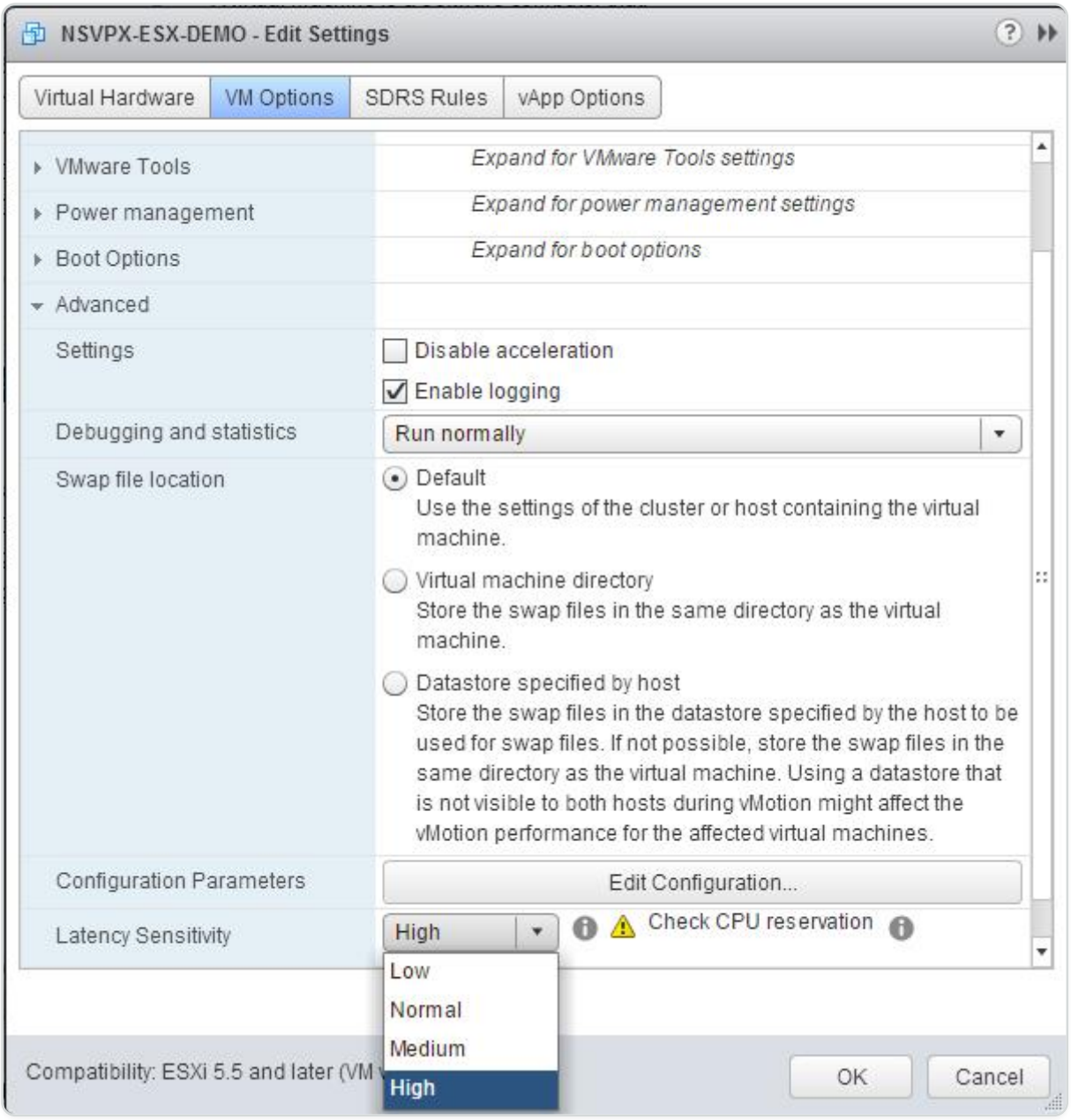
© 1997–2026 Citrix Systems, Inc. All rights reserved.



c. 在“**客户机操作系统 MTU 更改**”下拉列表中，选择“**不允许**”。

9. 在“**\<virtual_appliance\> - 编辑设置**”对话框中，单击“**VM 选项**”选项卡。
10. 在“**VM 选项**”选项卡上，选择“**高级**”部分。从“**延迟敏感度**”下拉列表中，选择“**高**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



11. 单击“**确定**”。
12. 启动 NetScaler VPX 实例。
13. NetScaler VPX 实例启动后，您可以使用以下命令验证配置：

    显示接口摘要

输出必须显示您配置的所有接口：

```
> show interface summary

---------------------------------------------------------------------------
------

      Interface  MTU        MAC                  Suffix
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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 &lt;ENABLED, UP, UP, HAMON, 802.1q>

        MTU=1500, native vlan=55, MAC=00:50:56:9f:0c:6f, uptime 0h21m53s

        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)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        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
```

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

您可以配置使用 E1000 网络接口的现有 NetScaler VPX 实例，以使用 SR-IOV 或 VMXNET3 网络接口。

要配置现有 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 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。

配置 NetScaler VPX 实例以使用 PCI 直通网络接口

概述

在 VMware ESX Server 上安装并配置 NetScaler VPX 实例后，您可以使用 vSphere Web Client 配置虚拟设备以使用 PCI 直通网络接口。

PCI 直通功能允许访客虚拟机直接访问连接到主机的物理 PCI 和 PCIe 设备。

先决条件

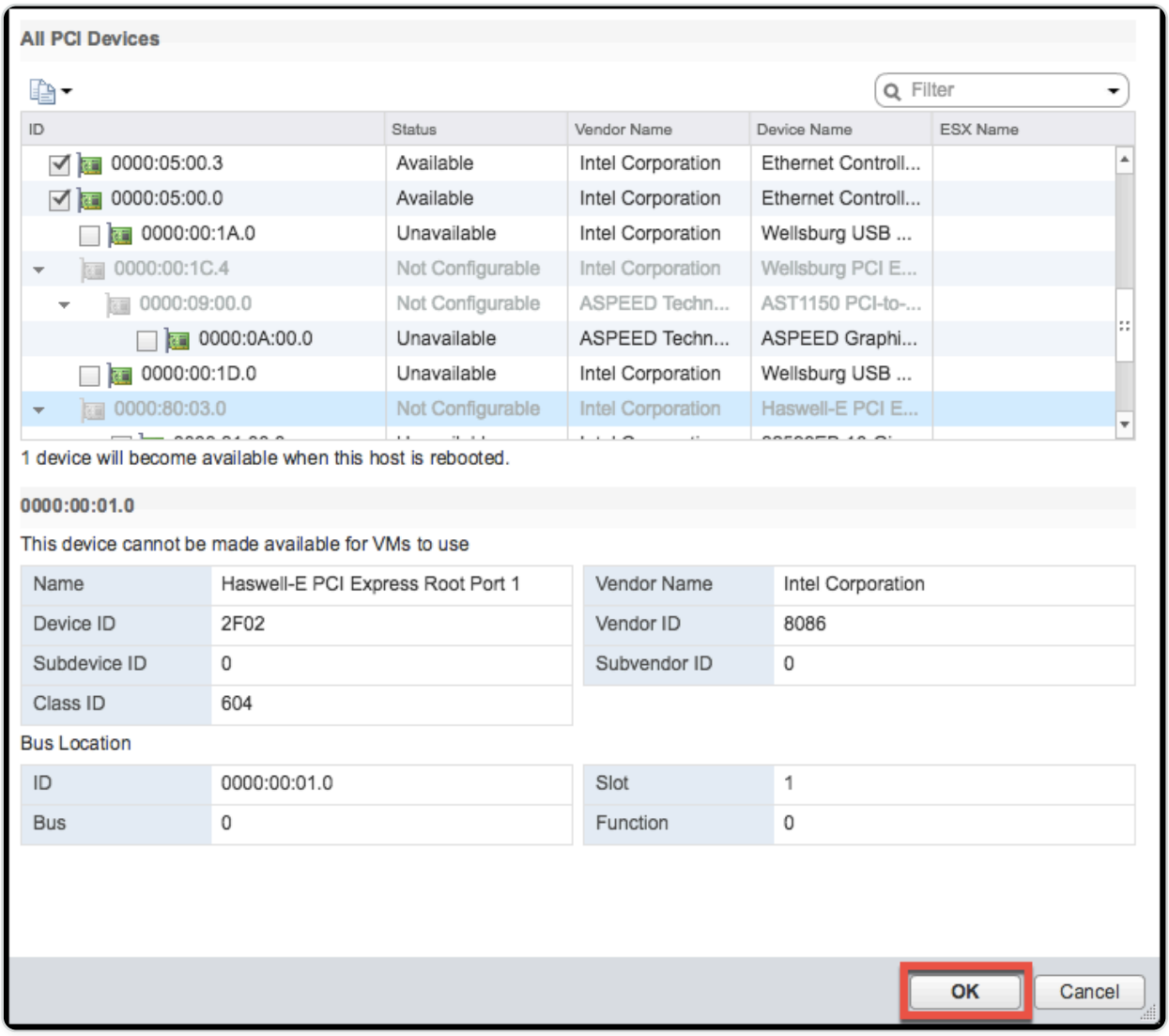
- 主机上 Intel XL710 NIC 的固件版本为 5.04。
- 连接到主机并在主机上配置的 PCI 直通设备
- 支持的网卡：
  - Intel X710 10G 网卡
  - Intel XL710 双端口 40G 网卡
  - Intel XL710 单端口 40G 网卡

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在主机上配置直通设备

在虚拟机上配置直通 PCI 设备之前，必须在主机上对其进行配置。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 **管理** > **设置** > **PCI 设备**。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“**编辑**”。
4. 出现“**编辑 PCI 设备可用性**”窗口。
5. 选择要用于直通的设备，然后单击“**确定**”。



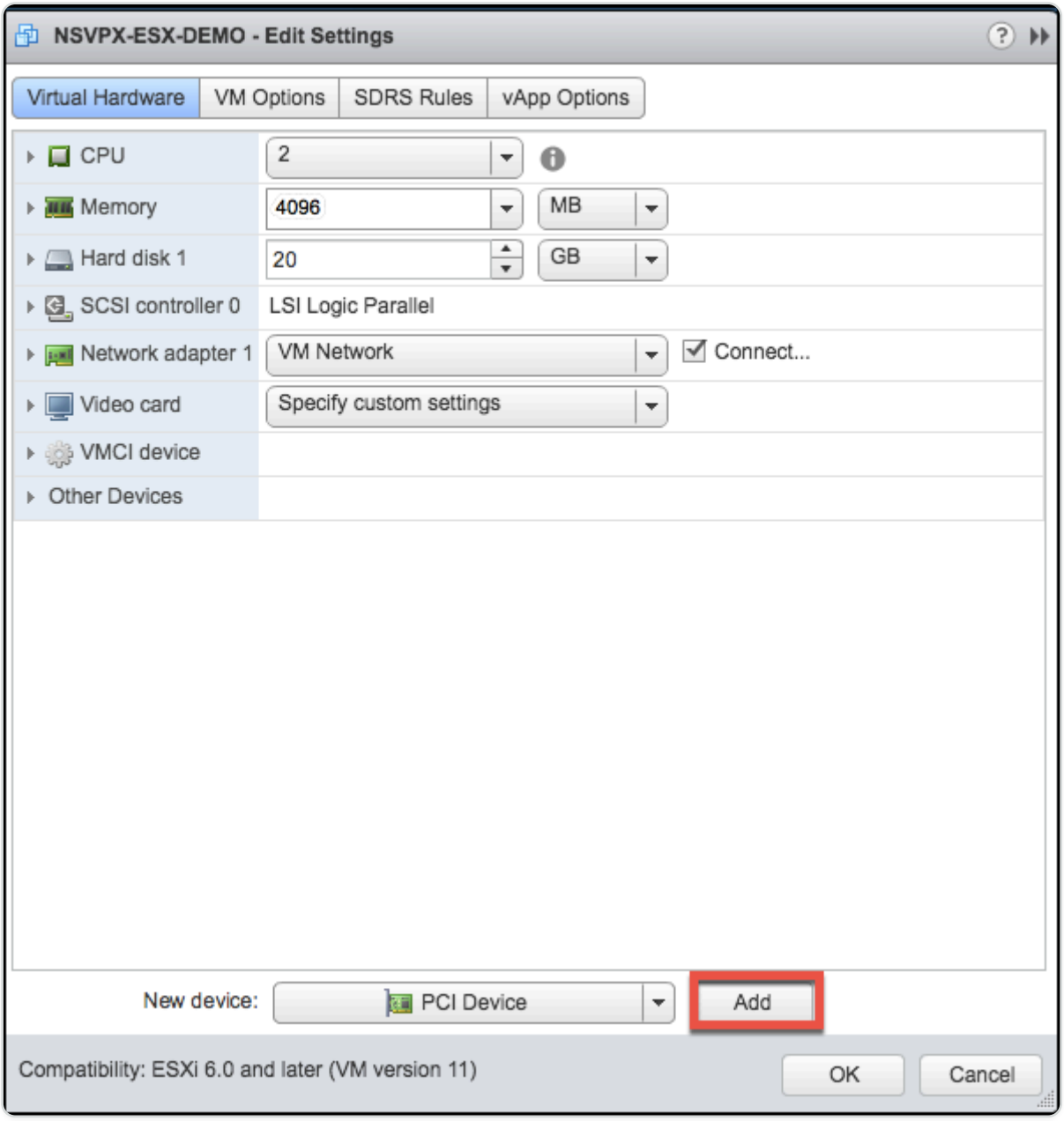
6. 重新启动主机。

在 NetScaler VPX 实例上配置直通设备

请按照以下步骤在 NetScaler VPX 实例上配置直通 PCI 设备。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 关闭虚拟机电源。
2. 右键单击虚拟机，然后选择“**编辑设置**”。
3. 在“**虚拟硬件**”选项卡上，从“**新设备**”下拉菜单中选择“**PCI 设备**”，然后单击“**添加**”。

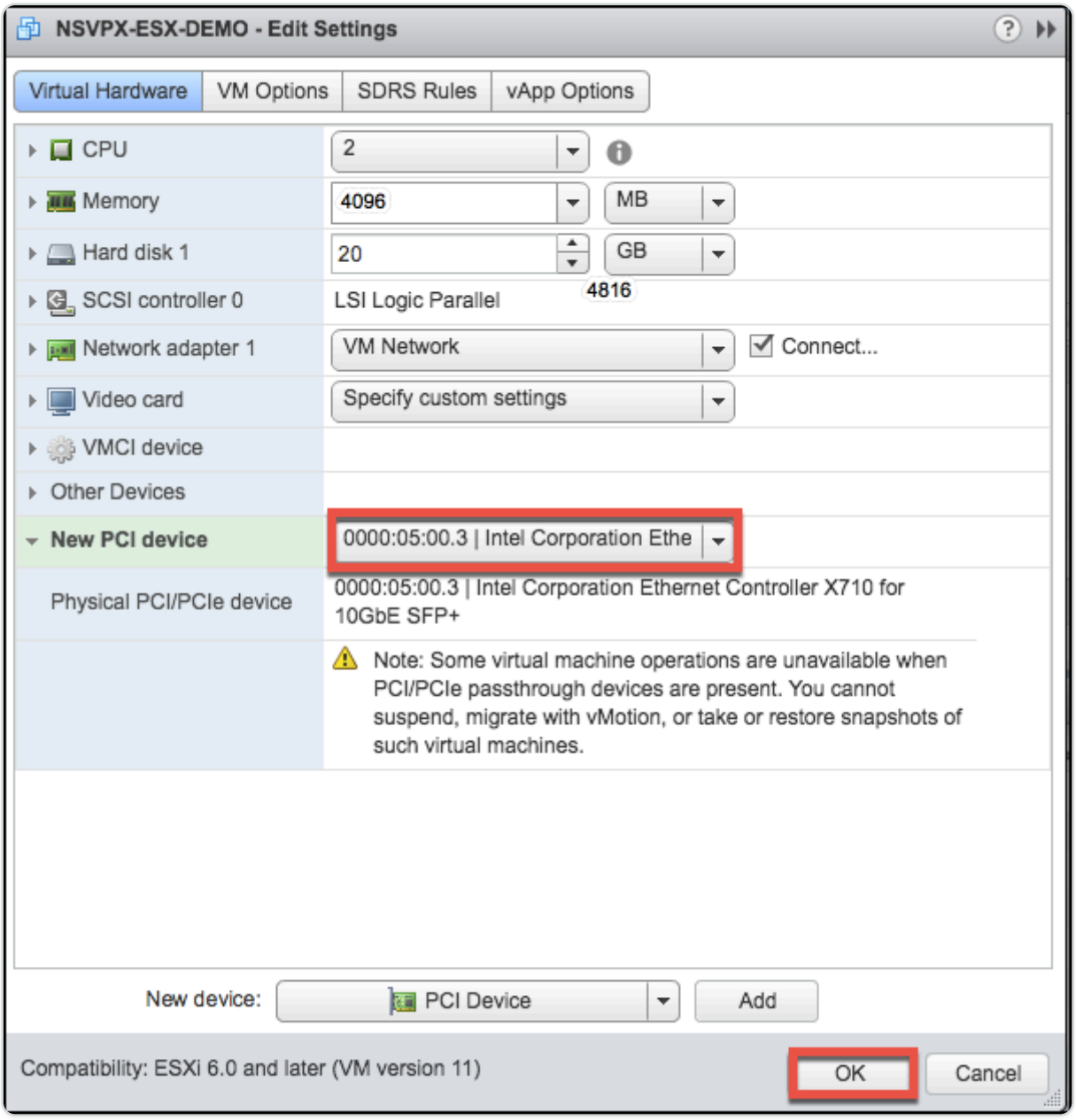


4. 展开“**新 PCI 设备**”，然后从下拉列表中选择要连接到虚拟机的直通设备，然后单击“**确定**”。

注意：

VMXNET3 网络接口和 PCI 直通网络接口不能共存。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 启动客户机虚拟机。

您已完成配置 NetScaler VPX 以使用 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

您可以在 VMware ESX 虚拟机管理程序上首次启动 NetScaler 设备时应用 NetScaler VPX 配置。因此，在某些情况下，可以更快地启动特定的设置或 VPX 实例。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

要在 ESX 中使用预启动用户数据进行引导，必须在 `<NS-CONFIG>` 部分中传递默认网关配置。有关 `<NS-CONFIG>` 标签内容的更多信息，请参阅 示例- `<NS-CONFIG>` -部分。

示例 `<NS-CONFIG>` 部分：

```
<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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

如何在 ESX 虚拟机管理程序上提供预启动用户数据

您可以通过以下两种方式，通过 Web 客户端或 vSphere 客户端在 ESX 虚拟机管理程序上提供预启动用户数据：

- 使用 CD/DVD ISO
- 使用 OVF 属性

使用 CD/DVD ISO 提供用户数据

您可以使用 VMware vSphere 客户端通过 CD/DVD 驱动器将用户数据作为 ISO 映像注入到 VM 中。

请按照以下步骤操作，以使用 CD/DVD ISO 提供用户数据：

1. 创建一个文件，文件名为 `userdata`，其中包含预启动用户数据内容。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 `userdata`。

2. 将 `userdata` 文件存储在一个文件夹中，并使用该文件夹构建 ISO 映像。

   您可以通过以下两种方法使用 `userdata` 文件构建 ISO 映像：

   - 使用任何图像处理工具，例如 PowerISO。
   - 在 Linux 中使用 `mkisofs` 命令。

   以下示例配置展示了如何在 Linux 中使用 `mkisofs` 命令生成 ISO 映像。

   ```
   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
   ```

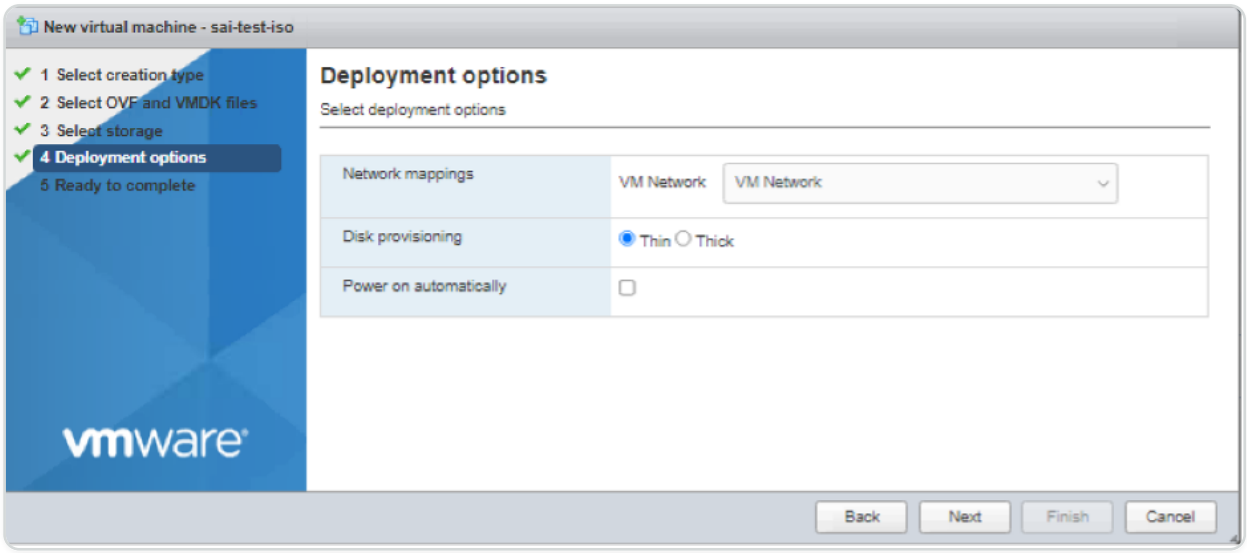
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-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
```

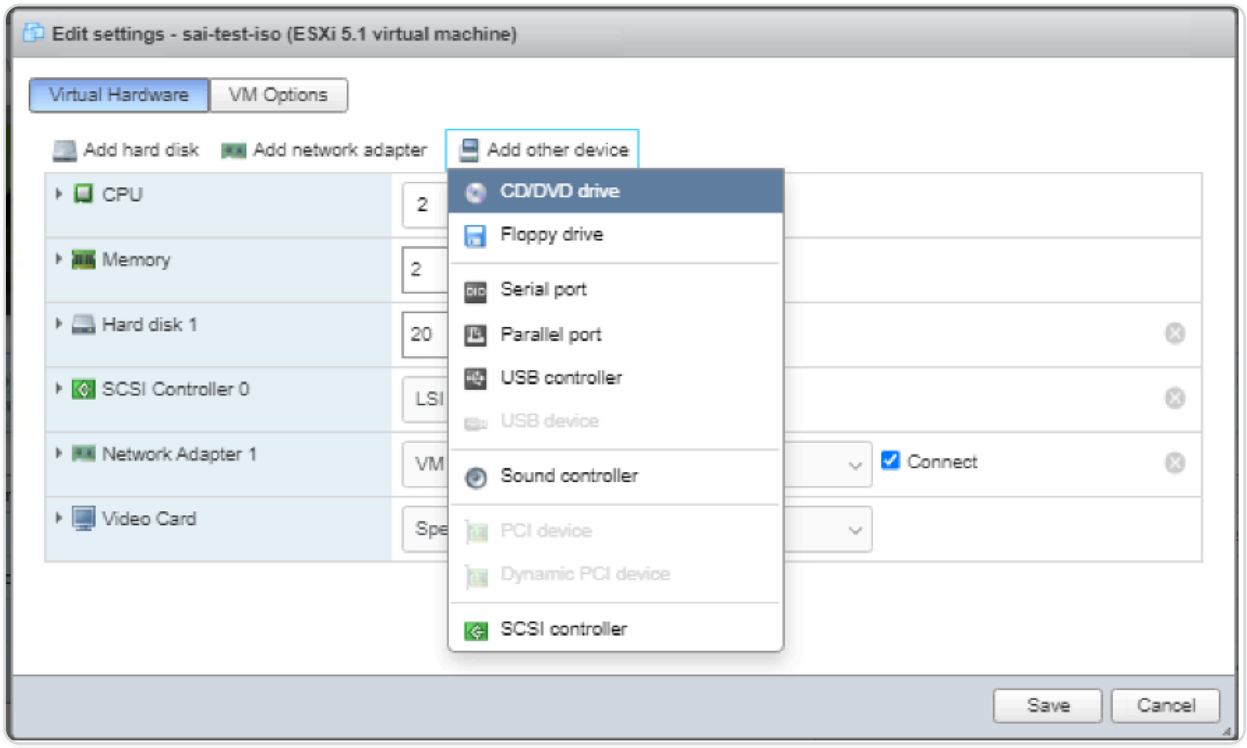
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Path table size(bytes): 10

Max brk space used 0

176 extents written (0 MB)
```

3. 使用标准部署过程预置 NetScaler VPX 实例以创建 VM。但不要自动启动 VM。

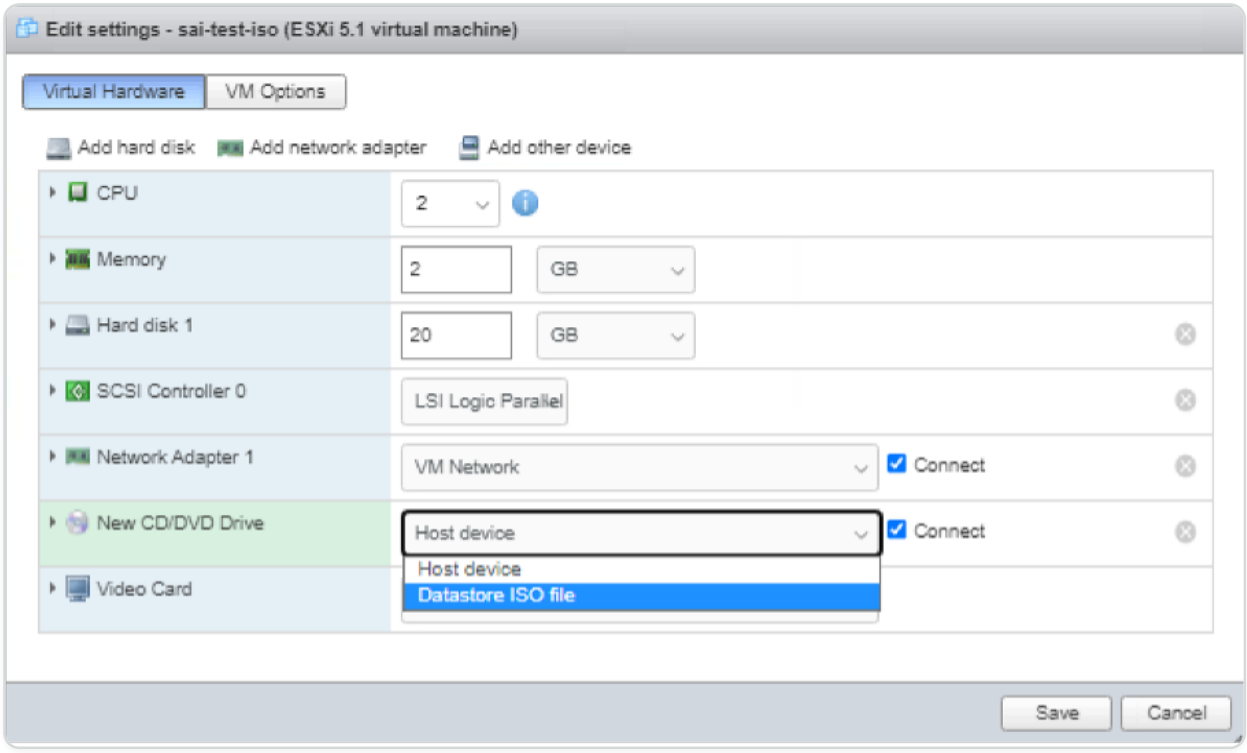


4. VM 成功创建后，将 ISO 文件作为 CD/DVD 驱动器附加到 VM。

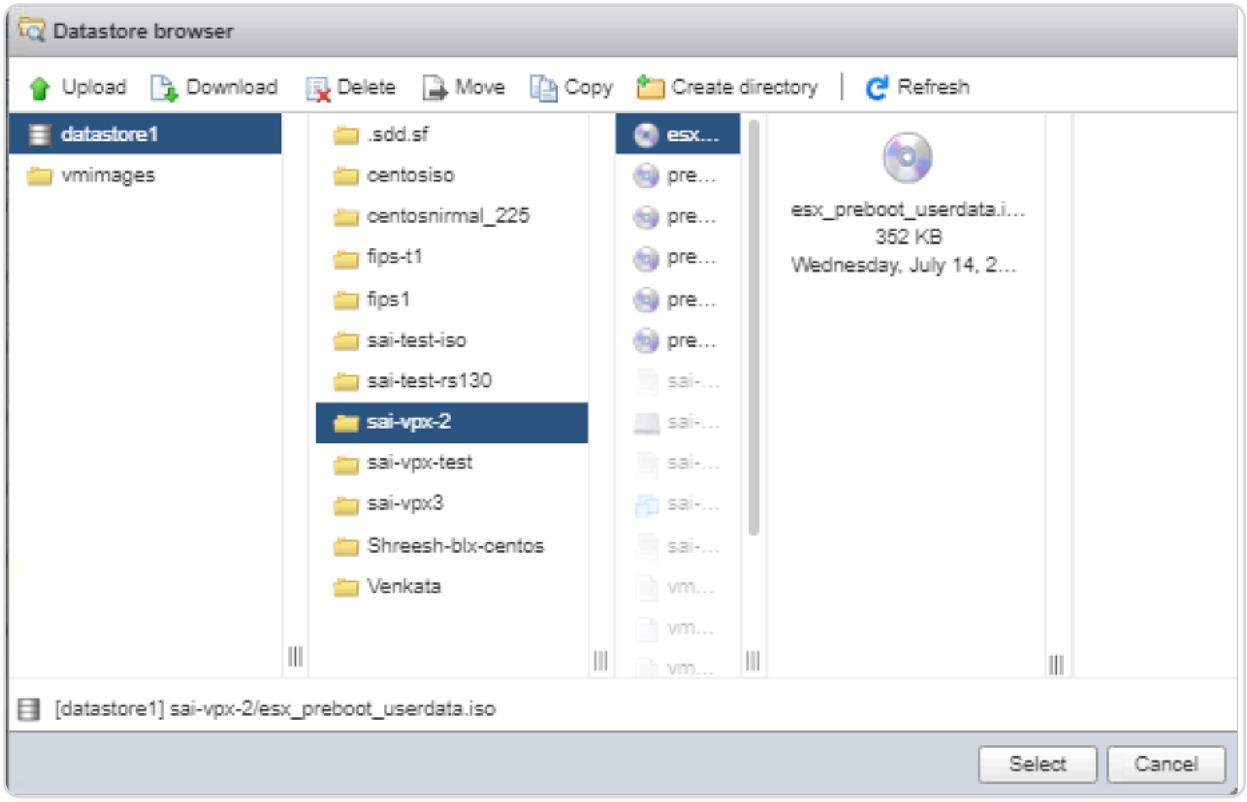


5. 导航到 **新建 CD/DVD 驱动器**，然后从下拉菜单中选择 **数据存储 ISO 文件**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 在 vSphere Client 中选择一个数据存储。



7. 启动 VM。

使用 ESX Web 客户端的 OVF 属性提供用户数据

请按照以下步骤使用 OVF 属性提供用户数据。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 创建包含用户数据内容的文件。

```
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。您可以使用以下两种方法执行 Base64 编码：

   - 在 Linux 中，使用以下命令：

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

     示例：

     ```
     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
     ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgPFNVQk5FVC1N
     QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
     RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg==
     ```

   - 使用在线工具编码用户数据内容，例如 Base64 Encode and Decode。

3. 在 ESX 虚拟机管理程序上的 NetScaler VPX 实例的 OVF 模板中包含一个 **Product** 部分。

   Product 部分示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<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. 在 Product 部分中，将 base64 编码的用户数据作为 `guestinfo.userdata` 属性的 `ovf:value` 提供。

```
<ProductSection>



  <Info>Information about the installed software</Info>

  <Product>NSVPX-VSK Template</Product>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  <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+CglhZGQgcm91
dGUgMC4wLjAuMCAw


LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkF
QPgog


ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1
CT09U


U1RSQVA+CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJ
PT1RT


VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICA
gICAg


ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICA
gICAg


ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5
FVC1N


QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULUlOVEV
SRkFD


RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg=
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  =">



      <Label>Userdata</Label>

      <Description> Userdata for ESX VPX </Description>

    </Property>



  </ProductSection>
```

5. 使用包含 Product 部分的修改后的 OVF 模板进行 VM 部署。

```
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 客户端的 OVF 属性提供用户数据

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

1. 创建包含用户数据内容的文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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。您可以使用以下两种方法执行 Base64 编码：

   - 在 Linux 中，使用以下命令：

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

     示例：

     ```
     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+CiAgICAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT
     VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAgICAg
     ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAgICAg
     ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgPFNVQk5FVC1N
     QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
     RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg==
     ```

   - 使用在线工具编码用户数据内容，例如 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 **Product** 部分。

   Product 部分示例：

   ```
   <ProductSection>
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  <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. 将 Base64 编码的用户数据作为 Product 部分中 `guestinfo.userdata` 属性的 `ovf:value` 提供。

```
<ProductSection>



  <Info>Information about the installed software</Info>

  <Product>NSVPX-VSK Template</Product>

  <Vendor>Citrix</Vendor>

  <VendorUrl>www.Citrix.com</VendorUrl>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  <Category> Preboot Userdata </Category>

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


ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+CglhZGQgcm91
dGUgMC4wLjAuMCAw


LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkF
QPgog


ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1
CT09U


U1RSQVA+CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJ
PT1RT


VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICA
gICAg


ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICA
gICAg


ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5
FVC1N


QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULUlOVEV
SRkFD


RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg=
=">
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      <Label>Userdata</Label>

      <Description> Userdata for ESX VPX </Description>

    </Property>



  </ProductSection>
```

5. 按如下方式将属性 `ovf:transport="com.vmware.guestInfo"` 添加到 VirtualHardwareSection：

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

6. 使用包含 Product 部分的修改后的 OVF 模板进行虚拟机部署。

```
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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 AWS 上的 VMware Cloud 上安装 NetScaler VPX 实例

AWS 上的 VMware Cloud (VMC) 使您能够在 AWS 上创建具有所需数量 ESX 主机的云软件定义数据中心 (SDDC)。AWS 上的 VMC 支持 NetScaler VPX 部署。VMC 提供与本地 vCenter 相同的用户界面。其功能与基于 ESX 的 NetScaler VPX 部署相同。

先决条件

在开始安装虚拟设备之前，请执行以下操作：

- 必须存在一个 VMware SDDC，且至少包含一个主机。
- 下载 NetScaler VPX 设备安装文件。
- 在 VMware SDDC 上创建虚拟机将连接到的适当网络段。
- 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 </zh-cn/licensing/licensing-guide-for-netscaler> 处的《*NetScaler VPX 许可指南*》。

VMware Cloud 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. 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

这不包括管理程序的任何磁盘要求。

对于 VPX 虚拟设备的生产用途，必须保留全部内存分配。

OVF Tool 1.0 系统要求

OVF Tool 是一个客户端应用程序，可以在 Windows 和 Linux 系统上运行。下表描述了最低系统要求。

表 2. OVF 工具安装的最低系统要求

组件	要求
操作系统	有关 VMware 的详细要求，请在 `<http://kb.vmware.com/>` 处搜索“OVF 工具用户指南”PDF 文件。
CPU	最低 750 MHz，建议 1 GHz 或更快
RAM	最低 1 GB，建议 2 GB
网卡	100 Mbps 或更快的网卡

有关安装 OVF 的信息，请在 `<http://kb.vmware.com/>` 处搜索“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 实例安装包遵循开放式虚拟机 (OVF) 格式标准。您可以从 Citrix 网站下载文件。您需要一个 Citrix 帐户才能登录。如果您没有 Citrix 帐户，请访问主页 http://www.citrix.com。单击**“新用户”链接**，然后按照说明创建新的 Citrix 帐户。

登录后，从 Citrix® 主页导航到以下路径：

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

将以下文件复制到与 ESX 服务器位于同一网络中的工作站。将所有三个文件复制到同一文件夹中。

- NSVPX-ESX-\<release number\>-\<build number\>-disk1.vmdk（例如，NSVPX-ESX-13.0-79.64-disk1.vmdk）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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，您可以使用 SDDC 在 VMware 云上安装虚拟设备。您可以安装的虚拟设备数量取决于 SDDC 上可用的内存量。

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

1. 在您的工作站上打开 VMware SDDC。
2. 在“**用户名**”和“**密码**”文本框中，键入管理员凭据，然后单击“登录”。
3. 在“**文件**”菜单上，单击“**部署 OVF 模板**”。
4. 在“**部署 OVF 模板**”对话框中，在“**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，请修改 OVF 以使用 VMXNET3 接口而不是 E1000。

5. 将虚拟设备 OVF 模板中显示的网络映射到您在 VMware SDDC 上配置的网络。单击“**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 实例了。在导航窗格中，选择您已安装的 NetScaler VPX 实例，然后从右键单击菜单中选择“**开机**”。单击“**控制台**”选项卡以模拟控制台端口。
7. 如果要安装另一个虚拟设备，请从步骤 6 开始重复操作。
8. 从选作管理网络的同一网段中指定管理 IP 地址。网关使用相同的子网。
9. VMware SDDC 要求明确创建 NAT 和防火墙规则，适用于属于网络段的所有私有 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

要在 Microsoft Windows Server 上安装 NetScaler VPX 实例，您必须首先在具有足够系统资源的计算机上安装已启用 Hyper-V 角色的 Windows Server。安装 Hyper-V 角色时，请务必指定 Hyper-V 用于创建虚拟网络的服务器上的网卡。您可以为主机保留一些网卡。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。它包括 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，您可以在虚拟设备上配置网络适配器，添加虚拟网卡，然后分配 NetScaler IP 地址、子网掩码和网关，并完成虚拟设备的基本配置。

在 VPX 实例的初始配置之后，如果您想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：

中间系统到中间系统 (ISIS) 协议在托管于 HyperV-2012 平台上的 NetScaler VPX 虚拟设备上不受支持。

在 Microsoft 服务器上安装 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 Windows Server 上启用 Hyper-V 角色。有关详细信息，请参阅 `<http://technet.microsoft.com/zh-cn/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 实例许可证的更多信息，请参阅 `<https://support.citrix.com/s/article/CTX255959-how-to-allocate-and-install-citrix-netscaler-vpx-licenses?language=en_US>` 处的《*NetScaler VPX 许可指南*》。

Microsoft 服务器硬件要求

下表描述了适用于 Microsoft 服务器的最低系统要求。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表 1. Microsoft 服务器的最低系统要求

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 NetScaler VPX 实例的虚拟计算资源。

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) 格式提供。您可以从 Citrix 网站下载这些文件。您需要一个 Citrix 帐户才能登录。如果您没有 Citrix 帐户，请访问主页，单击 **Sign In > My account > Create Citrix Account**，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 **Downloads**。
4. 在 **Select a Product** 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. 将压缩文件下载到您的服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 Microsoft 服务器上安装 NetScaler VPX 实例

在 Microsoft Server 上启用 Hyper-V 角色并提取虚拟设备文件后，您可以使用 Hyper-V 管理器安装 NetScaler VPX 实例。导入虚拟机后，您需要通过将虚拟 NIC 与 Hyper-V 创建的虚拟网络关联来配置它们。

最多可以配置八个虚拟 NIC。即使物理 NIC 处于关闭状态，虚拟设备也会认为虚拟 NIC 处于开启状态，因为它仍然可以与同一主机（服务器）上的其他虚拟设备通信。

注意：

虚拟设备运行时无法更改任何设置。请关闭虚拟设备，然后进行更改。

使用 Hyper-V 管理器在 Microsoft 服务器上安装 NetScaler VPX 实例：

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 管理器**”下，选择要安装 NetScaler VPX 实例的服务器。
3. 在“**操作**”菜单上，单击“**导入虚拟机**”。
4. 在“**导入虚拟机**”对话框中，在“**位置**”中，指定包含 NetScaler VPX 实例软件文件的文件夹路径，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：

如果您收到的是压缩文件，请务必先将文件解压到一个文件夹中，然后再指定该文件夹的路径。

1. 单击“**导入**”。
2. 验证您导入的虚拟设备是否列在“**虚拟机**”下。
3. 要安装另一个虚拟设备，请重复步骤 **2** 到 **6**。

重要提示：

确保在步骤 **4** 中将文件解压到不同的文件夹。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 Hyper-V 上自动预配 NetScaler VPX 实例

NetScaler VPX 实例的自动预配是可选的。如果未进行自动预配，虚拟设备提供配置 IP 地址等选项。

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

1. 使用示例中所示的 xml 文件创建符合 ISO9660 标准的 ISO 映像。确保 xml 文件的名称为 **userdata**。

   您可以使用以下方式从 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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Version>2013.1</Version>

<Vendor>CITRIX</Vendor>

<Locale>en</Locale>

</PlatformSection>

<PropertySection>

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

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

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

<Property oe:key="com.citrix.netscaler.mgmt.ip"
oe:value="10.102.100.122"/>

<Property oe:key="com.citrix.netscaler.mgmt.netmask"
oe:value="255.255.255.128"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property oe:key="com.citrix.netscaler.mgmt.gateway"
oe:value="10.102.100.67"/></PropertySection>



</Environment>
```

2. 将 ISO 映像复制到 Hyper-V 服务器。
3. 选择您导入的虚拟设备，然后从“**操作**”菜单中选择“**设置**”。您也可以选择虚拟设备，然后右键单击并选择“**设置**”。将显示所选虚拟设备的“**设置**”窗口。
4. 在“**设置**”窗口中，在硬件部分下，单击“**IDE 控制器**”。
5. 在右侧窗格中，选择“**DVD 驱动器**”并单击“**添加**”。DVD 驱动器将添加到左侧窗格的“**IDE 控制器**”部分下。
6. 选择在步骤 5 中添加的“**DVD 驱动器**”。在右侧窗格中，选择“**映像文件**”单选按钮，然后单击“**浏览**”，选择您在步骤 2 中复制到 Hyper-V 服务器上的 ISO 映像。
7. 单击“**应用**”。

注意：

虚拟设备实例在以下情况下以默认 IP 地址启动：

- DVD 驱动器已连接，但未提供 ISO 文件。
- ISO 文件不包含用户数据文件。
- 用户数据文件名或格式不正确。

要在 NetScaler VPX 实例上配置虚拟 NIC，请执行以下步骤：

1. 选择您导入的虚拟设备，然后在“**操作**”菜单上，选择“**设置**”。
2. 在“**\<虚拟设备名称\> 的设置**”对话框中，单击左窗格中的“**添加硬件**”。
3. 在右窗格中，从设备列表中选择“**网络适配器**”。
4. 单击“**添加**”。
5. 验证左窗格中是否显示“**网络适配器（未连接）**”。
6. 在左窗格中选择网络适配器。
7. 在右窗格中，从“**网络**”菜单中选择要将适配器连接到的虚拟网络。
8. 要为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**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. 单击“**应用**”，然后单击“**确定**”。

配置 NetScaler VPX 实例：

1. 右键单击您之前安装的虚拟设备，然后选择“**启动**”。
2. 通过双击虚拟设备访问控制台。
3. 输入虚拟设备的 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 浏览器中输入 IP 地址以访问虚拟设备。

注意：

您还可以使用虚拟机 (VM) 模板通过 SCVMM 预配 NetScaler VPX 实例。

如果您将 Microsoft Hyper-V NIC 组队解决方案与 NetScaler VPX 实例配合使用，请参阅文章 CTX224494 以获取更多信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 Linux-KVM 平台上安装 NetScaler VPX 实例

要在 Linux-KVM 平台上设置 NetScaler VPX，您可以使用图形化虚拟机管理器 (Virtual Manager) 应用程序。如果您更喜欢 Linux-KVM 命令行，可以使用 `virsh` 程序。

必须使用 KVM 模块和 QEMU 等虚拟化工具在合适的硬件上安装主机 Linux 操作系统。可以在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。

预置 NetScaler VPX 实例后，您可以添加更多接口。

限制和使用指南

一般建议

为避免不可预测的行为，请遵循以下建议：

- 请勿更改与 VPX VM 关联的 VNet 接口的 MTU。在修改任何配置参数（例如接口模式或 CPU）之前，请关闭 VPX VM。
- 请勿强制关闭 VPX VM。也就是说，请勿使用 **强制关闭** 命令。
- 在主机 Linux 上进行的任何配置都可能不是持久性的，具体取决于您的 Linux 发行版设置。您可以选择使这些配置持久化，以确保主机 Linux 操作系统在重新启动后行为一致。
- 对于每个预置的 NetScaler VPX 实例，NetScaler 包必须是唯一的。

限制

- 不支持在 KVM 上运行的 VPX 实例的实时迁移。

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

检查运行 NetScaler VPX 实例的 Linux-KVM 服务器的最低系统要求。

CPU 要求：

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

如果上述扩展的 **BIOS** 设置已禁用，则必须在 BIOS 中启用它们。

- 为主机 Linux 提供至少 2 个 CPU 核心。
- 对处理器速度没有具体建议，但速度越快，VM 应用程序的性能越好。

内存 (RAM) 要求：

主机 Linux 内核至少需要 4 GB。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 要求的空间。单个 NetScaler VPX VM 需要 20 GB 磁盘空间。

软件要求

使用的主机内核必须是 64 位 Linux 内核，版本 2.6.20 或更高版本，并包含所有虚拟化工具。Citrix 建议使用较新的内核，例如 3.6.11-4 及更高版本。

许多 Linux 发行版，例如 Red Hat、CentOS 和 Fedora，都具有经过测试的内核版本和相关的虚拟化工具。

客户机虚拟机硬件要求

NetScaler VPX 支持 IDE 和 virtIO 硬盘类型。硬盘类型已在 XML 文件中配置，该文件是 NetScaler 软件包的一部分。

网络要求

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

有关支持的网络接口的更多信息，请参阅：

- 使用虚拟机管理器预置 NetScaler VPX 实例
- 配置 NetScaler VPX 实例以使用 SR-IOV 网络接口
- 配置 NetScaler VPX 实例以使用 PCI 直通网络接口

源接口和模式

源设备类型可以是 Bridge 或 MacVTap。在 MacVTap 中，有四种模式可能：VEPA、Bridge、Private 和 Pass-through。请根据以下内容检查您可以使用的接口类型和支持的流量类型：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

网桥：

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

MacVTap (VEPA 模式)：

- 比网桥性能更好。
- 同一底层设备的接口可以在虚拟机之间共享。
- 使用同一底层设备进行虚拟机间通信
- 仅当上游或下游交换机支持 VEPA 模式时才可能实现。

MacVTap（私有模式）：

- 性能优于网桥。
- 同一底层设备的接口可以在虚拟机之间共享。
- 使用同一底层设备进行虚拟机间通信是不可能的。

MacVTap（网桥模式）：

- 与网桥相比更好。
- 同一底层设备的接口可以在虚拟机之间共享。
- 如果底层设备链路处于 UP 状态，则可以使用同一底层设备进行虚拟机间通信。

MacVTap（直通模式）：

- 与网桥相比更好。
- 同一底层设备的接口不能在虚拟机之间共享。
- 只有一个虚拟机可以使用该底层设备。

注意：

为了获得 VPX 实例的最佳性能，请确保在源接口上关闭 `gro` 和 `lro` 功能。

源接口的属性

确保关闭源接口的通用接收卸载 (`gro`) 和大型接收卸载 (`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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

示例：

```
[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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    rx-vlan-offload: on


                    tx-vlan-offload: on


                    ntuple-filters: off


                    receive-hashing: on


    [root@localhost ~]#
```

示例：

如果主机 Linux 网桥用作源设备（如以下示例所示），则必须在 VNet 接口（连接主机与客户机 VM 的虚拟接口）上关闭 `lro` 功能。

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


    bridge name     bridge  id               STP enabled interfaces


    eth6_br         8000.00e0ed1861ae          no         eth6


                                                          vnet0


                                                          vnet2
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    [root@localhost ~]#
```

在前面的示例中，这两个虚拟接口派生自 eth6_br，并表示为 vnet0 和 vnet2。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

必须启用混杂模式才能使以下功能正常工作：

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

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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            collisions:0 txqueuelen:1000

            RX bytes:14330008 (14.3 MB)  TX bytes:1019416071 (1.0 GB)



[root@localhost ~]#
```

所需模块

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 vhost_net 模块是否存在，请在 Linux 主机上运行以下命令：

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

如果 vhost_net 尚未运行，请输入以下命令来运行它：

```
modprobe vhost\_net
```

使用 OpenStack 预置 NetScaler VPX 实例

您可以使用 **Nova boot** 命令 (OpenStack CLI) 或 Horizon (OpenStack 控制面板) 在 OpenStack 环境中预置 NetScaler VPX 实例。

预置 VPX 实例时，可以选择使用配置驱动器中的数据。配置驱动器是一种特殊的配置驱动器，在实例启动时作为 CD-ROM 设备附加到实例。此配置驱动器可用于传递网络配置，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 环境中的 NetScaler VPX 实例支持 SSH 密钥对身份验证机制。

在使用公钥加密机制之前，会生成密钥对（公钥和私钥）。您可以使用不同的机制来生成密钥对，例如 Horizon、适用于 Windows 的 Puttygen.exe 以及适用于 Linux 环境的 `ssh-keygen`。有关生成密钥对的更多信息，请参阅相应机制的在线文档。

密钥对可用后，将私钥复制到授权人员可以访问的安全位置。在 OpenStack 中，可以使用 Horizon 或 Nova boot 命令将公钥部署到 VPX 实例上。当使用 OpenStack 预置 VPX 实例时，它首先通过读取特定的 BIOS 字符串来检测实例是否在 OpenStack 环境中启动。此字符串为“OpenStack Foundation”，对于 Red Hat Linux 发行版，它存储在 /etc/nova/release 中。这是所有基于 KVM 虚

© 1997–2026 Citrix Systems, Inc. All rights reserved.

拟机管理程序平台的 OpenStack 实现中都可用的标准机制。该驱动器必须具有特定的 OpenStack 标签。

如果检测到配置驱动器，实例将尝试读取网络配置、自定义脚本以及（如果提供）SSH 密钥对。

用户数据文件

NetScaler VPX 实例使用自定义的 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。以下是自定义 OVF 文件的一个示例。

```
```

<?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-
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.
```

```
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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                <BootScript>after</BootScript>

                 <Text>

                      #!/bin/python

print("Hello");

                 </Text>

          </Script>

  <Script>

                <Type>perl</Type>

                <BootScript>before</BootScript>

                 <Text>

                      !/usr/bin/perl

my $name = "VPX";

print "Hello, World $name !\n" ;

                 </Text>

          </Script>

          <Script>

               <Type>nscli</Type>

               <BootScript>after</BootScript>

               <Text>

                add vlan 33

bind vlan 33 -ifnum 1/2

               </Text>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            </Script>

          </Scripts>

      </ScriptSettingSection>

  </cs:ScriptSection>

 </Environment>

 ```
```

在 OVF 文件中，前面的“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。每个脚本标签具有以下字段/标签：

a) \<Type\>: 指定脚本类型的值。可能的值：Shell/Perl/Python/NSLCI（用于 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。此标签的可能值：before/after。“before”指定脚本在 PE 启动之前运行。“after”指定脚本在 PE 启动之后运行。

d) \<Text\>: 粘贴脚本内容。

注意：

目前，VPX 实例不负责脚本的清理。作为管理员，您必须检查脚本的有效性。

并非所有部分都必须存在。使用空的“PropertySection”仅定义在首次启动时运行的脚本，或使用空的 \<cs:ScriptSection\> 仅定义网络配置。
填充 OVF 文件（用户数据文件）的所需部分后，使用该文件预置 VPX 实例。

网络配置

作为网络配置的一部分，VPX 实例读取以下内容：

- 管理 IP 地址
- 网络掩码

© 1997–2026 Citrix Systems, Inc. All rights reserved.
```

- 默认网关

参数成功读取后，它们将填充到 NetScaler® 配置中，以允许远程管理实例。如果参数未成功读取或配置驱动器不可用，则实例将转换为默认行为，即：

- 实例尝试从 DHCP 检索 IP 地址信息。
- 如果 DHCP 失败或超时，实例将使用默认网络配置 (192.168.100.1/16) 启动。

客户脚本

VPX 实例允许在初始预置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一部分的公钥复制到其“authorized_keys”文件中。这允许用户使用私钥访问实例。

注意：

当提供 SSH 密钥时，默认凭据 (nsroot/nsroot) 将不再有效。如果需要基于密码的访问，请使用相应的 SSH 私钥登录并手动设置密码。

开始之前

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

一个 OpenStack 镜像，该镜像来自 qcow2 镜像。请按照以下步骤操作：

1. 通过键入以下命令从 `.tqz` 文件中提取 `.qcow2` 文件

   ```
   tar xvzf &lt;TAR file>

   tar xvzf &lt;NSVPX-KVM-12.0-26.2_nc.tgz>

   NSVPX-KVM.xml

   NSVPX-KVM-12.0-26.2_nc.qcow2
   ```

2. 通过键入以下命令，使用在步骤 1 中提取的 `.qcoz2` 文件构建 OpenStack 镜像。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
openstack image create --container-format bare --property
hw_disk_bus=ide --disk-format qcow2 --file &lt;path to qcow2 file> --
public &lt;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                                                |
+------------------+-------------------------------------------------------+
```

预置 VPX 实例

您可以通过以下两种方式之一预置 VPX 实例：

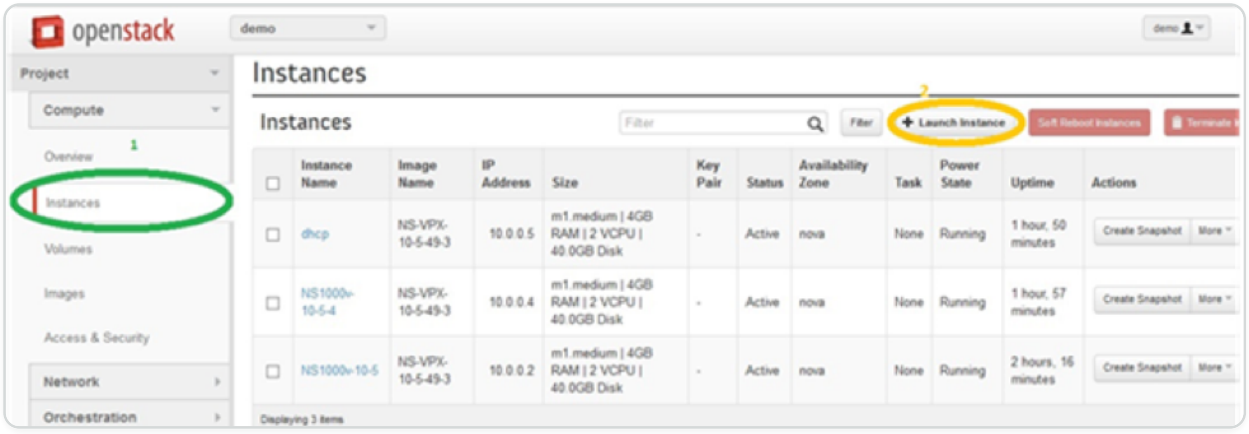
- Horizon (OpenStack 控制面板)
- Nova 启动命令 (OpenStack CLI)

使用 OpenStack 控制面板预置 VPX 实例

请按照以下步骤使用 Horizon 预置 VPX 实例：

1. 登录 OpenStack 控制面板。
2. 在控制面板左侧的“项目”面板中，选择 **实例**。
3. 在“实例”面板中，单击 **启动实例** 以打开实例启动向导。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 在“启动实例”向导中，填写详细信息，例如：

   a. 实例名称

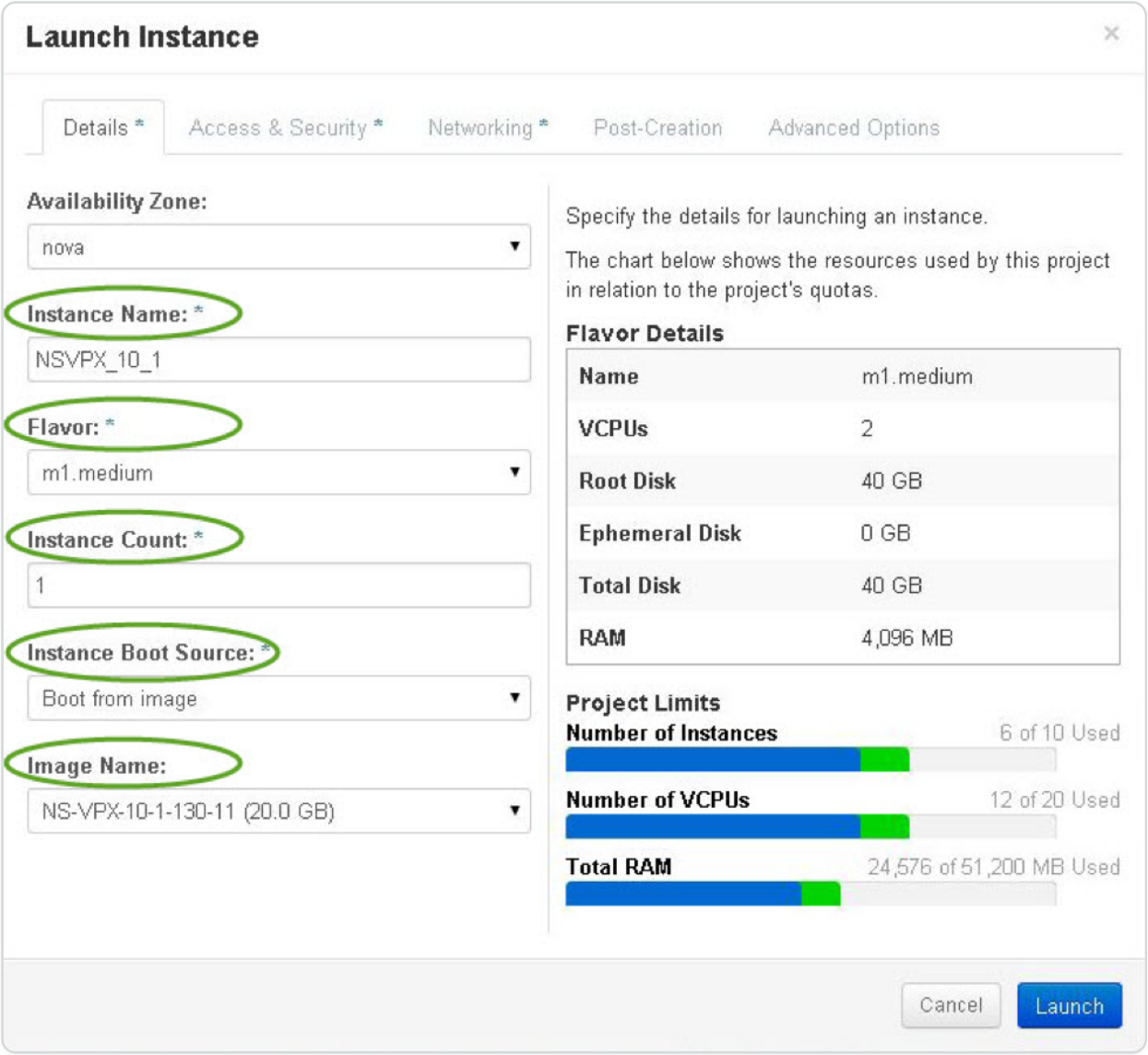
   b. 实例类型

   c. 实例数量

   d. 实例启动源

   e. 映像名称

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 通过完成以下步骤，通过 Horizon 部署新的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) 复制公钥内容。

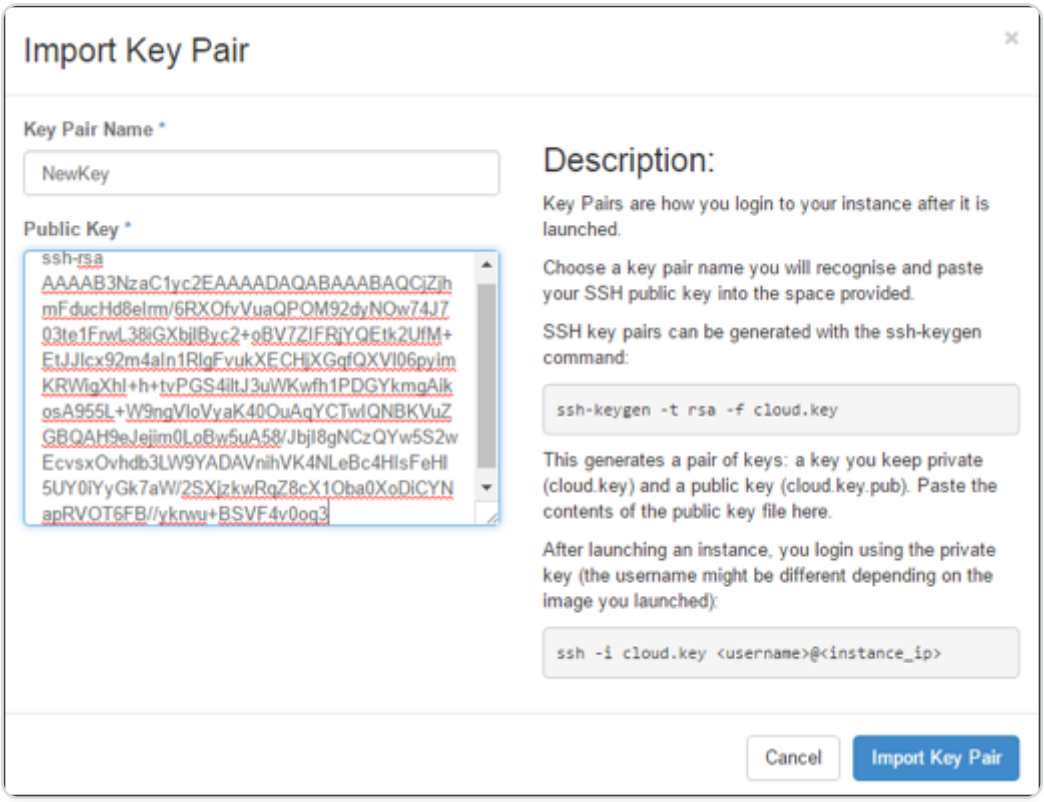
   c) 转到 **Horizon > 实例 > 创建新实例**。

   d) 单击**访问与安全**。

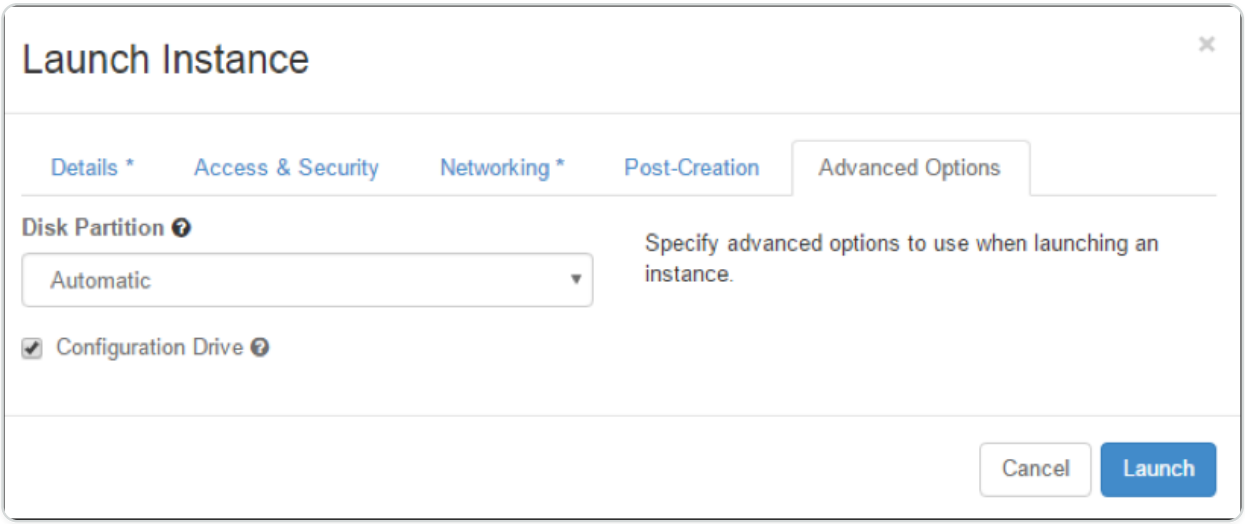
   e) 单击**密钥对**下拉菜单旁边的 + 号，并为显示的参数提供值。

   f) 将公钥内容粘贴到*公钥*框中，为密钥命名，然后单击**导入密钥对**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 在向导中单击**创建后**选项卡。在自定义脚本中，添加用户数据文件的内容。用户数据文件包含 VPX 实例的 IP 地址、子网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 config-drive 选项，然后单击**启动**。



使用 OpenStack CLI 预置 VPX 实例

请按照以下步骤操作，使用 OpenStack CLI 预置 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 要选择用于创建实例的映像，请键入以下命令：

   `openstack image list | more`

3. 要创建特定类型的实例，请键入以下命令从列表中选择类型 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：

```
openstack server create --flavor FLAVOR_ID --image IMAGE_ID --key-name
KEY_NAME

--user-data USER_DATA_FILE_PATH --config-drive True --nic net-id=net-
uuid

INSTANCE_NAME

openstack server create --image VPX-ToT-Image --flavor m1.medium --
user-data

ovf.xml --config-drive True --nic net-id=2734911b-ee2b-48d0-
a1b6-3efd44b761b9

VPX-ToT
```

图 2：以下插图提供了示例输出。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
+-------------------------------------+-----------------------------------------------------------------+
| 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

虚拟机管理器是一个用于管理虚拟机客户机的桌面工具。它使您能够创建新的虚拟机客户机和各种类型的存储，并管理虚拟网络。您可以使用内置的 VNC 查看器访问虚拟机客户机的图形控制台，并查看本地或远程的性能统计信息。

安装您首选的 Linux 发行版并启用 KVM 虚拟化后，您可以继续配置虚拟机。

在使用虚拟机管理器配置 NetScaler VPX 实例时，您有两个选项：

- 手动输入 IP 地址、网关和子网掩码
- 自动分配 IP 地址、网关和子网掩码（自动配置）

您可以使用两种类型的映像来配置 NetScaler VPX 实例：

- RAW
- QCOW2

您可以将 NetScaler VPX RAW 映像转换为 QCOW2 映像并配置 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.qcow2
```

例如：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

KVM 上典型的 NetScaler VPX 部署包括以下步骤：

- 检查自动配置 NetScaler VPX 实例的先决条件
- 使用 RAW 镜像置备 NetScaler VPX 实例
- 使用 QCOW2 镜像置备 NetScaler VPX 实例
- 使用虚拟机管理器向 VPX 实例添加更多接口

检查自动置备 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。如果启用此功能，则在初始设置期间无需输入 NetScaler VPX 实例的管理 IP 地址、网络掩码和默认网关。

在自动置备 VPX 实例之前，您需要完成以下任务：

1. 创建自定义的开放虚拟化格式 (OVF) XML 文件或用户数据文件。
2. 使用在线应用程序（例如 PowerISO）将 OVF 文件转换为 ISO 镜像。
3. 使用任何基于安全复制 (SCP) 的工具将 ISO 镜像挂载到 KVM 主机上。

OVF XML 文件示例：

以下是 OVF XML 文件内容的示例，您可以将其用作创建文件的参考。

```
<?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"`
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

<PlatformSection>

<Kind></Kind>

<Version>2016.1</Version>

<Vendor>VPX</Vendor>

<Locale>en</Locale>

</PlatformSection>

<PropertySection>

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

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

<Property oe:key="com.citrix.netscaler.orch\_env" oe:value="KVM"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"/>

<Property oe:key="com.citrix.netscaler.mgmt.netmask"
oe:value="255.255.255.0"/>

<Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="10.1.2.1"/>

</PropertySection>

</Environment>
```

在前面的 OVF XML 文件中，“PropertySection”用于 NetScaler® 网络配置。创建文件时，请为示例末尾突出显示的参数指定值：

- 管理 IP 地址
- 子网掩码
- 网关

重要提示：

如果 OVF 文件未正确格式化为 XML，则 VPX 实例将分配默认网络配置，而不是文件中指定的值。

使用 RAW 镜像配置 NetScaler VPX 实例

虚拟机管理器使您能够使用 RAW 镜像配置 NetScaler VPX 实例。

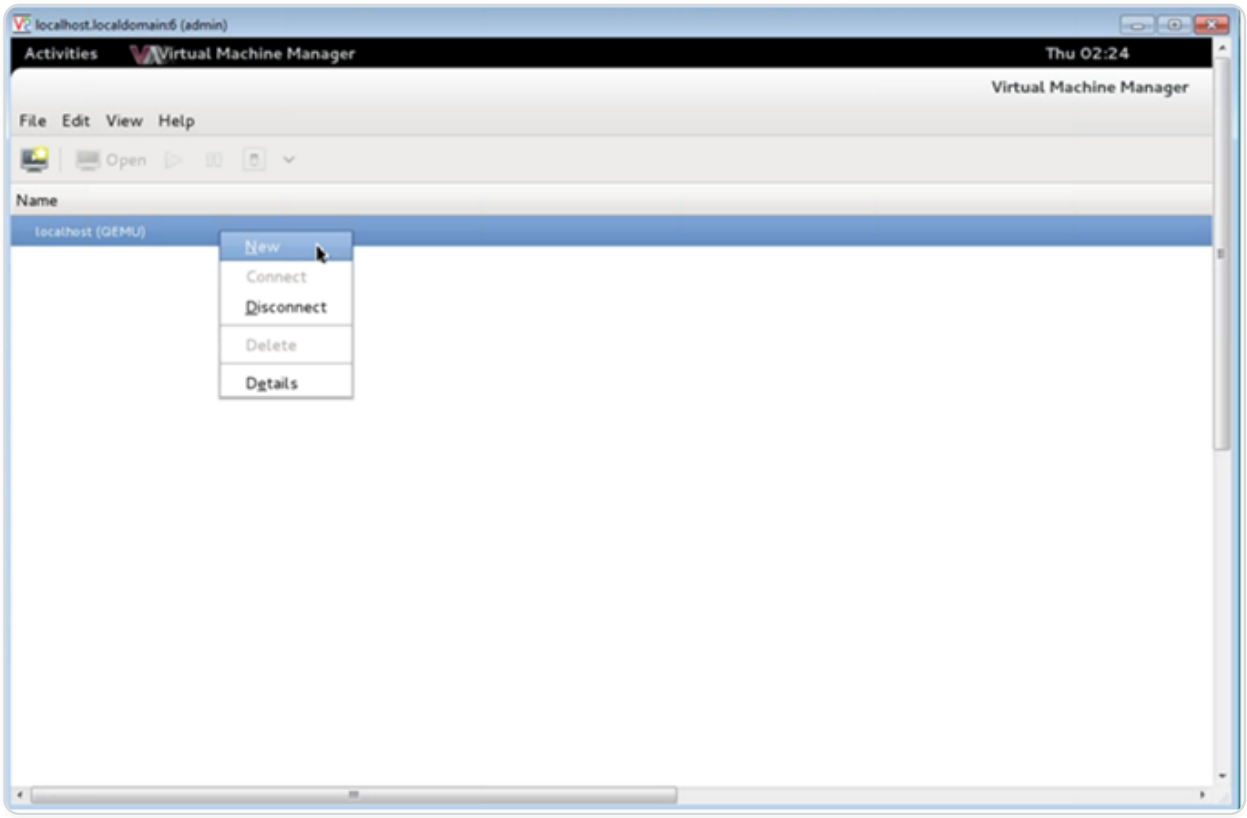
要使用虚拟机管理器配置 NetScaler VPX 实例，请按照以下步骤操作：

1. 打开虚拟机管理器（**应用程序** > **系统工具** > **虚拟机管理器**），并在 **Authenticate** 窗口中输入登录凭据。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

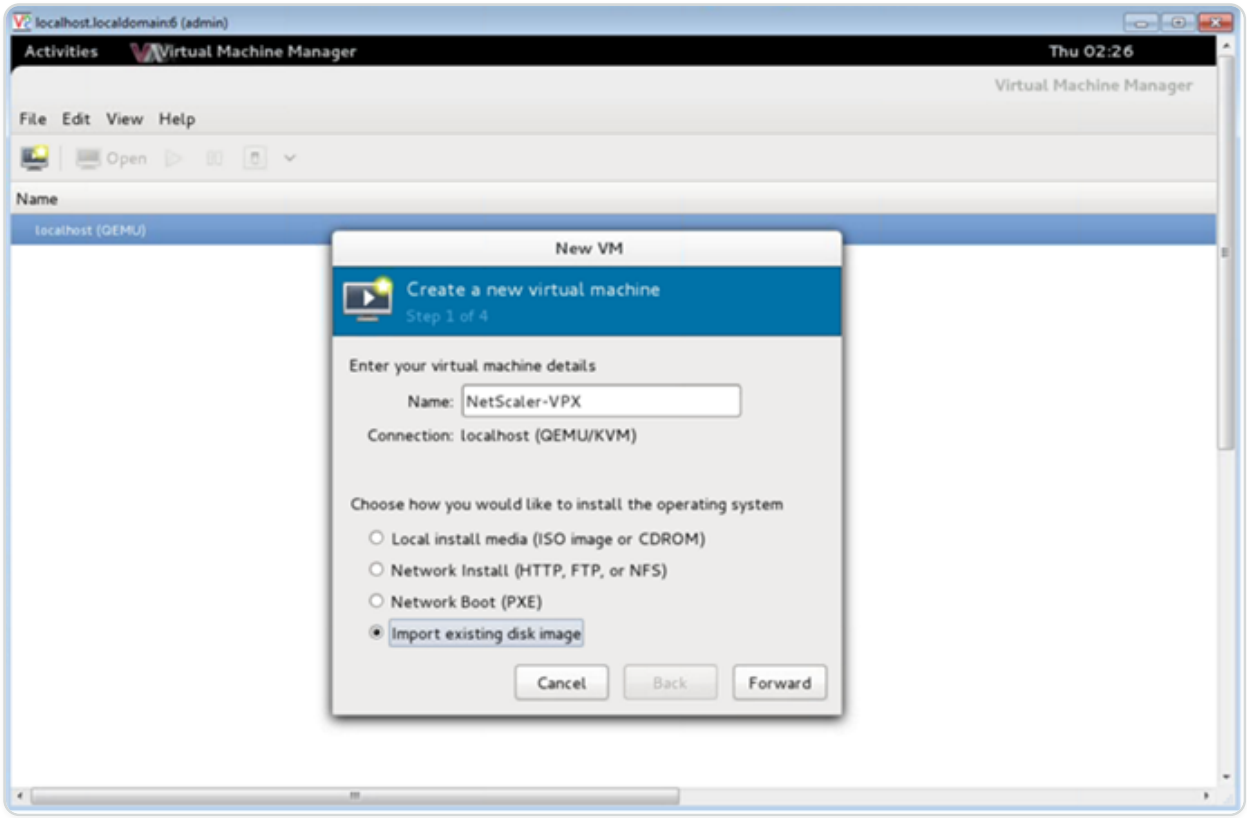
2. 单击

图标或右键单击 **localhost (QEMU)** 以创建新的 NetScaler VPX 实例。

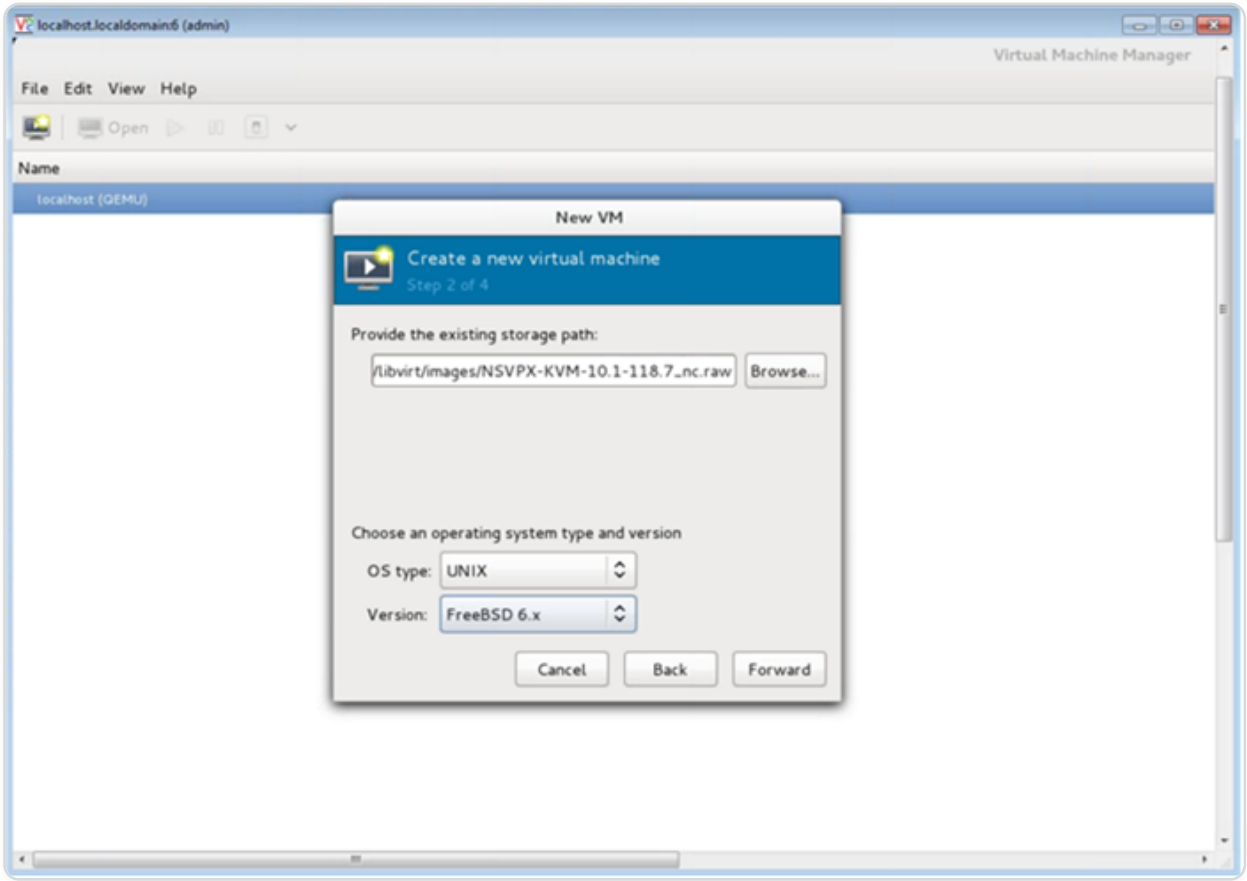


3. 在 **Name** 文本框中，输入新 VM 的名称（例如，NetScaler-VPX）。
4. 在 **New VM** 窗口中，在“选择安装操作系统的方式”下，选择 **Import existing disk image**，然后单击 **Forward**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



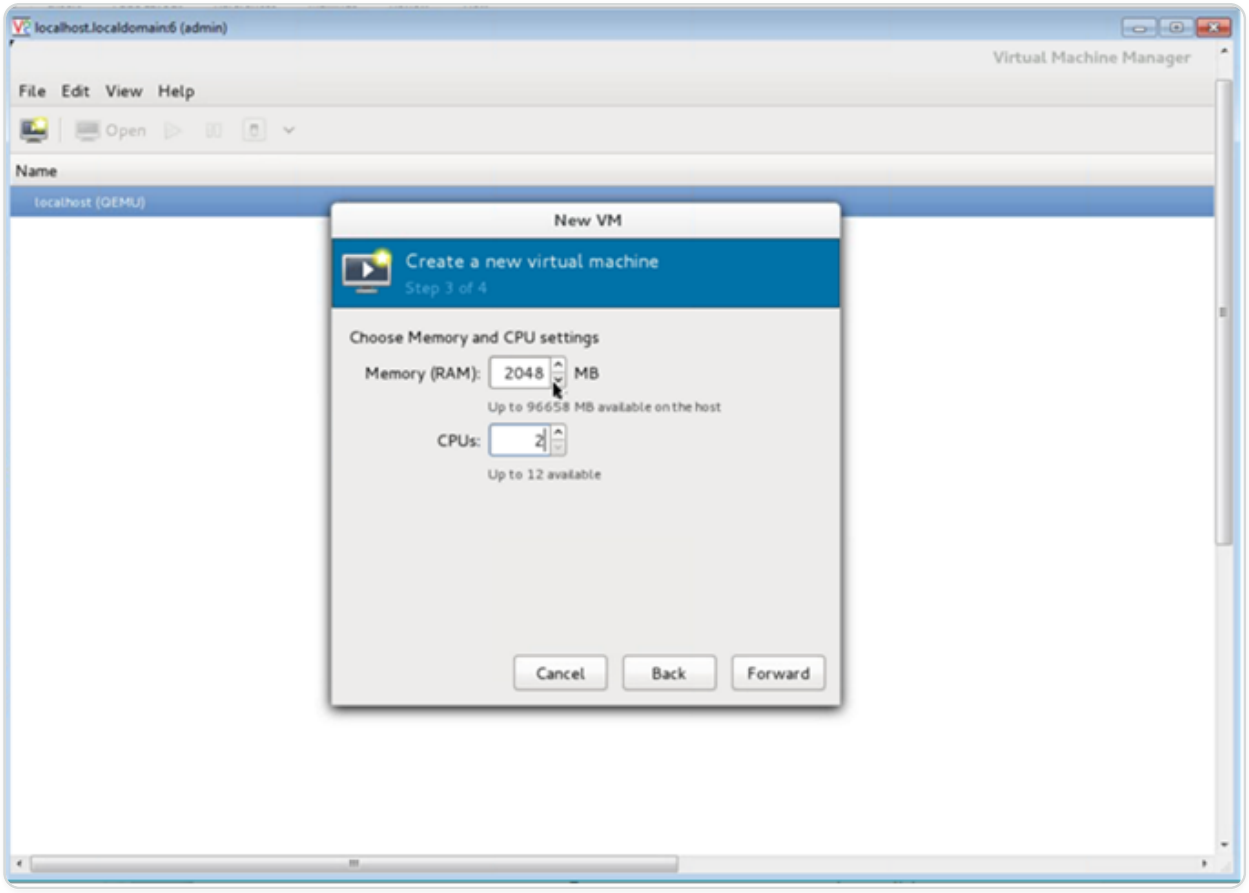
5. 在 **Provide the existing storage path** 字段中，导航到镜像路径。选择操作系统类型为 UNIX，版本为 FreeBSD 6.x。然后，单击 **Forward**。



6. 在 **Choose Memory and CPU** 设置下，选择以下设置，然后单击 **Forward**：

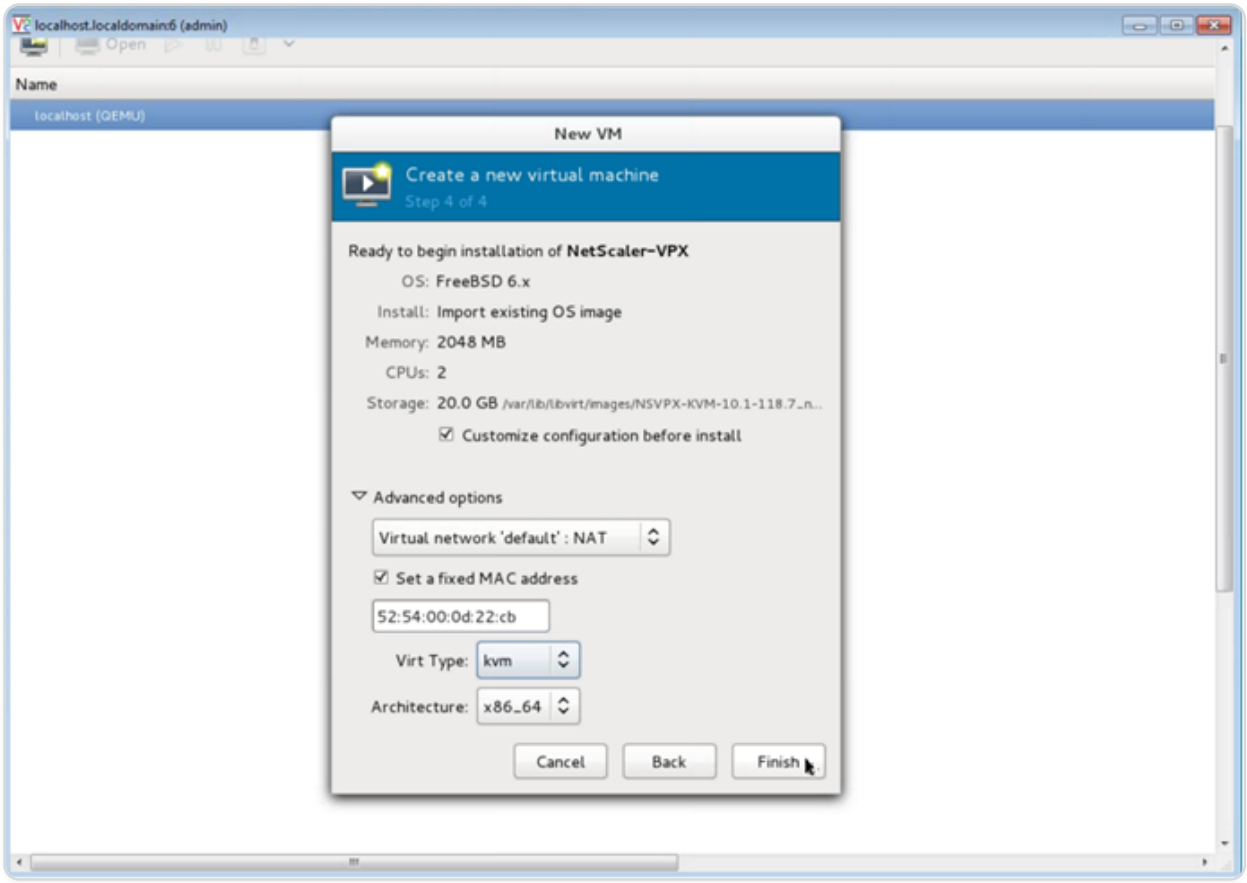
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 内存 (RAM)— 2048 MB
- CPU — 2



7. 选中**安装前自定义配置**复选框。可选地，在**高级选项**下，您可以自定义MAC地址。确保选择的**虚拟类型**是KVM，并且选择的架构是x86_64。点击**完成**。

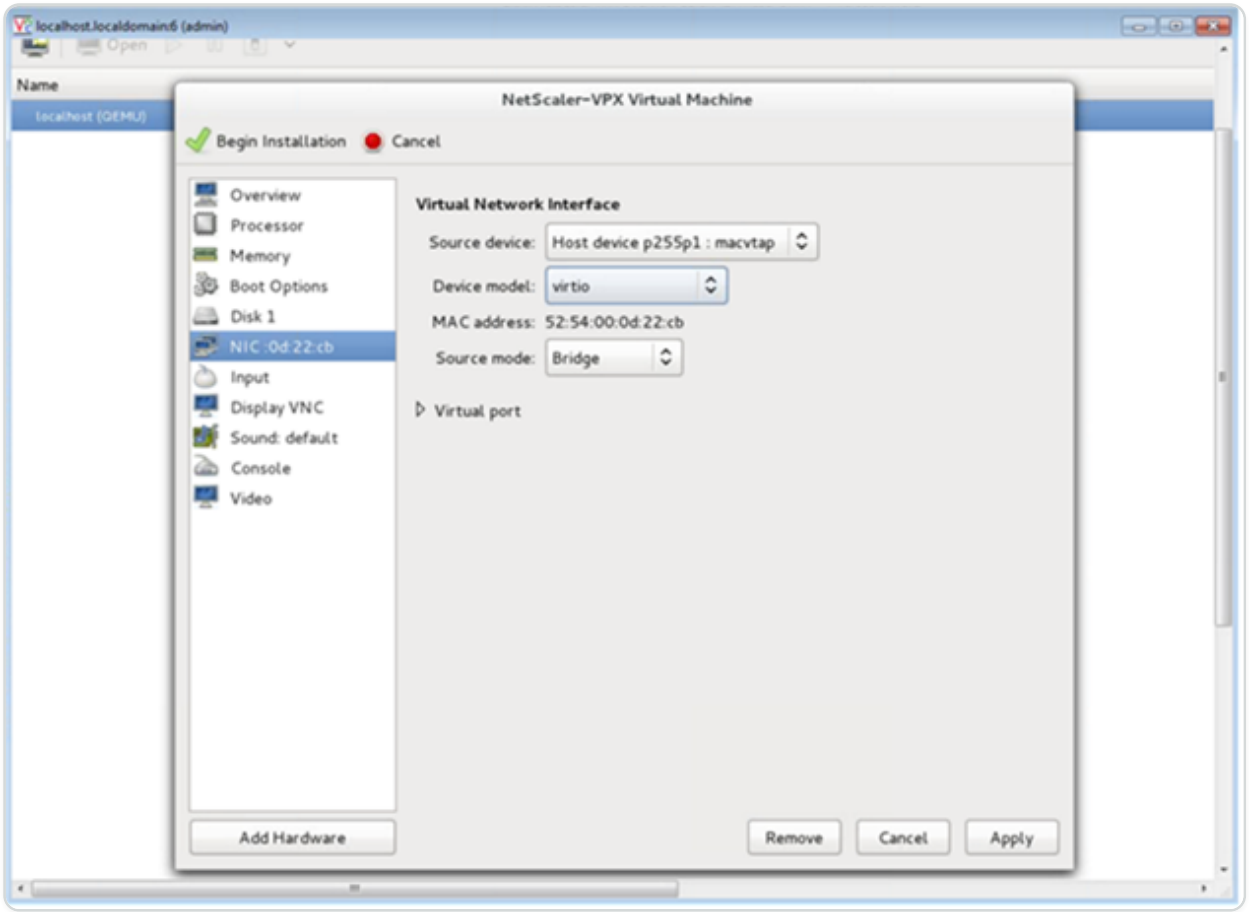
© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. 选择一个网卡并提供以下配置：

   - 源设备 — `ethX macvtap` 或桥接
   - 设备模型 — `virtio`
   - 源模式 — 桥接

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. 点击**应用**。
10. 如果您想自动配置VPX实例，请参阅本文档中的**通过连接CDROM驱动器启用自动配置**部分。否则，点击**开始安装**。在KVM上配置NetScaler VPX后，您可以添加更多接口。

使用QCOW2镜像配置NetScaler VPX实例

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

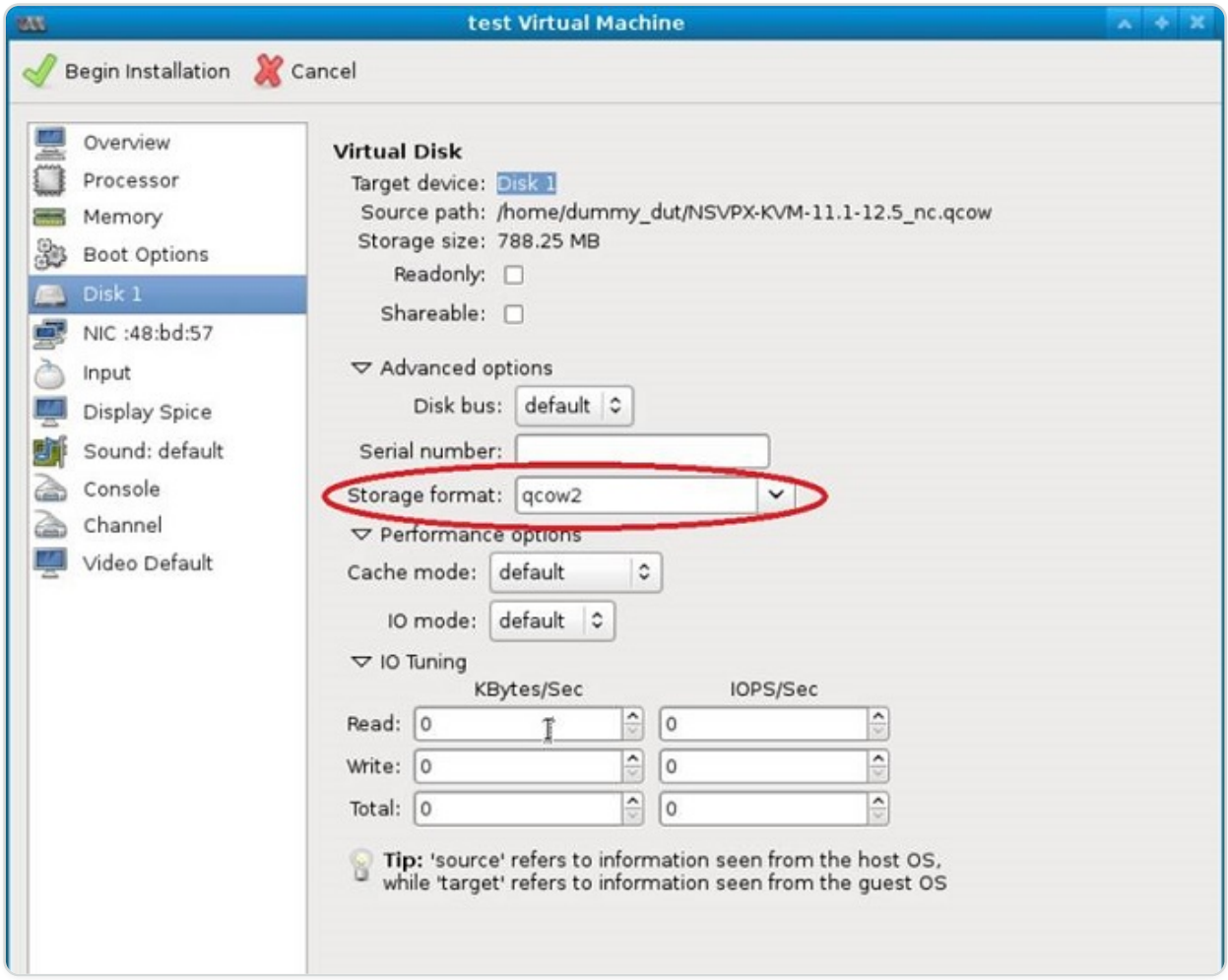
要使用QCOW2镜像配置NetScaler VPX实例，请按照以下步骤操作：

1. 请遵循使用RAW镜像配置NetScaler VPX实例中的**步骤1**到**步骤8**。

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

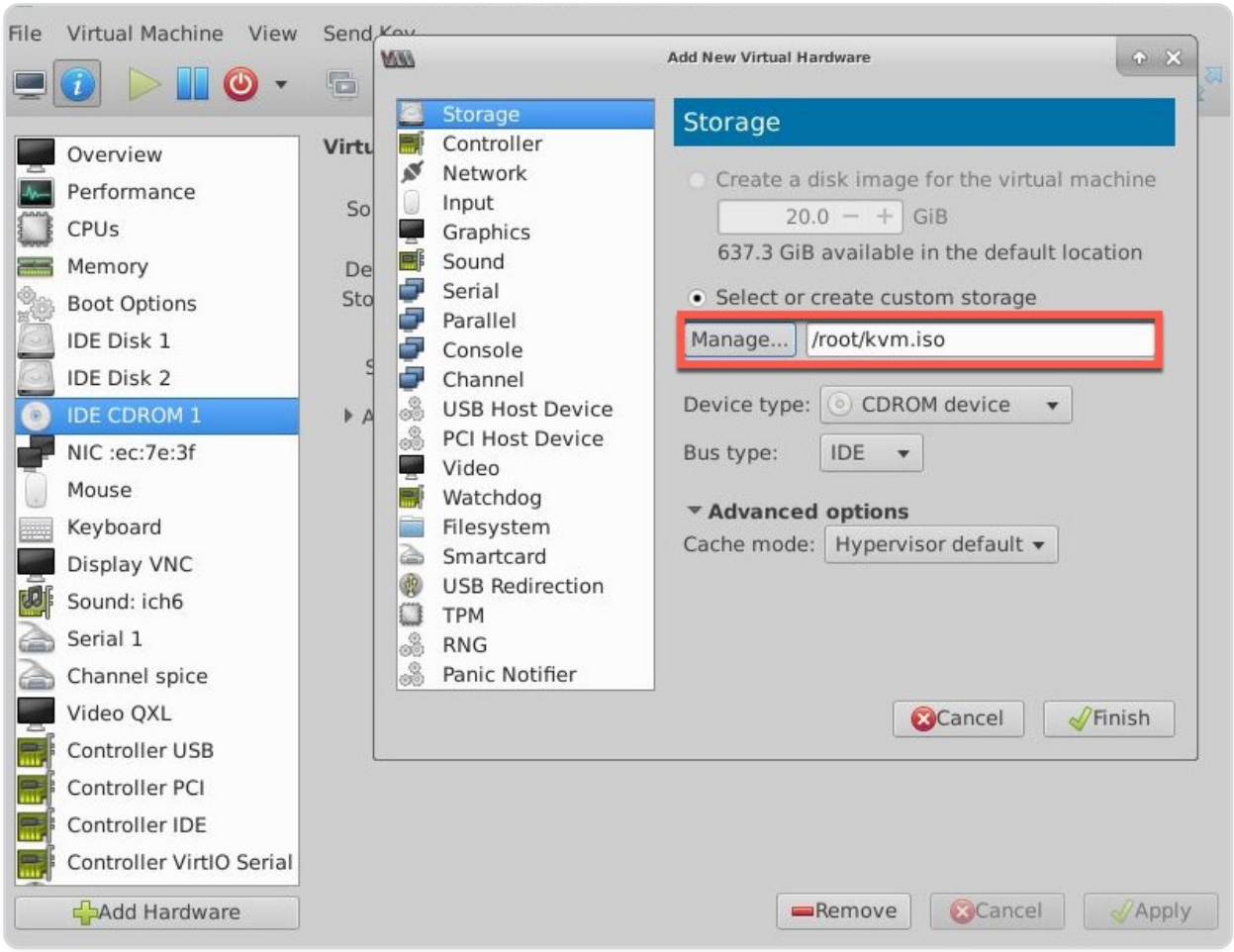


4. 单击 **Apply**（应用），然后单击 **Begin Installation**（开始安装）。在 KVM 上预配 NetScaler VPX 后，您可以添加更多接口。

通过连接 CDROM 驱动器启用自动预配

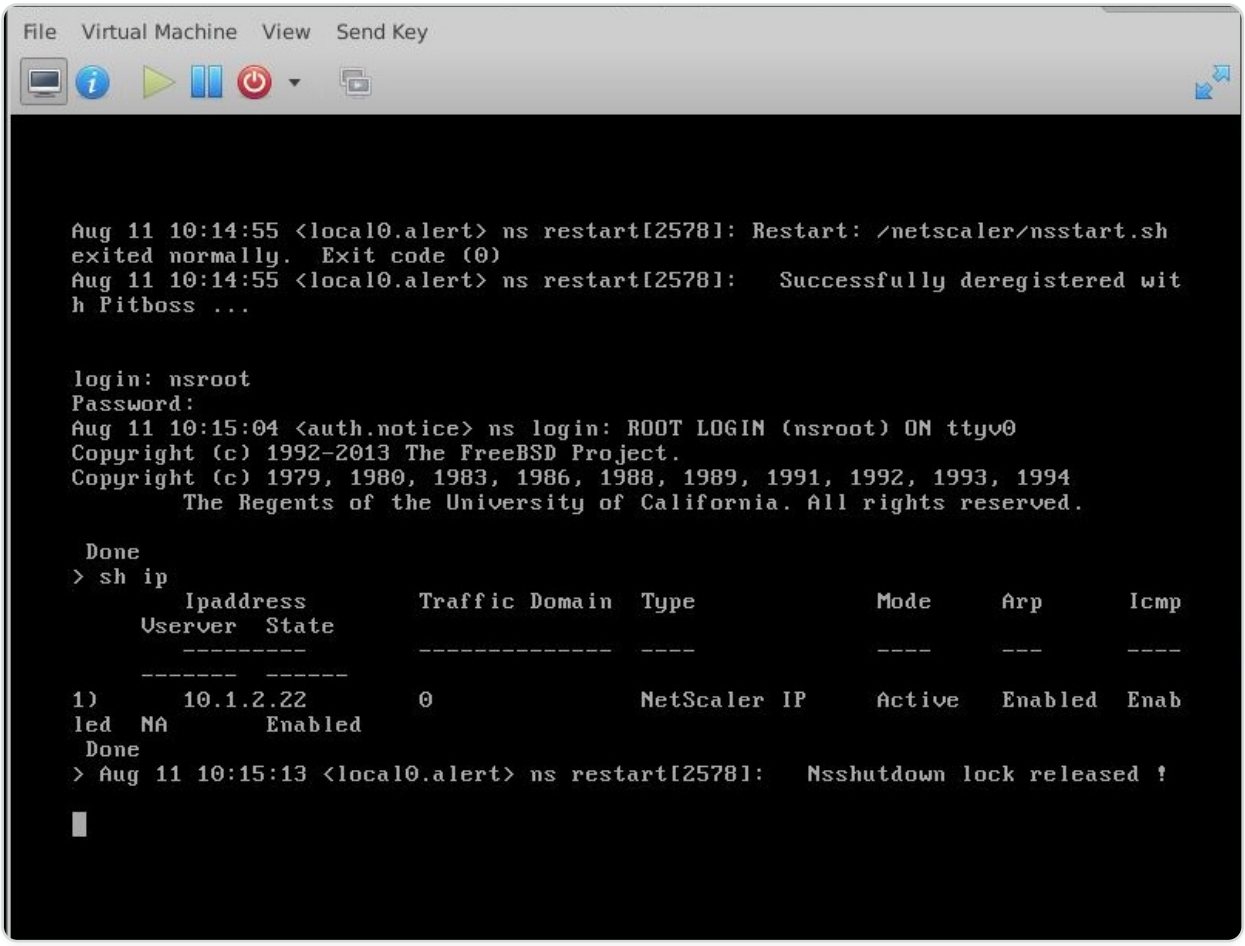
1. 单击 **Add Hardware > Storage > Device type > CDROM device**（添加硬件 > 存储 > 设备类型 > CDROM 设备）。
2. 单击 **Manage**（管理），然后选择在“自动预配 NetScaler VPX 实例的先决条件”部分中装载的正确 ISO 文件，然后单击 **Finish**（完成）。您的 NetScaler VPX 实例的“Resources”（资源）下将创建一个新的 CDROM。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 启动 VPX 实例，它将使用 OVF 文件中提供的网络配置进行自动预配，如示例屏幕截图所示。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 如果自动预配失败，实例将使用默认 IP 地址 (192.168.100.1) 启动。在这种情况下，您必须手动完成初始配置。有关详细信息，请参阅首次配置 ADC。

使用虚拟机管理器向 NetScaler VPX 实例添加更多接口

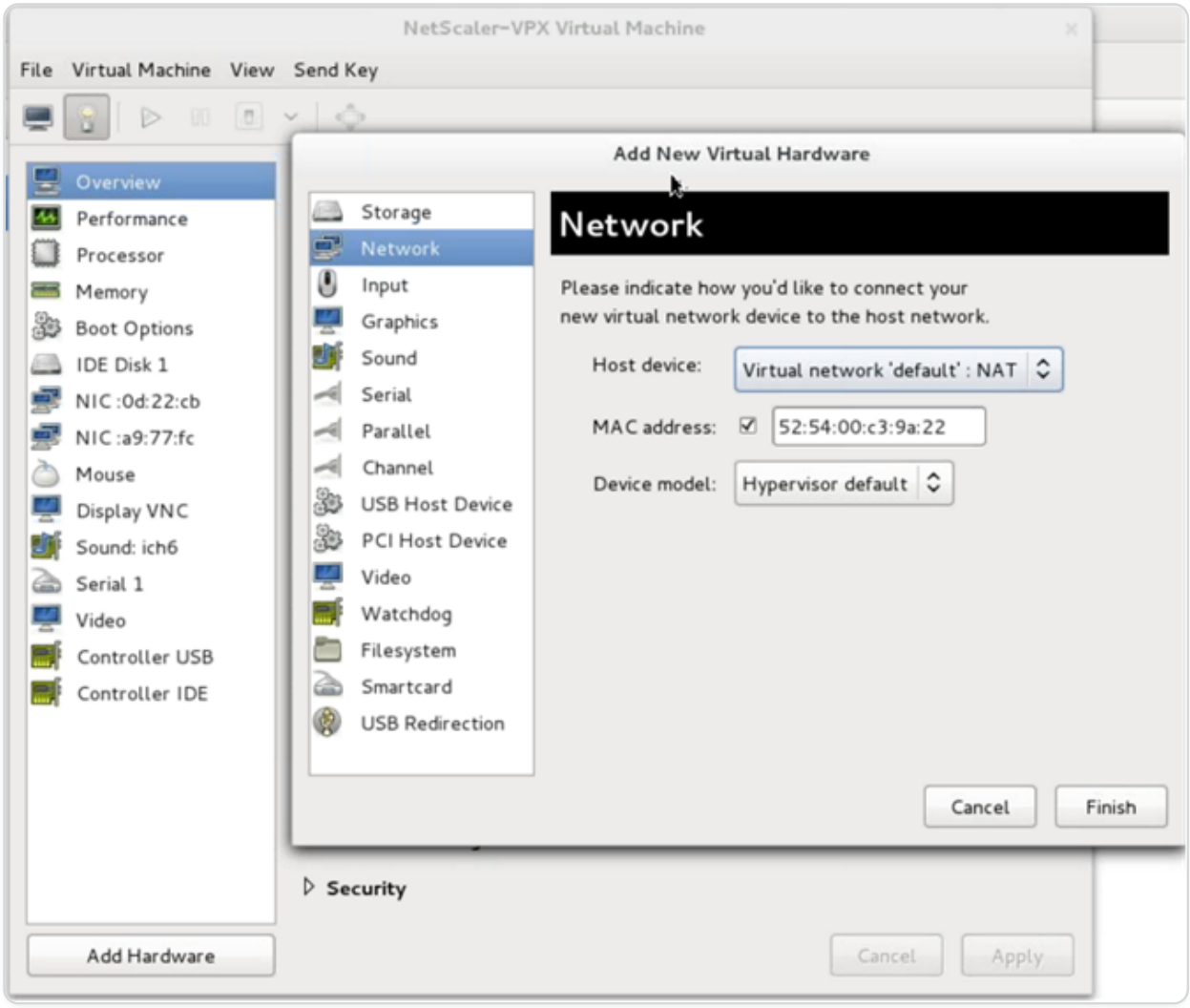
在 KVM 上预配 NetScaler VPX™ 实例后，您可以添加更多接口。

要添加更多接口，请按照以下步骤操作。

1. 关闭在 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**打开**。
3. 单击标题中的

   图标以查看虚拟硬件详细信息。
4. 单击**添加硬件**。在**添加新虚拟硬件窗口**中，从导航菜单中选择**网络**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 在**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 或 MacVTap。如果是 MacVTap，则有四种可能的模式：VEPA、Bridge、Private 和 Pass-through。

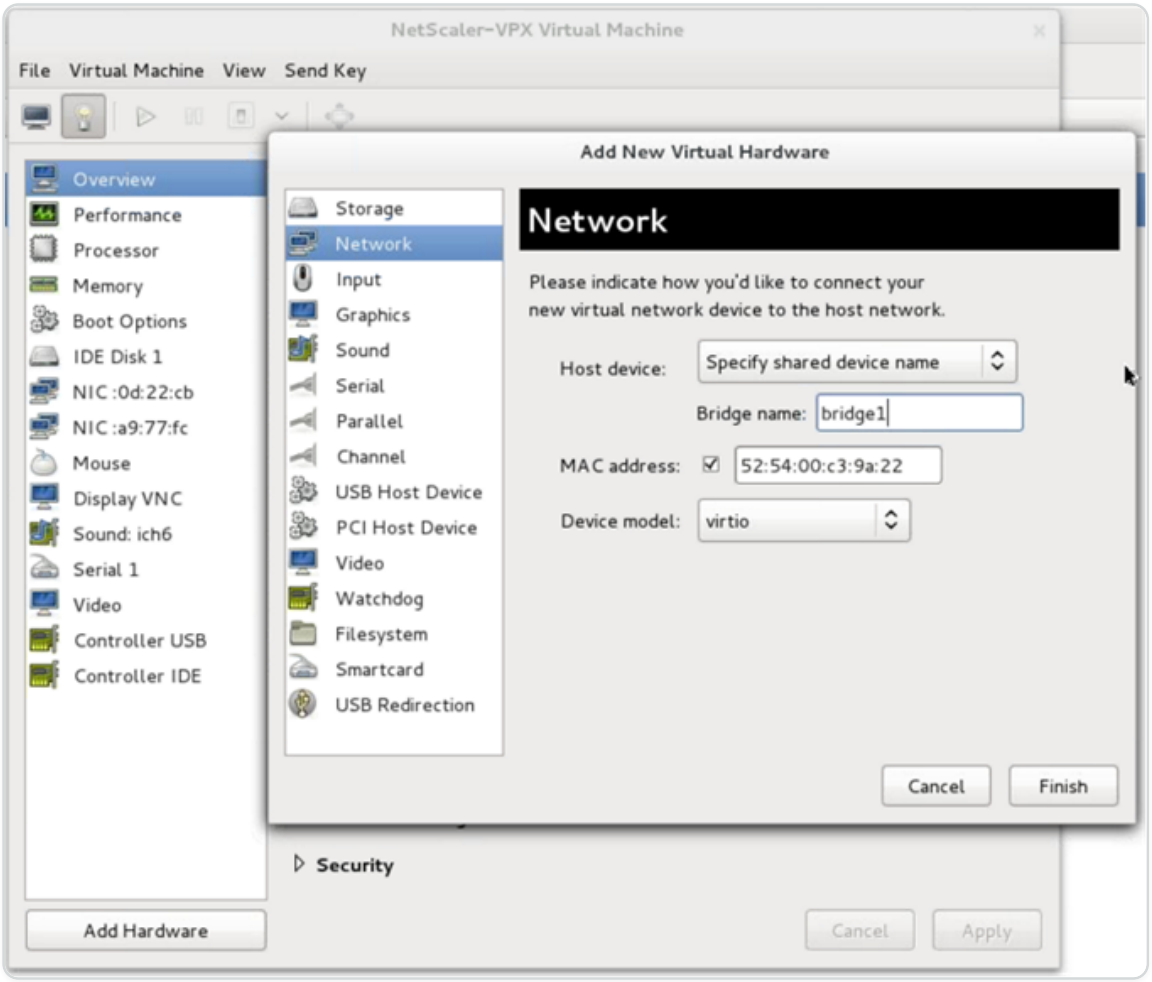
   a. 对于 Bridge

      i. 主机设备 — 选择“指定共享设备名称”选项。

      ii. 提供在 KVM 主机中配置的 Bridge 名称。

> **注意：**
>
> 确保您已在 KVM 主机中配置了 Linux bridge，将物理接口绑定到该 bridge，并将该 bridge 置于 UP 状态。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



iii. 设备型号—`virtio`。

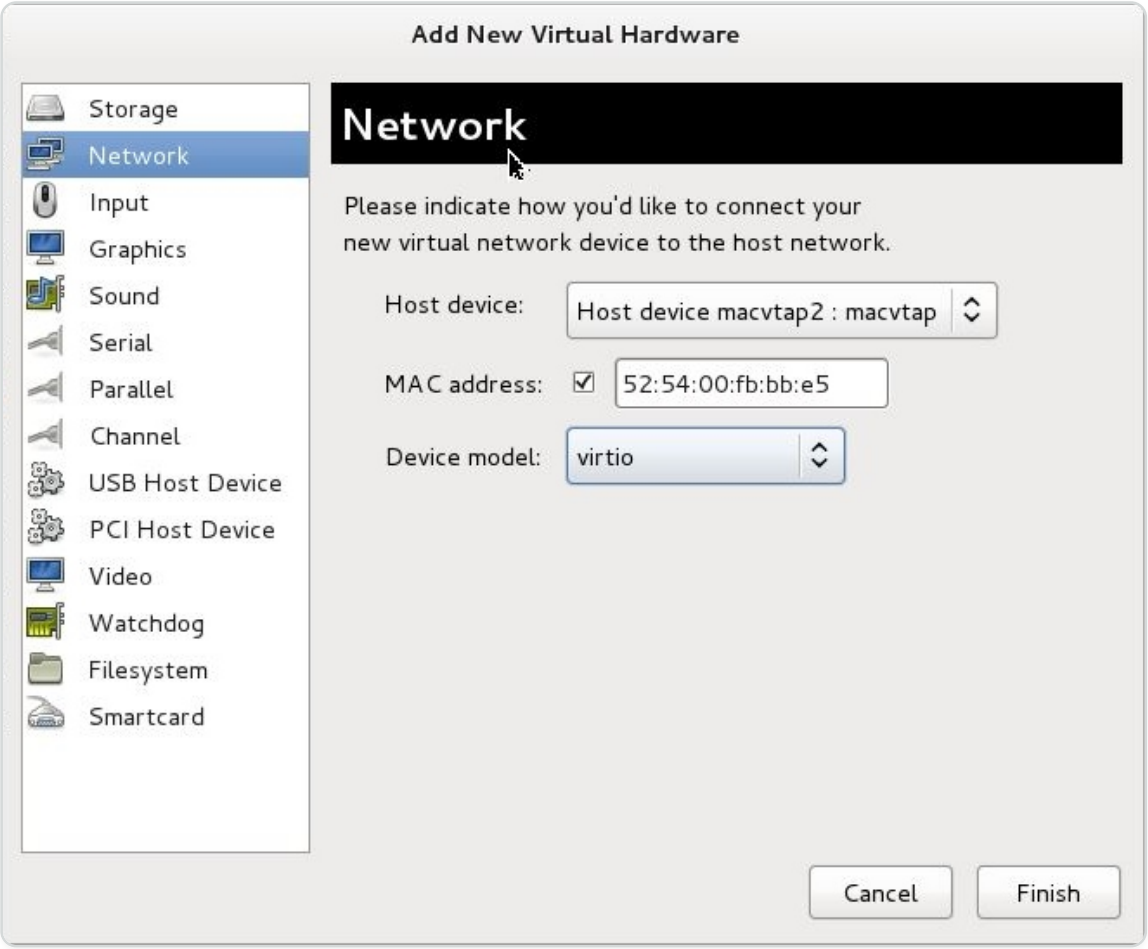
iv. 单击**完成**。

b. 对于 MacVTap

i. 主机设备—从菜单中选择物理接口。

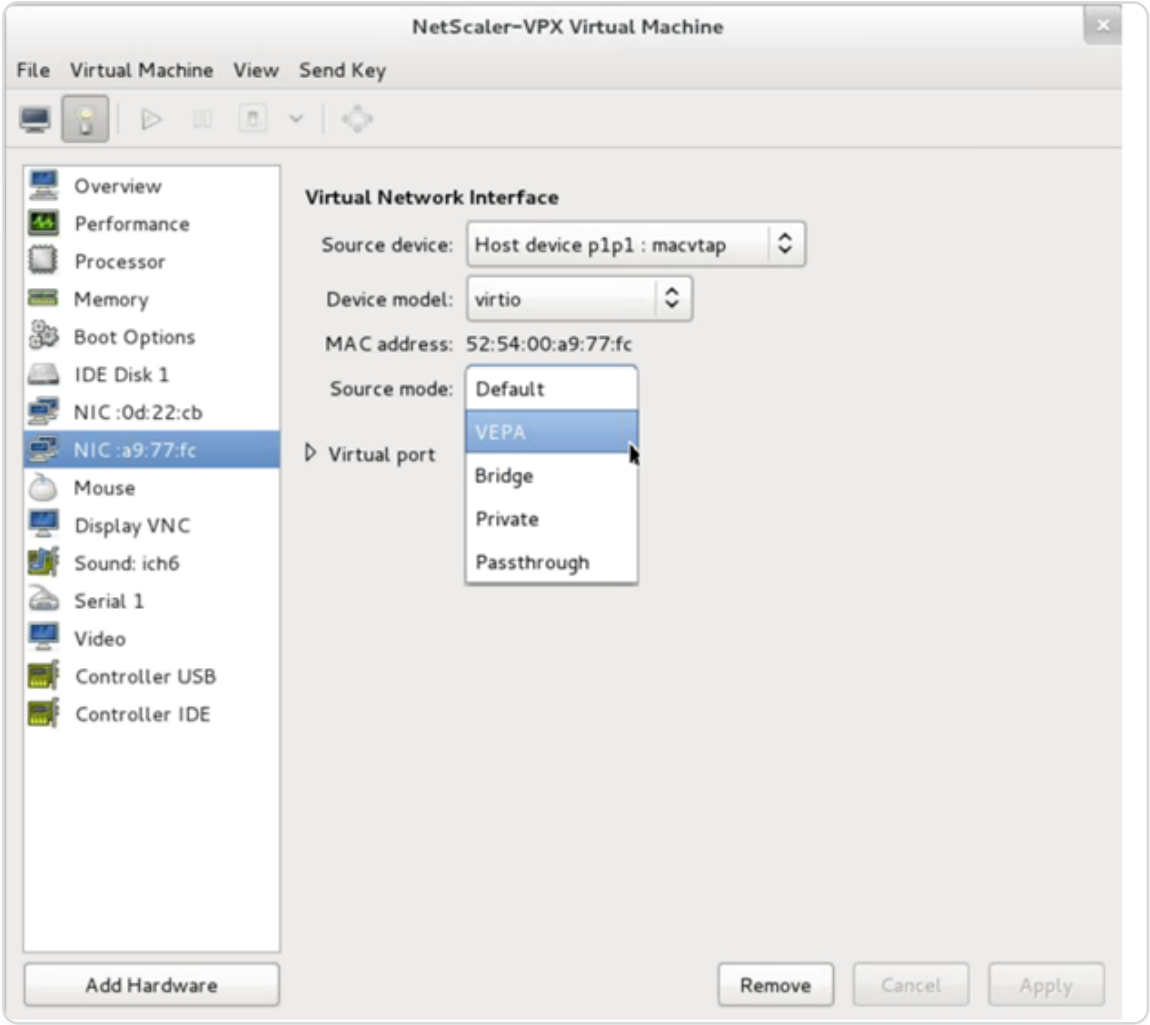
ii. 设备型号—`virtio`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



iii. 单击 **完成**。您可以在导航窗格中查看新添加的 NIC。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



iv. 选择新添加的 NIC 并选择此 NIC 的源模式。可用模式包括 VEPA、Bridge、Private 和 Passthrough。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. 如果要自动预配 VPX 实例，请参阅本文档中的“添加配置驱动器以启用自动预配”部分。否则，请启动 VPX 实例以手动完成初始配置。

重要提示：

接口参数配置（例如速度、双工和自动协商）不受支持。

配置 NetScaler VPX 实例以使用 SR-IOV 网络接口

您可以使用以下网卡，在 Linux-KVM 平台上配置运行单根 I/O 虚拟化 (SR-IOV) 的 NetScaler VPX 实例：

- 英特尔 82599 10G
- 英特尔 X710 10G

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 英特尔 XL710 40G
- 英特尔 X722 10G

本节介绍如何：

- 配置 NetScaler VPX 实例以使用 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

使用英特尔 82599、X710、XL710 和 X722 网卡时，请记住以下限制。不支持以下功能。

英特尔 82599 网卡的限制：

- 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。
- 通过 `ip link` 命令在管理程序上为 SRIOV VF 接口配置 VLAN 不受支持。
- 不支持接口参数配置，例如速度、双工和自动协商。

Intel X710 10G、Intel XL710 40G 和 Intel X722 10G 网卡的限制：

- L2 模式切换。
- 管理分区（共享 VLAN 模式）。
- 在群集中，当 XL710 网卡用作数据接口时，不支持巨型帧。
- 当接口断开连接并重新连接时，接口列表会重新排序。
- 不支持接口参数配置，例如速度、双工和自动协商。
- 对于 Intel X710 10G、Intel XL710 40G 和 Intel X722 10G 网卡，接口名称为 40/X
- VPX 实例最多支持 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 网卡支持 IPv6，您需要在 KVM 主机上键入以下命令以在虚拟功能 (VF) 上启用信任模式：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

示例：

`# ip link set ens785f1 vf 0 trust on`

先决条件

在配置 NetScaler VPX 实例以使用 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“网卡”列。

任务	INTEL 82599 网卡	INTEL X710、XL710 和 X722 网卡
1. 将网卡添加到 KVM 主机。	-	-
1. 下载并安装最新的 Intel 驱动程序。	IXGBE 驱动程序	I40E 驱动程序
1. 在 KVM 主机上将驱动程序列入黑名单。	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（推荐）。	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（推荐）。
4.在 KVM 主机上启用 SR-IOV 虚拟功能 (VF)。在接下来的两列命令中： `number_of_VFs` = 您要创建的虚拟 VF 数量。 `device_name` = 接口名称。	如果您使用的是 kernel 3.8 之前的版本，请将以下条目添加到 /etc/modprobe.d/ixgbe 文件并重新启动 KVM 主机：`options ixgbe max_vfs=<number_of_VFs>`。如果您使用的是 kernel 3.8 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`。请参见图 1 中的示例。	如果您使用的是 kernel 3.8 之前的版本，请将以下条目添加到 /etc/modprobe.d/i40e.conf 文件并重新启动 KVM 主机：`options i40e max_vfs=<number_of_VFs>`。如果您使用的是 kernel 3.8 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`。请参见图 2 中的示例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

任务	INTEL 82599 网卡	INTEL X710、XL710 和 X722 网卡
1. 通过将用于创建 VF 的命令添加到 rc.local 文件中，使 VF 持久化。	请参见图 3 中的示例。	请参见图 3 中的示例。

重要提示：

创建 SR-IOV VF 时，请确保不要为 VF 分配 MAC 地址。

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

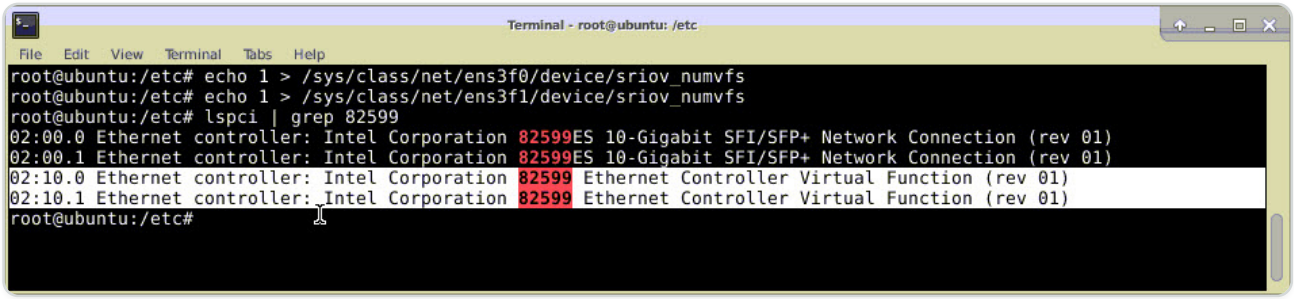


图 2：在 KVM 主机上为 Intel X710 10G 和 XL710 40G NIC 启用 SR-IOV VF。

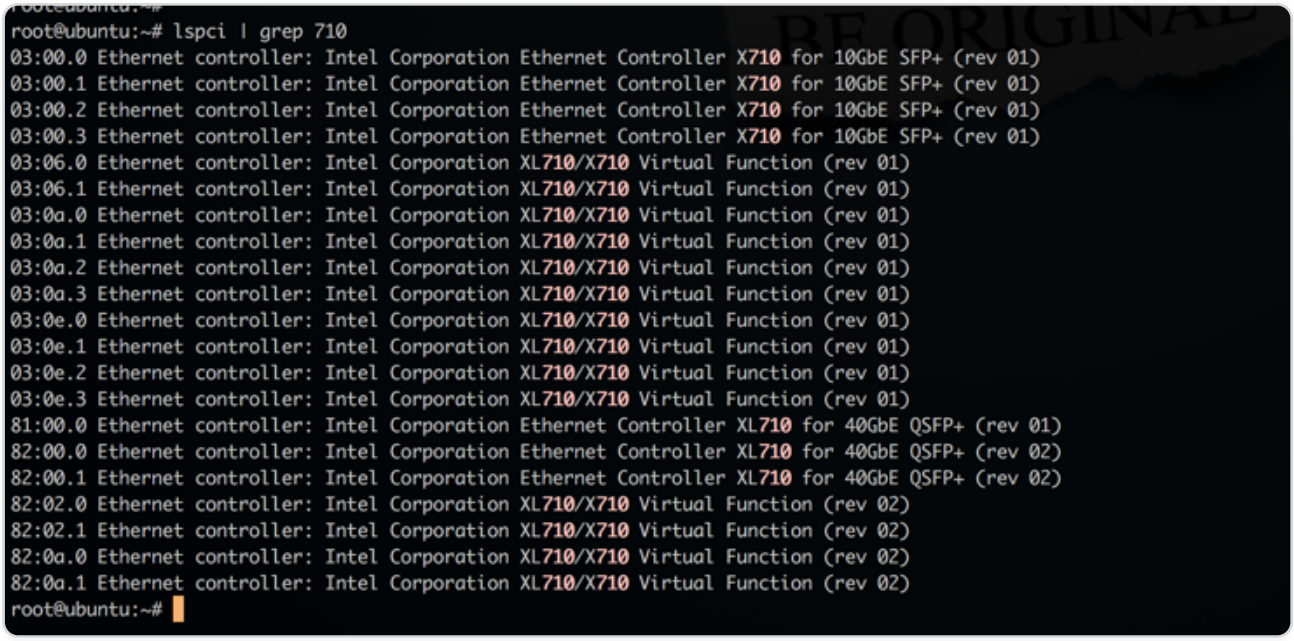


图 3：在 KVM 主机上为 Intel X722 10G NIC 启用 SR-IOV VF。

适用于 X722 的 SR-IOV VF(/en-us/vpx/media/sr-iov-x722-nic.png)

图 4：使 VF 持久化。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SR-IOV VF 持久化(/en-us/vpx/media/enable_sriov_2.jpg)

配置 NetScaler VPX 实例以使用 SR-IOV 网络接口

要使用 Virtual Machine Manager 配置 NetScaler VPX 实例以使用 SR-IOV 网络接口，请完成以下步骤：

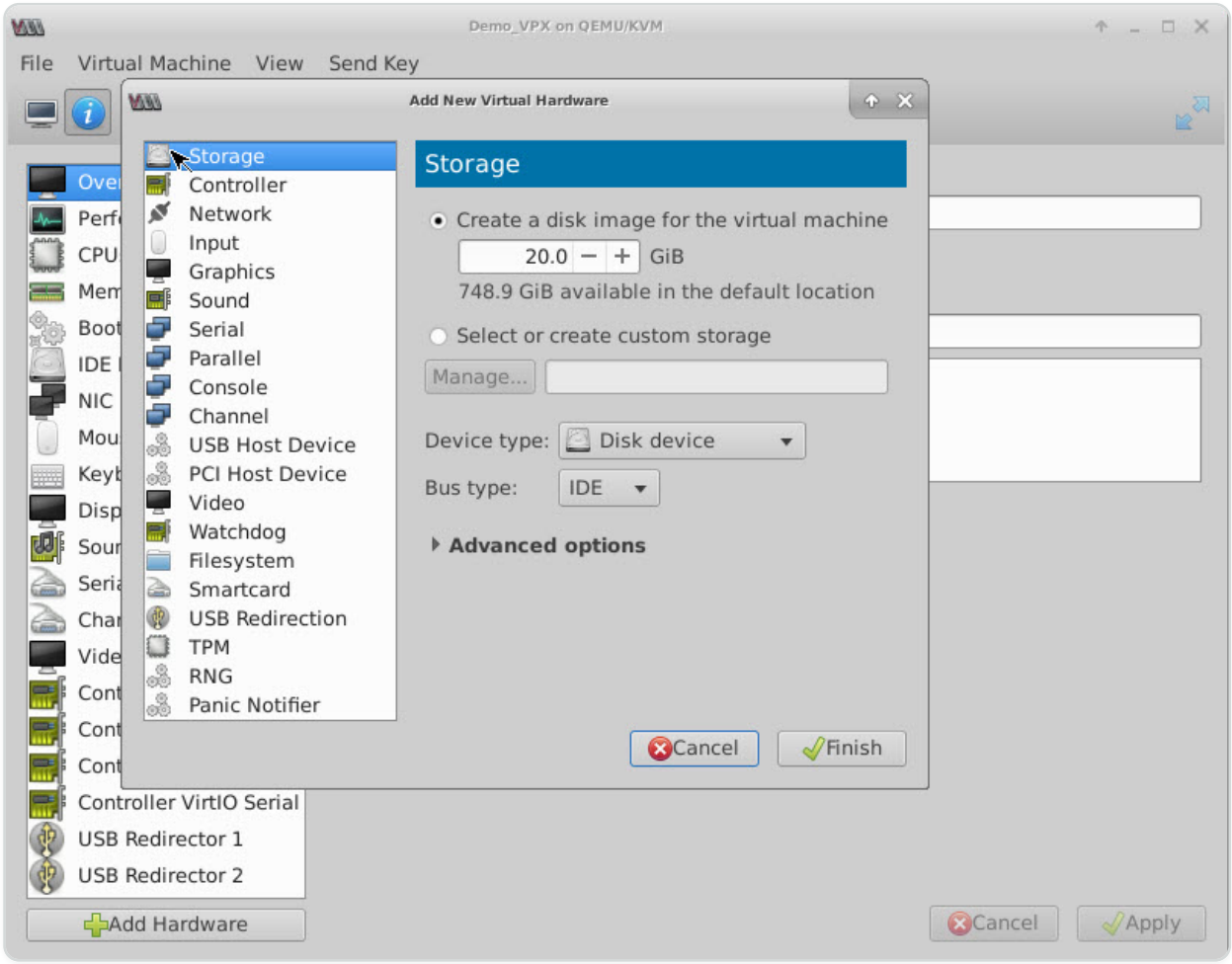
1. 关闭 NetScaler VPX 实例。
2. 选择 NetScaler VPX 实例，然后选择“打开”。

   配置 SR-IOV VM1(/en-us/vpx/media/config_sriov_vmm1.jpg)

3. 在 \<virtual machine on KVM\> 窗口中，选择 **i** 图标。

   配置 SR-IOV VM2(/en-us/vpx/media/config_sriov_vmm2.jpg)

4. 选择“**添加硬件**”。



5. 在“**添加新虚拟硬件**”对话框中，执行以下操作：

   a. 选择“PCI 主机设备”。

   b. 在“主机设备”部分中，选择您已创建的 VF，然后单击“完成”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

图 4：适用于 Intel 82599 10G NIC 的 VF

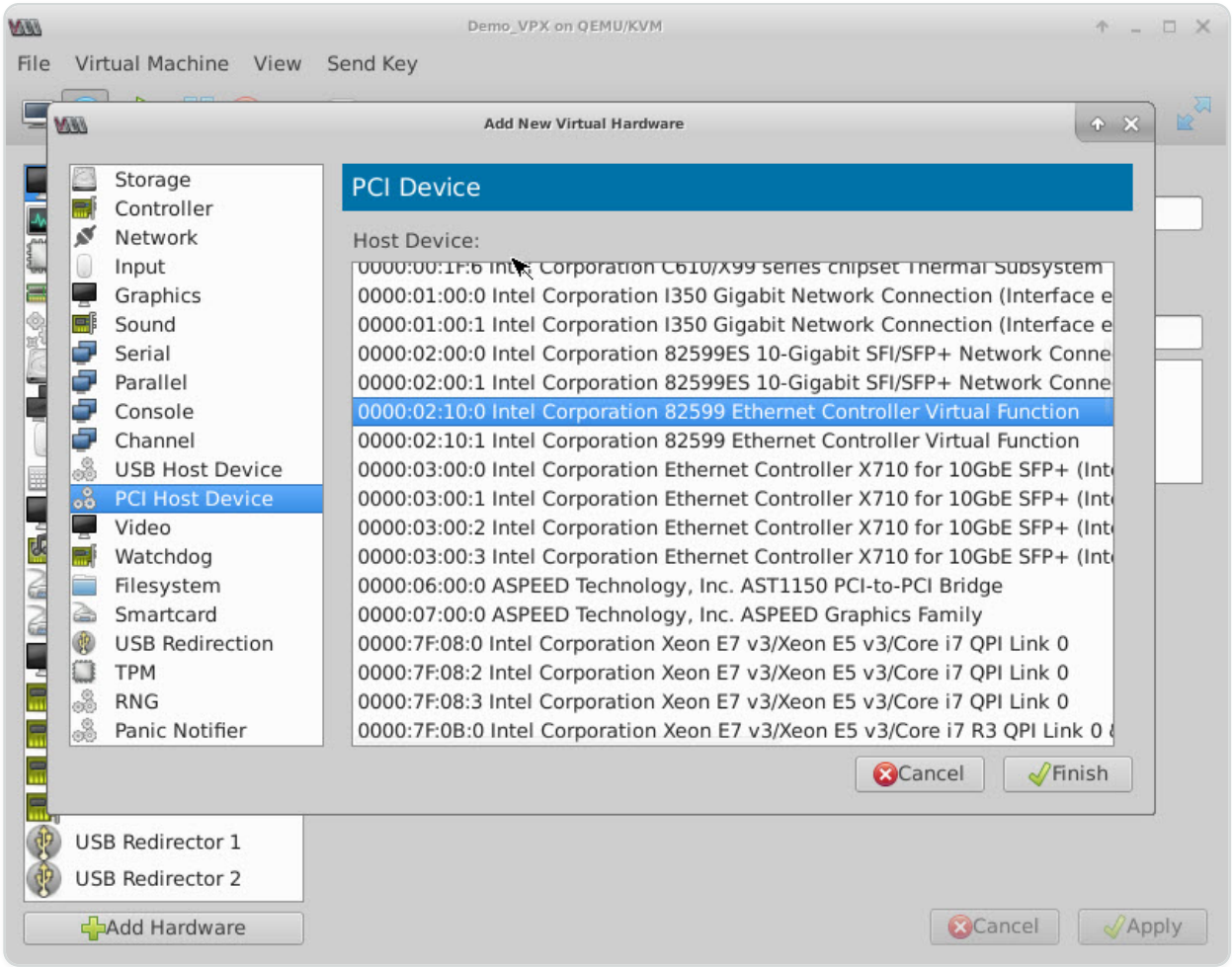
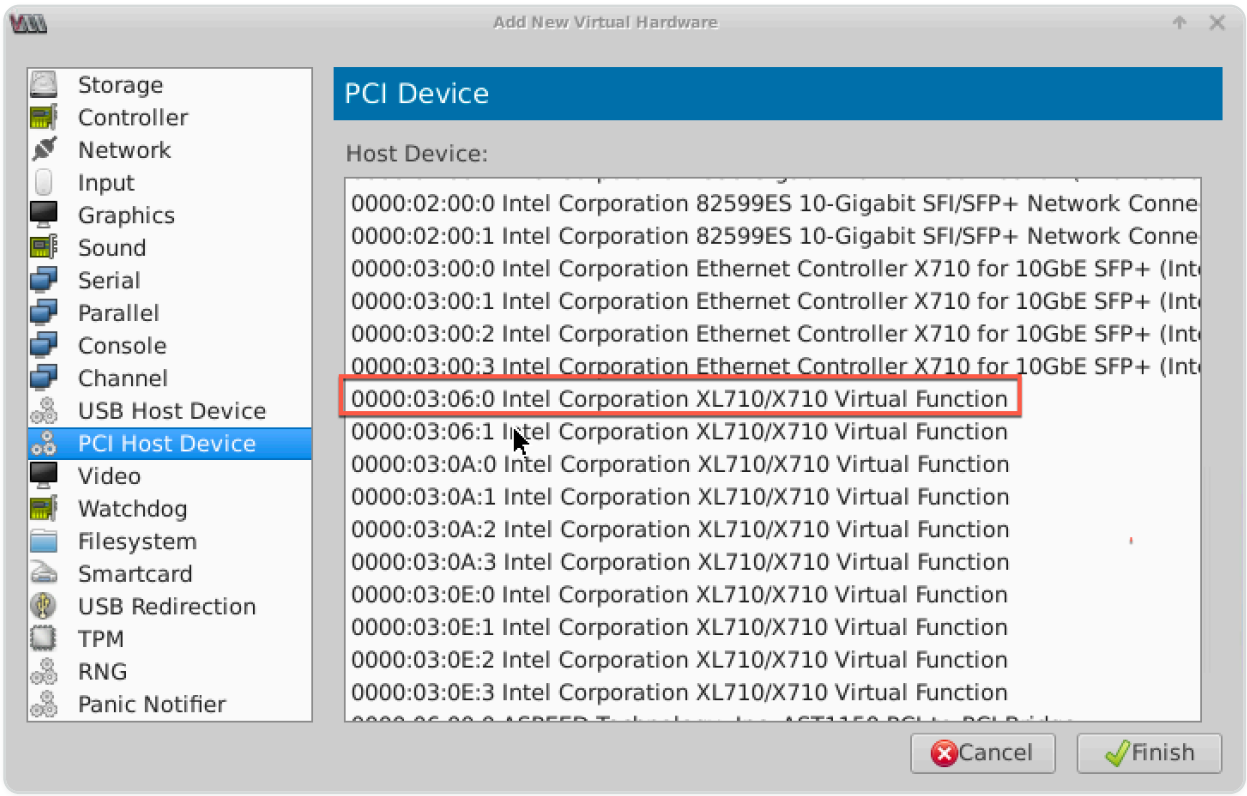
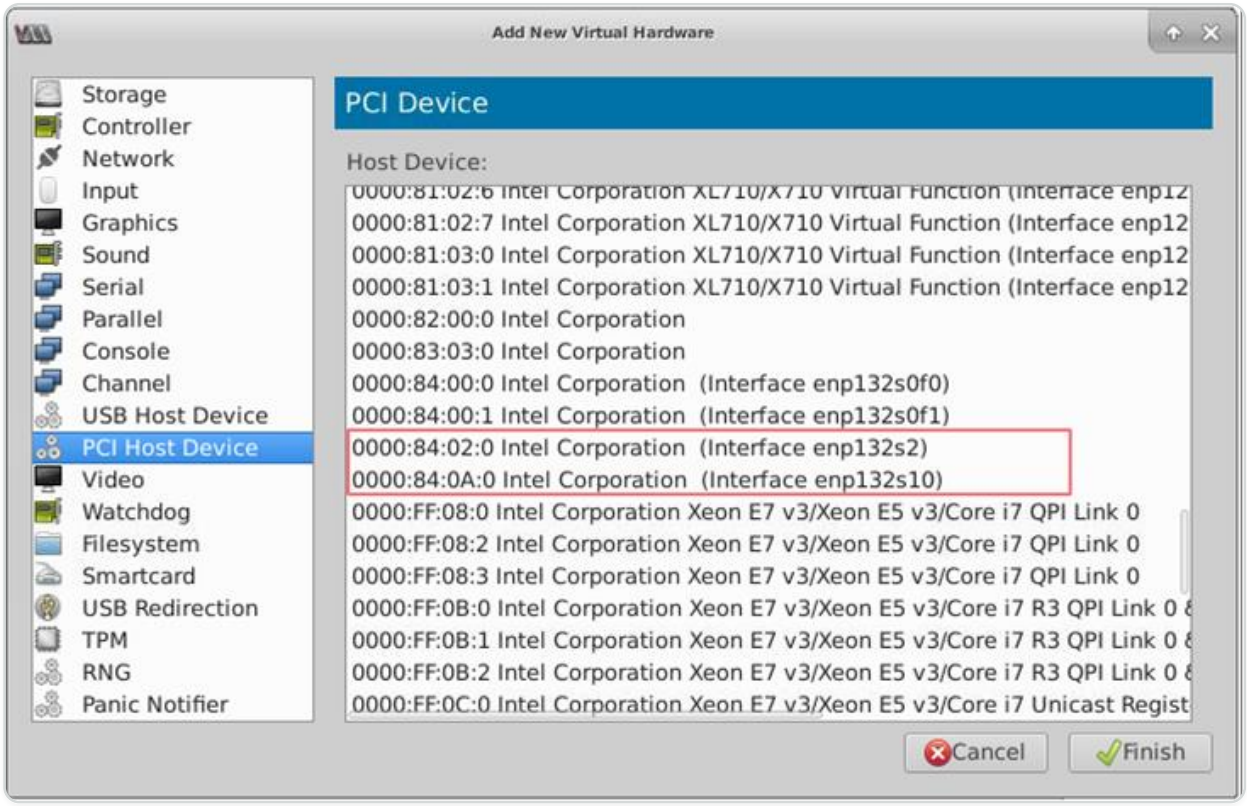


图 5：适用于 Intel XL710 40G NIC 的 VF



© 1997–2026 Citrix Systems, Inc. All rights reserved.

图 6：适用于 Intel X722 10G NIC 的 VF



6. 重复步骤 4 和 5 以添加您已创建的 VF。
7. 启动 NetScaler VPX 实例。
8. NetScaler VPX 实例启动后，使用以下命令验证配置：

```
show interface summary
```

输出显示您配置的所有接口。

图 6：Intel 82599 NIC 的输出摘要。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

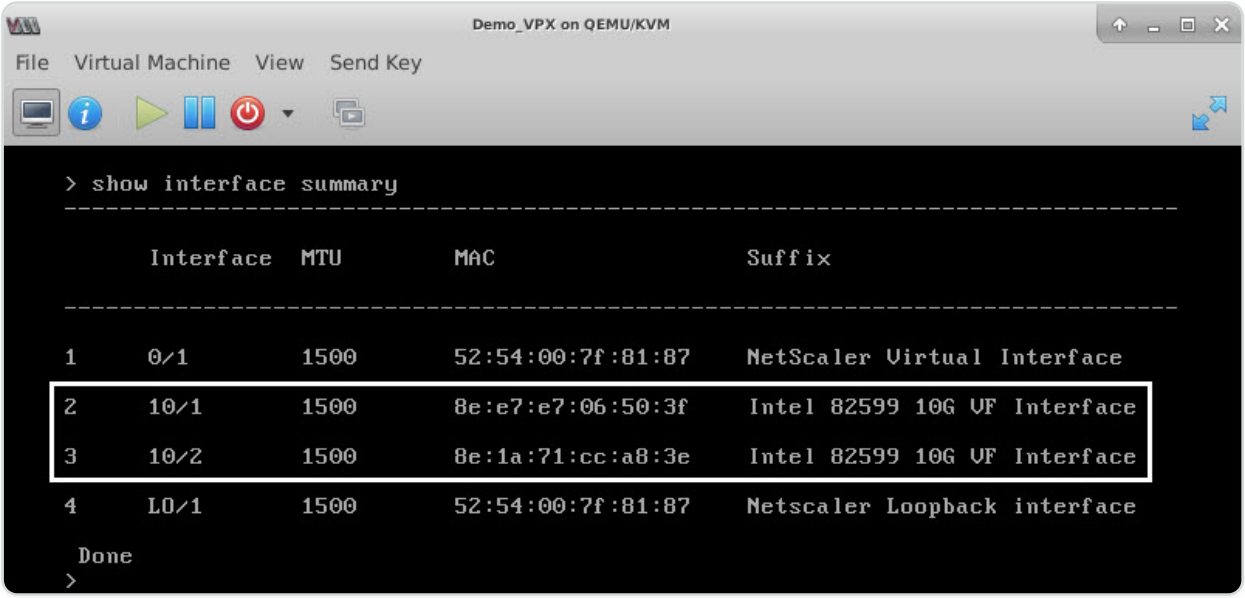
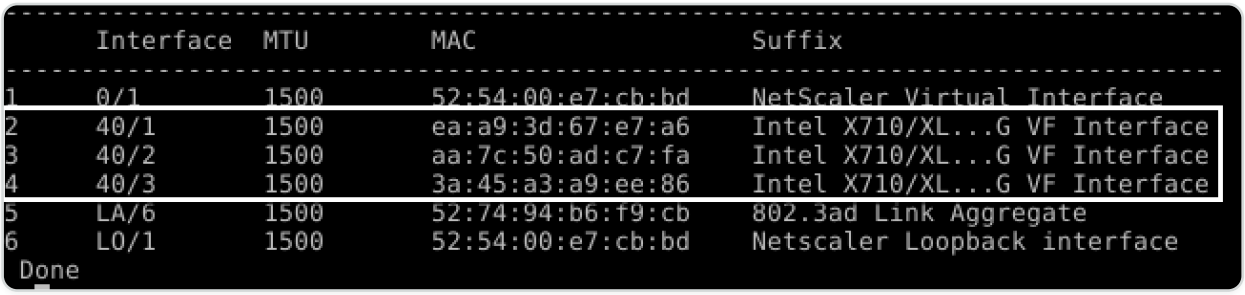


图 7。Intel X710 和 XL710 NIC 的输出摘要。



在 SR-IOV 接口上配置静态 LA/LACP

重要：

创建 SR-IOV VF 时，请确保不要将 MAC 地址分配给 VF。

要在链路聚合模式下使用 SR-IOV VF，请禁用已创建 VF 的欺骗检查。在 KVM 主机上，使用以下命令禁用欺骗检查：

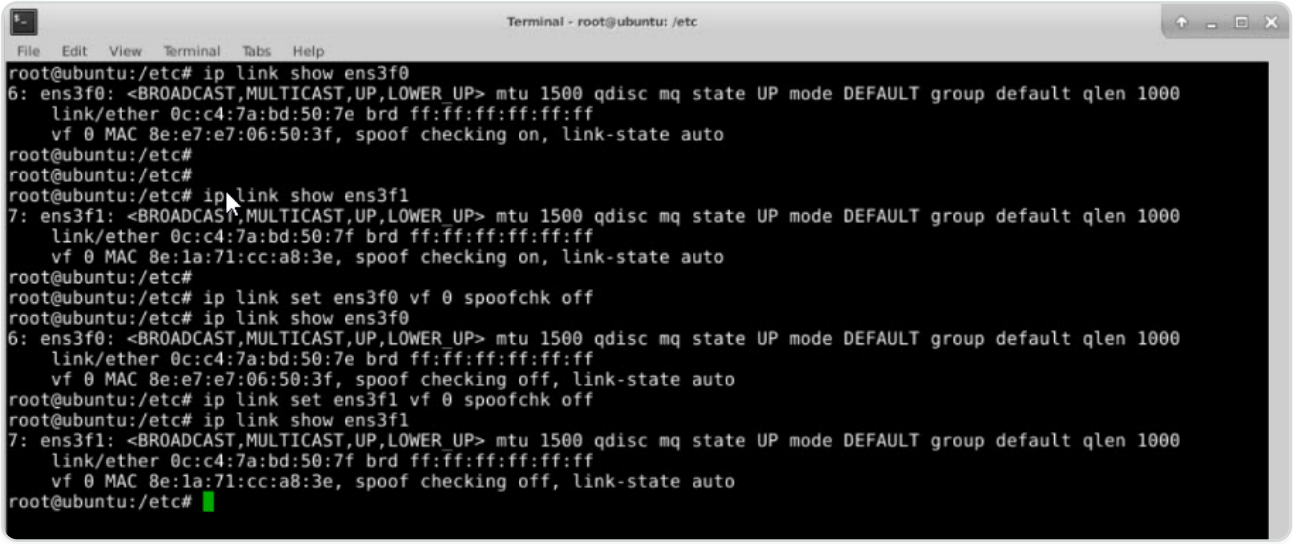
```
*ip link set \<interface\_name\> vf \<VF\_id\> spoofchk off*
```

其中：

- Interface_name – 是接口名称。
- VF_id – 是虚拟功能 ID。

示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



禁用所有已创建 VF 的欺骗检查后。重新启动 NetScaler VPX 实例并配置链路聚合。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：

确保 KVM 主机不包含 VF 接口的 VLAN 设置。

配置 NetScaler VPX 实例以使用 PCI 直通网络接口

在 Linux-KVM 平台上安装并配置 NetScaler VPX 实例后，您可以使用虚拟机管理器配置虚拟设备以使用 PCI 直通网络接口。

先决条件

- KVM 主机上 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，并且它们已在 KVM 主机的 BIOS 中启用。在 KVM 主机上，要启用 IOMMU，请将以下条目添加到 **/boot/grub2/grub.cfg** 文件中：**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配置 NetScaler VPX 实例以使用 PCI 直通网络接口，请执行以下操作：

1. 关闭 NetScaler VPX 实例。
2. 选择 NetScaler VPX 实例，然后单击“**打开**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置 SR-IOV(/en-us/vpx/media/config_sriov_vmm1.jpg)

3. 在“**virtual_machine on KVM>**”窗口中，单击“**i**”图标。

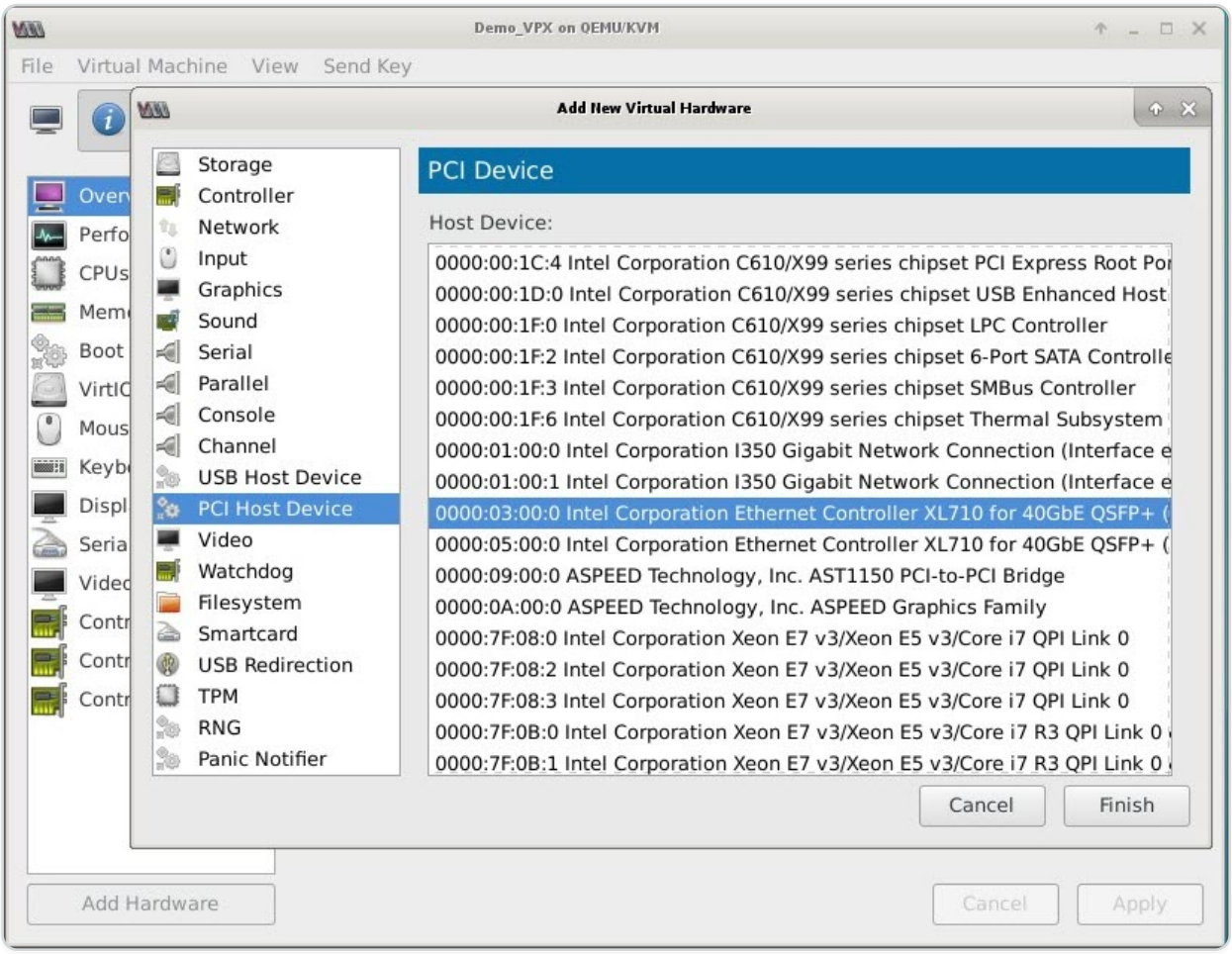
配置 KVM 上的 VM(/en-us/vpx/media/config_sriov_vmm2.jpg)

4. 单击“**添加硬件**”。
5. 在“**添加新虚拟硬件**”对话框中，执行以下操作：

   a. 选择“**PCI 主机设备**”。

   b. 在“**主机设备**”部分，选择 Intel XL710 物理功能。

   c. 单击“**完成**”。

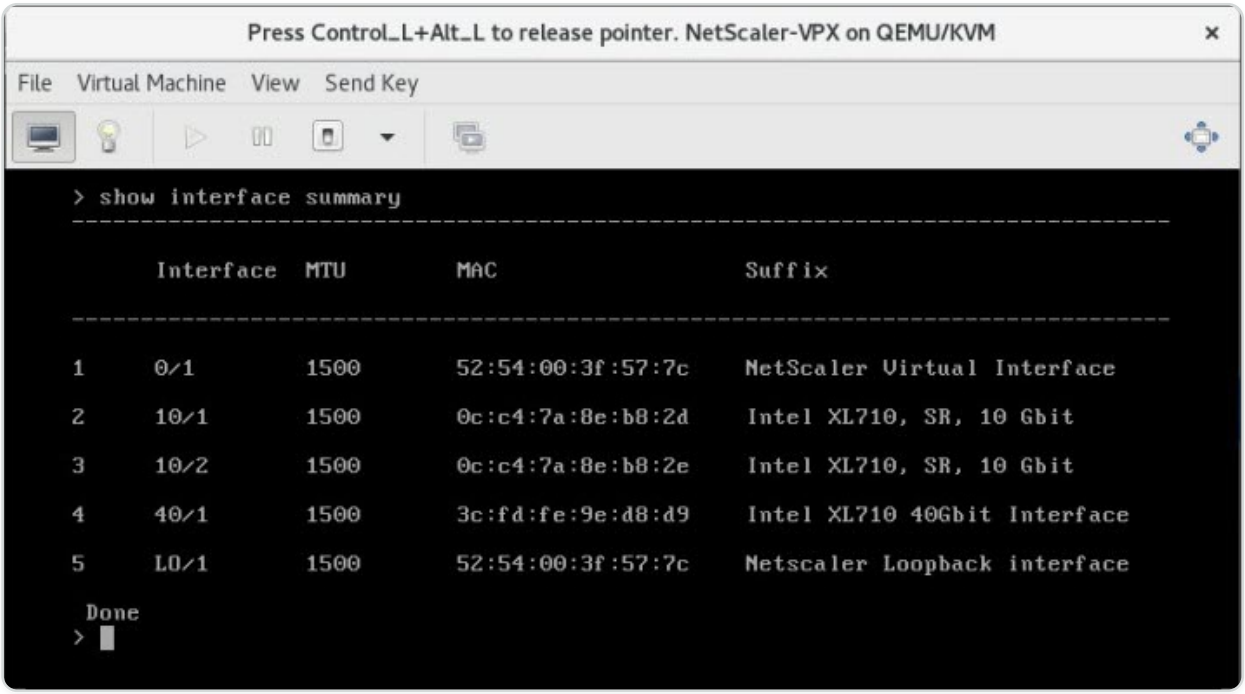


6. 重复步骤 **4** 和 **5** 以添加任何其他 Intel XL710 物理功能。
7. 启动 NetScaler VPX 实例。
8. NetScaler VPX 实例启动后，您可以使用以下命令验证配置：

```
COMMAND

> show interface summary
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

输出必须显示您配置的所有接口：



使用 `virsh` 程序预配 NetScaler VPX 实例

`virsh` 程序是一个用于管理 VM Guest 的命令行工具。其功能类似于虚拟机管理器。它使您能够更改 VM Guest 的状态（启动、停止、暂停等）、设置新的 Guest 和设备以及编辑现有配置。`virsh` 程序对于编写 VM Guest 管理操作脚本也很有用。

要使用 `virsh` 程序预配 NetScaler VPX，请按照以下步骤操作：

1. 使用 tar 命令解压 NetScaler VPX 软件包。NSVPX-KVM-*_nc.tgz 软件包包含以下组件：

   - 指定 VPX 属性的域 XML 文件 \[NSVPX-KVM-*_nc.xml\]
   - NS-VM 磁盘映像的校验和 \[Checksum.txt\]
   - NS-VM 磁盘映像 \[NSVPX-KVM-*_nc.raw\]

   示例：

   ```
   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
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 将 `NSVPX-KVM-*\_nc.xml XML` 文件复制到名为 `\<DomainName\>-NSVPX-KVM-*\_nc.xml` 的文件。\<DomainName\> 也是虚拟机的名称。示例：

```
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。文件路径必须是绝对路径。您可以指定 RAW 映像文件或 QCOW2 映像文件的路径。

     如果您想指定一个 RAW 镜像文件，请按照以下示例指定磁盘镜像源路径：

     示例：

```
<name>NetScaler-VPX</name>

<mac address='52:54:00:29:74:b3'/>

<source file='/root/NSVPX-KVM-10.1-117_nc.raw'/>
```

     指定绝对 QCOW2 磁盘镜像源路径，并将驱动程序类型定义为 **qcow2**，如以下示例所示：

     示例：

```
<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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- source dev— 指定接口。
- mode— 指定模式。默认接口是 **Macvtap Bridge**。

示例：模式：MacVTap Bridge 将目标接口设置为 `ethx`，模式设置为 bridge，模型类型设置为 `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>
```

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
```

示例：

```
virsh define NS-VPX-NSVPX-KVM-10.1-117_nc.xml
```

6. 通过输入以下命令启动 VM：

```
virsh start \[\<DomainName\> | \<DomainUUID\>\]
```

示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
virsh start NetScaler-VPX
```

7. 通过控制台连接访客 VM：

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

示例：

```
virsh console NetScaler-VPX
```

使用 `virsh` 程序向 NetScaler VPX 实例添加更多接口

在 KVM 上预置 NetScaler VPX 后，您可以添加额外的接口。

要添加更多接口，请按照以下步骤操作：

1. 关闭在 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，追加以下参数：

   a. **对于 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 地址在所有接口中是唯一的。
   - 源设备 — 指定接口名称。
   - 模式 — 指定模式。支持的模式有 - Bridge、VEPA、Private 和 Pass-through
   - 模型类型 — 将模型类型指定为 `virtio`

   示例：

   模式：MacVTap 直通

   将目标接口设置为 `ethx`，模式设置为 bridge，模型类型设置为 `virtio`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<interface type='direct'>

      <mac address='52:54:00:29:74:b3'/>

      <source dev='eth1' mode='passthrough'/>

      <model type='virtio'/>

 </interface>
```

这里 eth1 是连接到虚拟机的物理接口。

b. **对于桥接模式**

> **注意：**
>
> 确保您已在 KVM 主机中配置了 Linux 网桥，将物理接口绑定到该网桥，并将该网桥置于 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 地址在所有接口中是唯一的。
- 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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

管理 NetScaler VPX 访客虚拟机

您可以使用虚拟机管理器和 `virsh` 程序执行管理任务，例如启动或停止虚拟机访客、设置新的访客和设备、编辑现有配置以及通过虚拟网络计算 (VNC) 连接到图形控制台。

使用虚拟机管理器管理 VPX 访客虚拟机

- 列出虚拟机访客

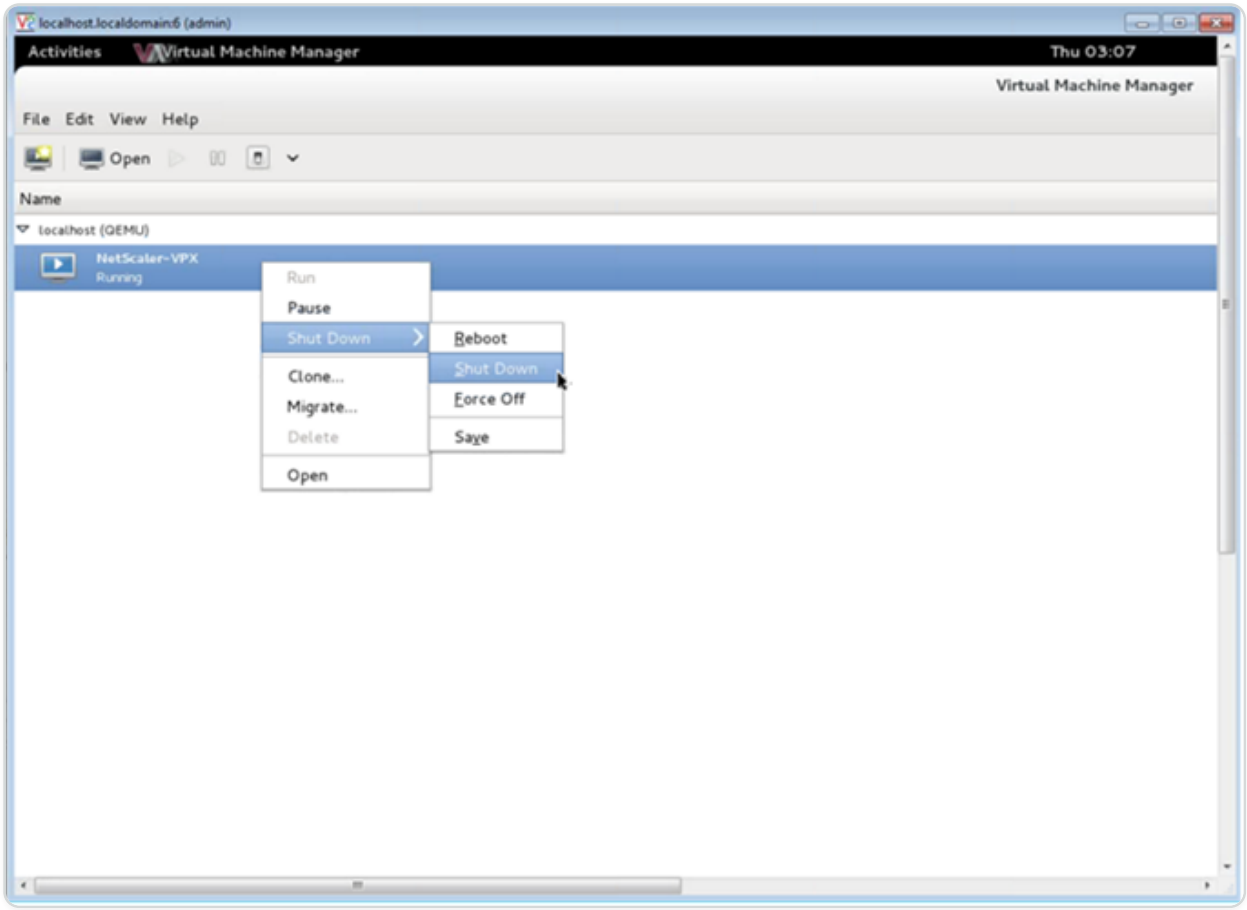
  虚拟机管理器的主窗口显示其连接到的每个虚拟机主机服务器的所有虚拟机访客列表。每个虚拟机访客条目包含虚拟机的名称及其状态（运行中、已暂停或已关机），如图标所示。

- 打开图形控制台

  打开虚拟机访客的图形控制台使您能够像通过 VNC 连接与物理主机交互一样与机器交互。要在虚拟机管理器中打开图形控制台，请右键单击虚拟机访客条目，然后从弹出菜单中选择“打开”选项。

- 启动和关闭访客

  您可以从虚拟机管理器启动或停止虚拟机访客。要更改虚拟机的状态，请右键单击虚拟机访客条目，然后从弹出菜单中选择“运行”或其中一个“关机”选项。



- 重启访客

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以从虚拟机管理器重启虚拟机访客。要重启虚拟机，请右键单击虚拟机访客条目，然后从弹出菜单中选择“关机”>“重启”。

- 删除访客

  删除虚拟机访客默认会删除其 XML 配置。您还可以删除访客的存储文件。这样做会彻底擦除访客。

  a. 在虚拟机管理器中，右键单击虚拟机访客条目。

  b. 从弹出菜单中选择“删除”。将打开一个确认窗口。

  > **注意：**
  >
  > 仅当虚拟机访客机关闭时，“删除”选项才可用。

  c. 单击“**删除**”。

  d. 要完全擦除访客机，请选中“删除关联存储文件”复选框以删除关联的 .raw 文件。

使用 `virsh` 程序管理 NetScaler VPX 访客虚拟机

- 列出虚拟机访客机及其当前状态。

  使用 `virsh` 显示有关访客机的信息

  `virsh list --all`

  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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

通过控制台连接访客虚拟机

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

示例：

`virsh console NetScaler-VPX`

- 启动和关闭访客。

  可以使用 DomainName 或 Domain-UUID 启动访客。

  `virsh start [<DomainName> | <DomainUUID>]`

  示例：

  `virsh start NetScaler-VPX`

  关闭访客：

  `virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]`

  示例：

  `virsh shutdown NetScaler-VPX`

- 重启访客

  `virsh reboot [<DomainID> | <DomainName> | <DomainUUID>]`

  示例：

  `virsh reboot NetScaler-VPX`

  删除访客

  要删除访客虚拟机，您必须先关闭访客并取消定义 \<DomainName\>-NSVPX-KVM-*_nc.xml，然后才能运行删除命令。

  ```
  virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]

  virsh undefine [<DomainName> | <DomainUUID>]
  ```

  示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
virsh shutdown NetScaler-VPX

virsh undefine NetScaler-VPX
```

注意：

删除命令不会移除磁盘映像文件，该文件必须手动移除。

在 OpenStack 上使用 SR-IOV 预置 NetScaler VPX 实例

您可以在 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。

您可以通过以下三个步骤在 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 上预置 NetScaler VPX。

先决条件

确保您：

- 将 Intel 82599 NIC (NIC) 添加到主机。
- 从 Intel 下载并安装最新的 IXGBE 驱动程序。
- 在主机上阻止 IXGBEVF 驱动程序。在 /etc/modprobe.d/blacklist.conf 文件中添加以下条目：阻止列表 `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

执行以下步骤之一以启用 SR-IOV VF：

- 如果您使用的内核版本早于 3.8，请将以下条目添加到 /etc/modprobe.d/ixgbe 文件并重新启动主机：options ixgbe max_vfs=\<number_of_VFs\>
- 如果您使用的内核版本为 3.8 或更高版本，请使用以下命令创建 VF：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
echo <number_of_VFs> > /sys/class/net/<device_name>/device/sriov_numvfs
```

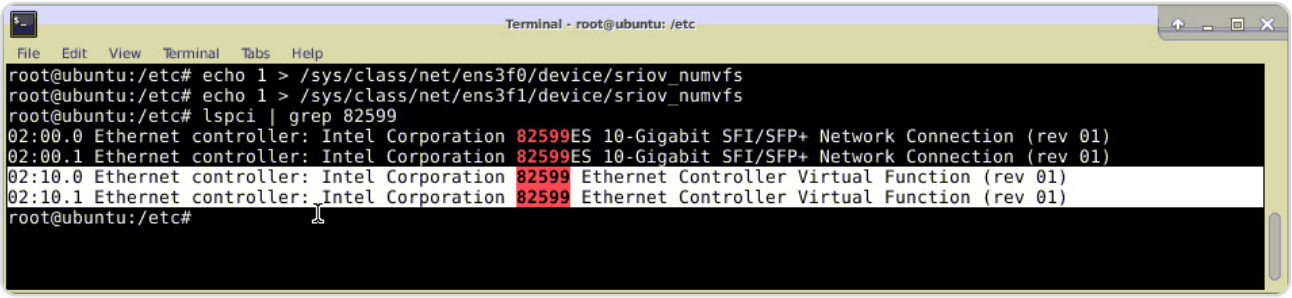
其中：

- number_of_VFs 是您要创建的虚拟功能 (Virtual Functions) 的数量。
- device_name 是接口名称。

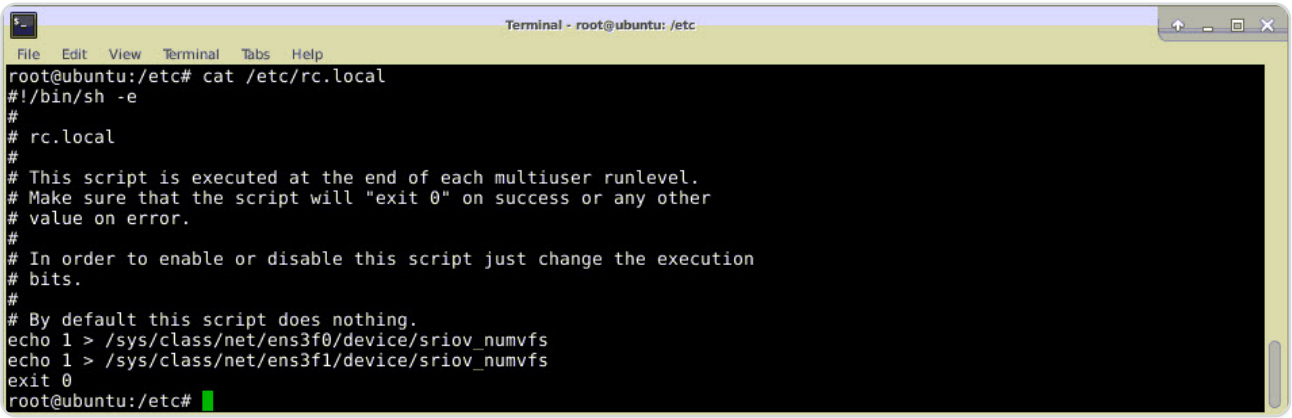
重要提示：

在创建 SR-IOV VF 时，请确保不要为 VF 分配 MAC 地址。

以下是创建四个 VF 的示例。



使 VF 持久化，将用于创建 VF 的命令添加到 **rc.local** 文件中。以下是显示 rc.local 文件内容的示例。



有关更多信息，请参阅此 Intel SR-IOV 配置指南。

配置 VF 并使其可用于 OpenStack

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 上预配 NetScaler VPX 实例

您可以使用 OpenStack CLI 在 OpenStack 环境中预置 NetScaler VPX 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

预置 VPX 实例可选地涉及使用配置驱动器中的数据。配置驱动器是一种特殊的配置驱动器，在实例启动时会附加到实例。在为实例配置网络设置之前，此配置驱动器可用于将网络配置信息（例如管理 IP 地址、网络掩码和默认网关等）传递给实例。

当 OpenStack 预置 VPX 实例时，它首先通过读取指示 OpenStack 的特定 BIOS 字符串 (OpenStack Foundation) 来检测实例正在 OpenStack 环境中启动。对于 Red Hat Linux 发行版，该字符串存储在 /etc/nova/release 中。这是基于 KVM 虚拟机管理程序平台的所有 OpenStack 实现中都可用的标准机制。该驱动器必须具有特定的 OpenStack 标签。如果检测到配置驱动器，实例会尝试从 `nova` 启动命令中指定的文件名读取以下信息。在下面的过程中，该文件名为“userdata.txt”。

- 管理 IP 地址
- 网络掩码
- 默认网关

参数成功读取后，它们将填充到 NetScaler® 堆栈中。这有助于远程管理实例。如果参数未成功读取或配置驱动器不可用，实例将转换为默认行为，即：

- 实例尝试从 DHCP 检索 IP 地址信息。
- 如果 DHCP 失败或超时，实例将使用默认网络配置 (192.168.100.1/16) 启动。

通过 CLI 在 OpenStack 上预置 NetScaler VPX 实例

您可以使用 OpenStack CLI 在 OpenStack 环境中预置 VPX 实例。以下是在 OpenStack 上预置 NetScaler VPX 实例的步骤摘要：

1. 从 .tgz 文件中提取 `.qcow2` 文件
2. 从 qcow2 映像构建 OpenStack 映像
3. 预置 VPX 实例

要在 OpenStack 环境中预置 VPX 实例，请执行以下步骤。

1. 通过输入以下命令，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
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 通过输入以下命令，使用在步骤 1 中提取的 `.qcoz2` 文件构建 OpenStack 镜像：

```
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 镜像后，预配 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-
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
02086a6bdee2 NSVPX-10
```

在上述命令中，userdata.txt 是一个文件，其中包含 VPX 实例的详细信息，例如 IP 地址、子网掩码和默认网关。用户数据文件是用户可自定义的文件。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 是 OpenStack VF。

下图提供了 `nova` 引导命令的示例输出。

```
+--------------------------------------+--------------------------------------------------------------+
| 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。\<PropertySection\>\</PropertySection\> 标签中的值是用户可配置的值，包含 IP 地址、子网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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<Kind>NOVA</Kind>

<Version>2013.1</Version>

<Vendor>Openstack</Vendor>

<Locale>en</Locale>

</PlatformSection>

<PropertySection>

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

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

citrix.com 4

<Property oe:key="com.citrix.netscaler.orch_env"

oe:value="openstack-orch-env"/>

<Property oe:key="com.citrix.netscaler.mgmt.ip"

oe:value="10.1.0.100"/>

<Property oe:key="com.citrix.netscaler.mgmt.netmask"

oe:value="255.255.0.0"/>

<Property oe:key="com.citrix.netscaler.mgmt.gateway"

oe:value="10.1.0.1"/>

</PropertySection>

</Environment>
```

其他支持的配置：从主机创建和删除 SR-IOV VF 上的 VLAN

输入以下命令以在 SR-IOV VF 上创建 VLAN：

`ip link show enp8s0f0 vf 6 vlan 10`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在上述命令中，"enp8s0f0" 是物理功能的名称。

示例：在 vf 6 上创建的 VLAN 10

```
4: enp8s0f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT qlen 1000
    link/ether 00:1b:21:7b:d7:88 brd ff:ff:ff:ff:ff:ff
    vf 0 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off
    vf 1 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off
    vf 2 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off
    vf 3 MAC fa:16:3e:1e:0b:ee, spoof checking on, link-state auto, trust off
    vf 4 MAC fa:16:3e:0d:05:62, spoof checking on, link-state auto, trust off
    vf 5 MAC 5e:46:0d:79:de:f8, spoof checking on, link-state auto, trust off
    vf 6 MAC fa:16:3e:db:ea:b3, vlan 10, spoof checking on, link-state auto, trust off
    vf 7 MAC 00:00:00:00:00:00, spoof checking on, link-state auto, trust off
```

输入以下命令以删除 SR-IOV VF 上的 VLAN：

```
ip link show enp8s0f0 vf 6 vlan 0
```

示例：VLAN 10，已从 vf 6 中移除

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

这些步骤完成了在 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

您可以配置在 KVM（Fedora 和 RHOS）上运行的 NetScaler VPX 实例，以使用 Open vSwitch (OVS) 和数据平面开发套件 (DPDK) 来获得更好的网络性能。本文档介绍了如何配置 NetScaler VPX 实例，使其在 KVM 主机上由 OVS-DPDK 暴露的 `vhost-user` 端口上运行。

OVS 是一个在开源 Apache 2.0 许可下授权的多层虚拟交换机。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 实例的条件：

费多拉	RHOS
费多拉 25	RHOS 7.4

© 1997–2026 Citrix Systems, Inc. All rights reserved.

费多拉	RHOS
OVS 2.7.0	OVS 2.6.1
DPDK 16.11.12	DPDK 16.11.12

先决条件

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。
- 构建并安装 OVS。
- 创建 OVS 网桥。
- 将物理接口连接到 OVS 网桥。
- 将 `vhost-user` 端口连接到 OVS 数据路径。
- 使用基于 OVS-DPDK 的 `vhost-user` 端口配置 KVM-VPX。

安装 DPDK

要安装 DPDK，请遵循此 Open vSwitch with DPDK 文档中提供的说明。

构建并安装 OVS

从 OVS 下载页面 下载 OVS。然后，使用 DPDK 数据路径构建并安装 OVS。请遵循 安装 Open vSwitch 文档中提供的说明。

有关更多详细信息，请参阅 DPDK Linux 入门指南。

创建 OVS 网桥

根据您的需要，键入 Fedora 或 RHOS 命令来创建 OVS 网桥：

Fedora 命令：

```
> $OVS_DIR/utilities/ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
datapath_type=netdev
```

RHOS 命令：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0 datapath_type=netdev
```

将物理接口连接到 OVS 网桥

通过键入以下 Fedora 或 RHOS 命令，将端口绑定到 DPDK，然后将其连接到 OVS 网桥：

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
```

选项中显示的 `dpdk-devargs` 指定了相应物理网卡的 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` 端口连接到 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user2 -- set
Interface vhost-user2 type=dpdkvhostuser -- set Interface vhost-user2
 mtu_request=9000



chmod g+w  /usr/local/var/run/openvswitch/vhost*
```

RHOS 命令：

```
ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1
type=dpdkvhostuser -- set Interface vhost-user1  mtu_request=9000



ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2
type=dpdkvhostuser -- set Interface vhost-user2  mtu_request=9000



chmod g+w /var/run/openvswitch/vhost*
```

预配具有基于 OVS-DPDK 的 `vhost-user` 端口的 KVM-VPX

您只能通过使用以下 QEMU 命令从 CLI 在 Fedora KVM 上预配具有基于 OVS-DPDK 的 `vhost-user` 端口的 VPX 实例： **Fedora 命令：**

```
qemu-system-x86_64 -name KVM-VPX -cpu host -enable-kvm -m 4096M \



-object memory-backend-file,id=mem,size=4096M,mem-path=/dev/
hugepages,share=on -numa node,memdev=mem \



-mem-prealloc -smp sockets=1,cores=2 -drive file=<absolute-path-to-disc-
image-file>,if=none,id=drive-ide0-0-0,format=<disc-image-format> \
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-device ide-drive,bus=ide.0,unit=0,drive=drive-
ide0-0-0,id=ide0-0-0,bootindex=1 \



-netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \



-device virtio-net-
pci,netdev=hostnet0,id=net0,mac=52:54:00:3c:d1:ae,bus=pci.0,addr=0x3 \



-chardev socket,id=char0,path=</usr/local/var/run/openvswitch/vhost-user1>
\



-netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device virtio-
net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \



-chardev socket,id=char1,path=</usr/local/var/run/openvswitch/vhost-user2>
\



-netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device virtio-
net



pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \



--nographic
```

对于 RHOS，请使用以下示例 XML 文件通过 `virsh` 预配 NetScaler VPX 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<domain type='kvm'>

  <name>dpdk-vpx1</name>

  <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>

  <memory unit='KiB'>16777216</memory>

  <currentMemory unit='KiB'>16777216</currentMemory>

  <memoryBacking>

    <hugepages>

      <page size='1048576' unit='KiB'/>

    </hugepages>

  </memoryBacking>

  <vcpu placement='static'>6</vcpu>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  <cpu mode='custom' match='minimum' check='full'>

    <model fallback='allow'>Haswell-noTSX</model>

    <vendor>Intel</vendor>

    <topology sockets='1' cores='6' threads='1'/>

    <feature policy='require' name='ss'/>

    <feature policy='require' name='pcid'/>

    <feature policy='require' name='hypervisor'/>

    <feature policy='require' name='arat'/>

<domain type='kvm'>

  <name>dpdk-vpx1</name>

  <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<memory unit='KiB'>16777216</memory>

<currentMemory unit='KiB'>16777216</currentMemory>

<memoryBacking>

  <hugepages>

    <page size='1048576' unit='KiB'/>

  </hugepages>

</memoryBacking>

<vcpu placement='static'>6</vcpu>

<cputune>

  <shares>4096</shares>

  <vcpupin vcpu='0' cpuset='0'/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    <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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    <topology sockets='1' cores='6' threads='1'/>

    <feature policy='require' name='ss'/>

    <feature policy='require' name='pcid'/>

    <feature policy='require' name='hypervisor'/>

    <feature policy='require' name='arat'/>

    <feature policy='require' name='tsc\_adjust'/>

    <feature policy='require' name='xsaveopt'/>

    <feature policy='require' name='pdpe1gb'/>

    <numa>

      <cell id='0' cpus='0-5' memory='16777216' unit='KiB'
memAccess='shared'/>

    </numa>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</cpu>

<clock offset='utc'/>

<on\_poweroff>destroy</on\_poweroff>

<on\_reboot>restart</on\_reboot>

<on\_crash>destroy</on\_crash>

<devices>

  <emulator>/usr/libexec/qemu-kvm</emulator>

  <disk type='file' device='disk'>

    <driver name='qemu' type='qcow2' cache='none'/>

    <source file='/home/NSVPX-KVM-12.0-52.18\_nc.qcow2'/>

    <target dev='vda' bus='virtio'/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
function='0x0'/>


    </disk>


    <controller type='ide' index='0'>


      <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'>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      <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'/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    </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>


    <interface type='vhostuser'>


      <mac address='52:54:00:2a:32:74'/>


      <source type='unix' path='/var/run/openvswitch/vhost-user3'
mode='client'/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      <model type='virtio'/>


      <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
function='0x0'/>


    </interface>


    <interface type='vhostuser'>


      <mac address='52:54:00:2a:32:84'/>


      <source type='unix' path='/var/run/openvswitch/vhost-user4'
mode='client'/>


     <model type='virtio'/>


      <address type='pci' domain='0x0000' bus='0x00' slot='0x09'
function='0x0'/>


    </interface>


    <serial type='pty'>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      <target port='0'/>

    </serial>

    <console type='pty'>

      <target type='serial' port='0'/>

    </console>

    <input type='mouse' bus='ps2'/>

    <input type='keyboard' bus='ps2'/>

    <graphics type='vnc' port='-1' autoport='yes'>

      <listen type='address'/>

    </graphics>

    <video>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      <model type='cirrus' vram='16384' heads='1' primary='yes'/>



      <address type='pci' domain='0x0000' bus='0x00' slot='0x02'
function='0x0'/>



    </video>



    <memballoon model='virtio'>



      <address type='pci' domain='0x0000' bus='0x00' slot='0x08'
function='0x0'/>



    </memballoon>



  </devices>



</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。

```
<memoryBacking>



    <hugepages>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      <page size='1048576' unit='KiB'/>


    </hugepages>
```

此外，在示例文件中，vhost-user1 是绑定到 ovs-br0 的 `vhost` 用户端口。

```
<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>
```

要启动 NetScaler VPX 实例，请开始使用 `virsh` 命令。

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

您可以在 KVM 虚拟机管理程序上首次启动 NetScaler 设备时应用 NetScaler VPX 配置。因此，可以在更短的时间内配置 VPX 实例上的客户设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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启动用户数据进行引导，必须在 `<NS-CONFIG>` 部分中传递默认网关配置。有关 `<NS-CONFIG>` 标签内容的更多信息，请参阅以下示例 `<NS-CONFIG>` 部分。

示例 `<NS-CONFIG>` 部分：

```
<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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

如何在 KVM 虚拟机管理程序上提供预启动用户数据

您可以通过 ISO 文件在 KVM 虚拟机管理程序上提供预启动用户数据，该文件使用 CDROM 设备附加。

使用 CDROM ISO 文件提供用户数据

您可以使用虚拟机管理器 (VMM) 通过 CDROM 设备将用户数据作为 ISO 映像注入虚拟机 (VM)。KVM 支持 VM Guest 中的 CD-ROM，可以通过直接访问 VM 主机服务器上的物理驱动器或访问 ISO 映像来实现。

以下步骤使您能够使用 CDROM ISO 文件提供用户数据：

1. 创建一个文件，文件名为 `userdata`，其中包含预启动用户数据内容。

   注意：

   文件名必须严格使用 `userdata`。

2. 将 `userdata` 文件存储在文件夹中，并使用该文件夹构建 ISO 映像。

   您可以通过以下两种方法使用 `userdata` 文件构建 ISO 映像：

   - 使用任何图像处理工具，例如 PowerISO。
   - 在 Linux 中使用 `mkisofs` 命令。

   以下示例配置展示了如何在 Linux 中使用 `mkisofs` 命令生成 ISO 映像。

```
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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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. 使用标准部署流程预置 NetScaler VPX 实例以创建虚拟机。但不要自动启动虚拟机。
4. 使用以下步骤通过虚拟机管理器添加 CD-ROM 设备：
   a. 在虚拟机管理器中双击 VM Guest 条目以打开其控制台，然后通过 **View > Details** 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 **Manage** 并选择正确的 ISO 文件，然后单击 **Finish**。您的 NetScaler VPX 实例的 **Resources** 下将创建一个新的 CDROM。
5. 启动虚拟机。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

AWS 上的 NetScaler VPX

您可以在 Amazon Web Services (AWS) 上启动 NetScaler VPX 实例。NetScaler VPX 设备在 AWS Marketplace 中作为 Amazon Machine Image (AMI) 提供。AWS 上的 NetScaler VPX 实例使您能够利用 AWS 云计算功能，并使用 NetScaler 负载平衡和流量管理功能来满足业务需求。VPX 实例支持物理 NetScaler 设备的所有流量管理功能，并且可以作为独立实例或 HA 对进行部署。有关 VPX 功能的更多信息，请参阅 VPX 数据表。

入门

在开始部署 VPX 之前，您必须熟悉以下信息：

- AWS 术语
- AWS-VPX 支持矩阵
- 限制和使用指南
- 先决条件
- 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
    - 使用私有 IP 在不同区域之间实现高可用性(/zh-cn/vpx/13-1/deploy-aws/vpx-ha-pip-different-aws-zones.html)
- 主动-主动 GSLB(/zh-cn/citrix-adc/13-1/global-server-load-balancing/deployment-types/active-active-site-deployment.html)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

混合部署

- 在 AWS Outpost 中部署 NetScaler(/zh-cn/vpx/13-1/deploy-aws/deploy-vpx-on-aws-outposts.html)
- 在 AWS 中的 VMC 中部署 NetScaler(/zh-cn/vpx/13-1/install-vpx-on-vmc-on-aws.html)

许可

AWS 上的 NetScaler VPX 实例需要许可证。在 AWS 上运行的 NetScaler VPX 实例可用的许可选项是自带许可证 (BYOL)。

自动化

- NetScaler ADM：智能部署(/zh-cn/citrix-application-delivery-management-service/getting-started.html)
- GitHub CloudFormation 模板：用于 AWS 部署的 NetScaler 模板和脚本
- GitHub Ansible：用于 AWS 部署的 NetScaler 模板和脚本
- GitHub Terraform：用于 AWS 部署的 NetScaler 模板和脚本
- AWS 模式库 (PL)：NetScaler VPX

博客

- NetScaler on AWS 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 轻松在公有云中横向扩展或收缩
- Citrix 通过 AWS Outposts 扩展 ADC 部署选择
- 将 NetScaler 与 Amazon VPC 入口路由结合使用
- Citrix 在 AWS 中提供选择、性能和简化的部署
- NetScaler Web App Firewall 的安全性 – 现已在 AWS Marketplace 上提供
- Aria Systems 如何在 AWS 上使用 NetScaler Web App Firewall

© 1997–2026 Citrix Systems, Inc. All rights reserved.

视频

- 通过 ADM 简化公有云 NetScaler 部署
- 使用现成的 Terraform 脚本在 AWS 中预置和配置 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
- 使用 ADM 进行 NetScaler 自动扩缩

客户案例研究

- 技术解决方案 - Xenit AB
- 探索 NetScaler 和 AWS 的优势

解决方案

- 使用 NetScaler 在 AWS 上部署数字广告平台
- 使用 NetScaler 增强 AWS 中的点击流分析

支持

- 开立支持案例
- 对于 NetScaler 订阅产品，请参阅 排查 AWS 上的 VPX 实例。要提交支持案例，请查找您的 AWS 账号和支持 PIN 码，然后致电 NetScaler 支持。
- 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。如果您没有协议，请联系您的 NetScaler 代表。

其他参考资料

- AWS 点播网络研讨会 - AWS 上的 NetScaler
- NetScaler VPX 数据表
- AWS Marketplace 中的 NetScaler
- NetScaler 是 AWS 网络合作伙伴解决方案（负载均衡器）的一部分
- AWS 常见问题

© 1997–2026 Citrix Systems, Inc. All rights reserved.

AWS 术语

本节介绍常用的 AWS 术语和短语。有关更多信息，请参阅AWS 词汇表。

术语	定义
亚马逊机器镜像 (AMI)	一种机器镜像，提供启动实例所需的信息，该实例是云中的虚拟服务器。
弹性块存储	为 AWS 云中的 Amazon EC2 实例提供持久性块存储卷。
简单存储服务 (S3)	互联网存储。它旨在让开发人员更轻松地进行网络规模计算。
弹性计算云 (EC2)	一种 Web 服务，可在云中提供安全、可调整大小的计算容量。它旨在让开发人员更轻松地进行网络规模云计算。
弹性负载均衡 (ELB)	将传入的应用程序流量分配到多个可用区中的多个 EC2 实例。这提高了应用程序的容错能力。
弹性网络接口 (ENI)	一个虚拟网络接口，您可以将其附加到虚拟私有云 (VPC) 中的实例。
弹性 IP (EIP) 地址	您在 Amazon EC2 或 Amazon VPC 中分配并附加到实例的静态公共 IPv4 地址。弹性 IP 地址与您的账户关联，而非特定实例。它们是弹性的，因为您可以根据需要轻松分配、附加、分离和释放它们。
实例类型	Amazon EC2 提供多种实例类型，经过优化以适应不同的用例。实例类型包含 CPU、内存、存储和网络容量的不同组合，让您可以灵活选择适合应用程序的资源组合。
身份和访问管理 (IAM)	一个具有权限策略的 AWS 身份，这些策略决定了该身份在 AWS 中可以做什么和不能做什么。您可以使用 IAM 角色使在 EC2 实例上运行的应用程序安全地访问您的 AWS 资源。在高可用性设置中部署 VPX 实例需要 IAM 角色。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

术语	定义
互联网网关	将网络连接到互联网。您可以将 VPC 外部 IP 地址的流量路由到互联网网关。
密钥对	一套安全凭证，用于以电子方式证明您的身份。密钥对由私钥和公钥组成。
路由表	一组路由规则，用于控制离开与路由表关联的任何子网的流量。您可以将多个子网与单个路由表关联，但一个子网一次只能与一个路由表关联。
安全组	为实例指定的一组允许的入站网络连接。
子网	VPC IP 地址范围的一个片段，EC2 实例可以附加到该片段。您可以创建子网，根据安全和操作需求对实例进行分组。
虚拟私有云 (VPC)	一种 Web 服务，用于预置 AWS 云中逻辑隔离的部分，您可以在其中在您定义的虚拟网络中启动 AWS 资源。
自动扩缩	一种 Web 服务，可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。
CloudFormation	一种用于编写或更改模板的服务，这些模板可将相关的 AWS 资源作为一个单元一起创建和删除。

AWS-VPX 支持矩阵

下表列出了支持的 VPX 型号以及 AWS 区域、实例类型和服务。

表 1：AWS 上支持的 VPX 型号

支持的 VPX 型号
NetScaler VPX 高级版 - 200 Mbps
NetScaler VPX 尊享版 - 1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持的 VPX 型号
NetScaler VPX 尊享版 - 5 Gbps
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

支持的 AWS 区域
美国西部（俄勒冈）
美国西部（北加利福尼亚）
美国东部（俄亥俄）
美国东部（弗吉尼亚北部）
亚太地区（孟买）
亚太地区（墨尔本）
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）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持的 AWS 区域
欧盟（法兰克福）
欧盟（爱尔兰）
欧盟（伦敦）
欧盟（巴黎）
欧盟（米兰）
南美洲（圣保罗）
AWS GovCloud（美国东部）
AWS GovCloud（美国西部）
AWS 绝密（C2S）
中东（巴林）
中东（阿联酋）
非洲（开普敦）
C2S

注意：

对于 AWS 香港区域，NetScaler VPX 支持仅适用于 BYOL 许可证。

表 3：支持的 AWS 实例类型

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持的 AWS 实例类型
c6in.large, c6in.xlarge, c6in.2xlarge, c6in.4xlarge, c6in.8xlarge, c6in.12xlarge, c6in.16xlarge, c6in.24xlarge, c6in.32xlarge
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 实例类型上预置的 NetScaler VPX 不支持 ENA 低延迟队列 (LLQ) 功能。

表 4：支持的 AWS 服务

支持的 AWS 服务
EC2： 启动 ADC 实例。
Lambda： 在通过 CFT 预置 NetScaler VPX 实例期间调用 NetScaler VPX NITRO API。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持的 AWS 服务
VPC 和 VPC 入口路由： VPC 创建隔离网络，可在其中启动 ADC。VPC 入口路由用于防火墙负载均衡解决方案。
Route53： 在 NetScaler 自动扩缩解决方案中，将流量分配到所有 NetScaler VPX 节点。
ELB： 在 NetScaler 自动扩缩解决方案中，将流量分配到所有 NetScaler VPX 节点。
Cloudwatch： 监控 NetScaler VPX 实例的性能和系统参数。
AWS 自动扩缩： 用于后端服务器自动扩缩。
Cloud formation： CloudFormation 模板用于部署 NetScaler VPX 实例。
简单队列服务 (SQS)： 监控后端自动扩缩中的扩容和缩容事件。
简单通知服务 (SNS)： 监控后端自动扩缩中的扩容和缩容事件。
身份和访问管理 (IAM)： 提供对 AWS 服务和资源的访问权限。
AWS Outposts： 在 AWS Outposts 中预置 NetScaler VPX 实例。

NetScaler 建议使用以下 AWS 实例类型：

- M6i 和 C5n 系列适用于市场版本或基于带宽的池许可。

采用池化或弹性许可的 VPX（带宽许可）	推荐的 AWS 实例
高达 200 Mbps	m6i.xlarge
1到5 Gbps	m6i.2xlarge
5到8 Gbps	c5n.4xlarge
8到25 Gbps	c5n.9xlarge

要根据每秒数据包数或 SSL 事务速率等指标确定适合您特定需求的实例，请联系您的 NetScaler 代表以获取指导。

限制和使用指南

在 AWS 上部署 NetScaler VPX 实例时，适用以下限制和使用指南：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 开始之前，请阅读 (/zh-cn/vpx/13-1/deploy-aws.html) 中“在 AWS 上部署 NetScaler VPX 实例”一节中的 AWS 术语部分。
- VPX 不支持群集功能。
- 为了使高可用性设置有效工作，请将专用 NAT 设备关联到管理接口，或将 EIP 关联到 NSIP。有关 NAT 的更多信息，请参阅 AWS 文档中的 NAT 实例。
- 数据流量和管理流量必须通过属于不同子网的 ENI 进行隔离。
- 管理 ENI 上只能存在 NSIP 地址。
- 如果使用 NAT 实例进行安全防护而不是将 EIP 分配给 NSIP，则需要进行适当的 VPC 级别路由更改。有关进行 VPC 级别路由更改的说明，请参阅 AWS 文档中的场景 2：具有公有和私有子网的 VPC。
- VPX 实例可以从一种 EC2 实例类型移动到另一种（例如，从 m3.large 移动到 m3.xlarge）。
- 对于 AWS 上的 VPX 存储选项，Citrix® 推荐使用 EBS，因为它具有持久性，并且即使从实例分离后数据仍然可用。
- 不支持将 ENI 动态添加到 VPX。重新启动 VPX 实例以应用更新。Citrix 建议您停止独立或 HA 实例，附加新的 ENI，然后重新启动实例。
- 您可以为 ENI 分配多个 IP 地址。每个 ENI 的最大 IP 地址数量由 EC2 实例类型决定，请参阅弹性网络接口中“每个实例类型每个网络接口的 IP 地址”一节。在将 IP 地址分配给 ENI 之前，您必须在 AWS 中分配这些 IP 地址。有关更多信息，请参阅弹性网络接口。
- Citrix 建议您避免在 NetScaler VPX 接口上使用 enable 和 disable 接口命令。
- NetScaler `set ha node \<NODE\_ID\> -haStatus STAYPRIMARY` 和 `set ha node \<NODE\_ID\> -haStatus STAYSECONDARY` 命令默认禁用。
- VPX 不支持 IPv6。
- 由于 AWS 限制，不支持以下功能：
  - 无偿 ARP (GARP)
  - L2 模式
  - 标记 VLAN
  - 动态路由
  - 虚拟 MAC
- 为了使 RNAT 正常工作，请确保禁用 **源/目标检查**。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 基础设施可能无法解析 AWS API 调用。如果 API 调用是通过 NetScaler VPX 实例上的非管理接口发出的，则会发生这种情

© 1997–2026 Citrix Systems, Inc. All rights reserved.

况。 作为一种变通方法，请将 API 调用限制为仅管理接口。为此，请在 VPX 实例上创建 NSVLAN，并使用相应的命令将管理接口绑定到 NSVLAN。 例如： `set ns config -nsvlan <vlan id> -ifnum 1/1 -tagged NO` `save config` 在提示符处重新启动 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，VPX 实例在 **监控** 选项卡下显示的 vCPU 使用率可能很高（高达 100%），即使实际使用率远低于此。要查看实际的 vCPU 使用率，请导航到 **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。

先决条件

在尝试在 AWS 中创建 VPX 实例之前，请确保您具备以下条件：

- **一个 AWS 账户**：用于在 AWS 虚拟私有云 (VPC) 中启动 NetScaler VPX AMI。您可以在 (http://www.aws.amazon.com) 免费创建一个 AWS 账户。
- **一个 AWS 身份和访问管理 (IAM) 用户账户**：用于安全地控制用户对 AWS 服务和资源的访问。有关如何创建 IAM 用户账户的更多信息，请参阅 创建 IAM 用户（控制台）。IAM 角色对于独立部署和高可用性部署都是强制性的。

  与您的 AWS 账户关联的 IAM 角色必须具有以下适用于各种场景的 IAM 权限。

  同一 AWS 区域中具有 IPv4 地址的 HA 对：

  ```
  "ec2:DescribeInstances",

  "ec2:AssignPrivateIpAddresses",

  "iam:SimulatePrincipalPolicy",

  "iam:GetRole",

  "ec2:CreateTags"
  ```

  同一 AWS 区域中具有 IPv6 地址的 HA 对：

  ```
  "ec2:DescribeInstances",

  "ec2:AssignIpv6Addresses",

  "ec2:UnassignIpv6Addresses",
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"iam:SimulatePrincipalPolicy",

"iam:GetRole",

"ec2:CreateTags"
```

同一 AWS 区域中同时具有 IPv4 和 IPv6 地址的 HA 对：

```
"ec2:DescribeInstances",

"ec2:AssignPrivateIpAddresses",

"ec2:AssignIpv6Addresses",

"ec2:UnassignIpv6Addresses",

"iam:SimulatePrincipalPolicy",

"iam:GetRole",

"ec2:CreateTags"
```

跨不同 AWS 区域具有弹性 IP 地址的 HA 对：

```
"ec2:DescribeInstances",

"ec2:DescribeAddresses",

"ec2:AssociateAddress",

"ec2:DisassociateAddress",

"iam:SimulatePrincipalPolicy",

"iam:GetRole",

"ec2:CreateTags"
```

跨不同 AWS 区域具有私有 IP 地址的 HA 对：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"ec2:DescribeInstances",

"ec2:DescribeRouteTables",

"ec2:DeleteRoute",

"ec2:CreateRoute",

"ec2:ModifyNetworkInterfaceAttribute",

"iam:SimulatePrincipalPolicy",

"iam:GetRole",

"ec2:CreateTags"
```

跨不同 AWS 区域同时具有私有 IP 和弹性 IP 地址的 HA 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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"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。
- 如果您使用 Citrix CloudFormation 模板，IAM 角色将自动创建。该模板不允许选择已创建的 IAM 角色。
- 当您通过 GUI 登录到 VPX 实例时，会出现一个提示，要求配置 IAM 角色所需的权限。如果您已配置权限，请忽略此提示。

- **AWS CLI**：用于从终端程序使用 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。您还需要 AWS CLI 来将网络接口类型更改为 SR-IOV。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **弹性网络适配器 (ENA)**：对于启用 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 及更高版本。
- 您必须在 EC2 实例上为 NetScaler VPX 配置实例元数据服务 (IMDS)。IMDSv1 和 IMDSv2 是从正在运行的 AWS EC2 实例访问实例元数据的两种可用模式。IMDSv2 比 IMDSv1 更安全。您可以将实例配置为使用这两种方法（默认选项）或仅使用 IMDSv2 模式（通过禁用 IMDSv1）。Citrix ADC VPX 从 NetScaler VPX 13.1.48.x 版本开始支持仅 IMDSv2 模式。

在 NetScaler VPX 实例上配置 AWS IAM 角色

在 Amazon EC2 实例上运行的应用程序必须在 AWS API 请求中包含 AWS 凭据。您可以将 AWS 凭据直接存储在 Amazon EC2 实例中，并允许该实例中的应用程序使用这些凭据。但您随后必须管理这些凭据，并确保它们安全地将凭据传递给每个实例，并在需要轮换凭据时更新每个 Amazon EC2 实例。这会增加大量额外工作。

相反，您可以使用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凭据。当您使用角色时，无需将长期凭据（例如用户名和密码或访问密钥）分发到 Amazon EC2 实例。相反，该角色提供临时权限，应用程序在调用其他 AWS 资源时可以使用这些权限。启动 Amazon EC2 实例时，您需要指定一个 IAM 角色以与该实例关联。然后，在该实例上运行的应用程序可以使用角色提供的临时凭据来签署 API 请求。

与您的 AWS 账户关联的 IAM 角色必须具有以下适用于各种场景的 IAM 权限。

在同一 AWS 区域中具有 IPv4 地址的 HA 对：

```
"ec2:DescribeInstances",

"ec2:AssignPrivateIpAddresses",

"iam:SimulatePrincipalPolicy",

"iam:GetRole"
```

在同一 AWS 区域中具有 IPv6 地址的 HA 对：

```
"ec2:DescribeInstances",

"ec2:AssignIpv6Addresses",

"ec2:UnassignIpv6Addresses",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"iam:SimulatePrincipalPolicy",

"iam:GetRole"
```

在同一 AWS 区域中同时具有 IPv4 和 IPv6 地址的 HA 对：

```
"ec2:DescribeInstances",

"ec2:AssignPrivateIpAddresses",

"ec2:AssignIpv6Addresses",

"ec2:UnassignIpv6Addresses",

"iam:SimulatePrincipalPolicy",

"iam:GetRole"
```

跨不同 AWS 区域具有弹性 IP 地址的 HA 对：

```
"ec2:DescribeInstances",

"ec2:DescribeAddresses",

"ec2:AssociateAddress",

"ec2:DisassociateAddress",

"iam:SimulatePrincipalPolicy",

"iam:GetRole"
```

跨不同 AWS 区域具有私有 IP 地址的 HA 对：

```
"ec2:DescribeInstances",

"ec2:DescribeRouteTables",

"ec2:DeleteRoute",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"ec2:CreateRoute",

"ec2:ModifyNetworkInterfaceAttribute",

"iam:SimulatePrincipalPolicy",

"iam:GetRole"
```

跨不同 AWS 区域同时具有私有 IP 和弹性 IP 地址的 HA 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",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"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，请使用每项功能的 IAM 权限组合。
- 如果您使用 Citrix CloudFormation 模板，IAM 角色将自动创建。该模板不允许选择已创建的 IAM 角色。
- 当您通过 GUI 登录到 VPX 实例时，会出现一个提示，要求配置 IAM 角色所需的权限。如果您已配置权限，请忽略该提示。
- IAM 角色对于独立部署和高可用性部署都是强制性的。

创建 IAM 角色

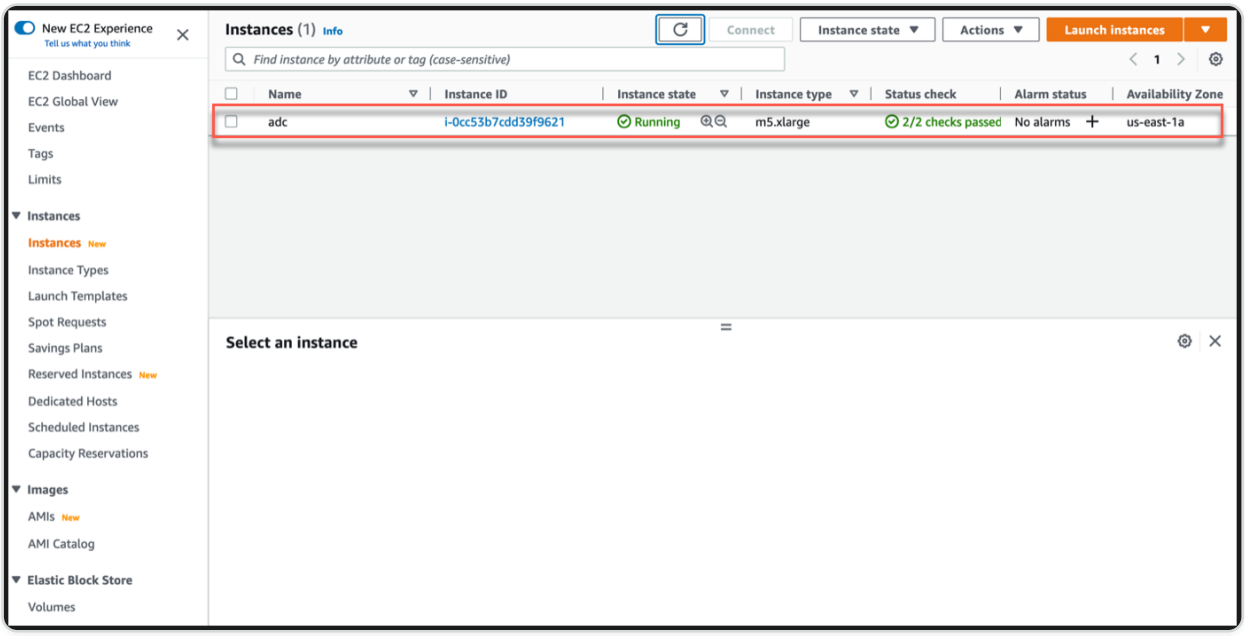
此过程描述了如何为 AWS 后端自动扩缩功能创建 IAM 角色。

注意：

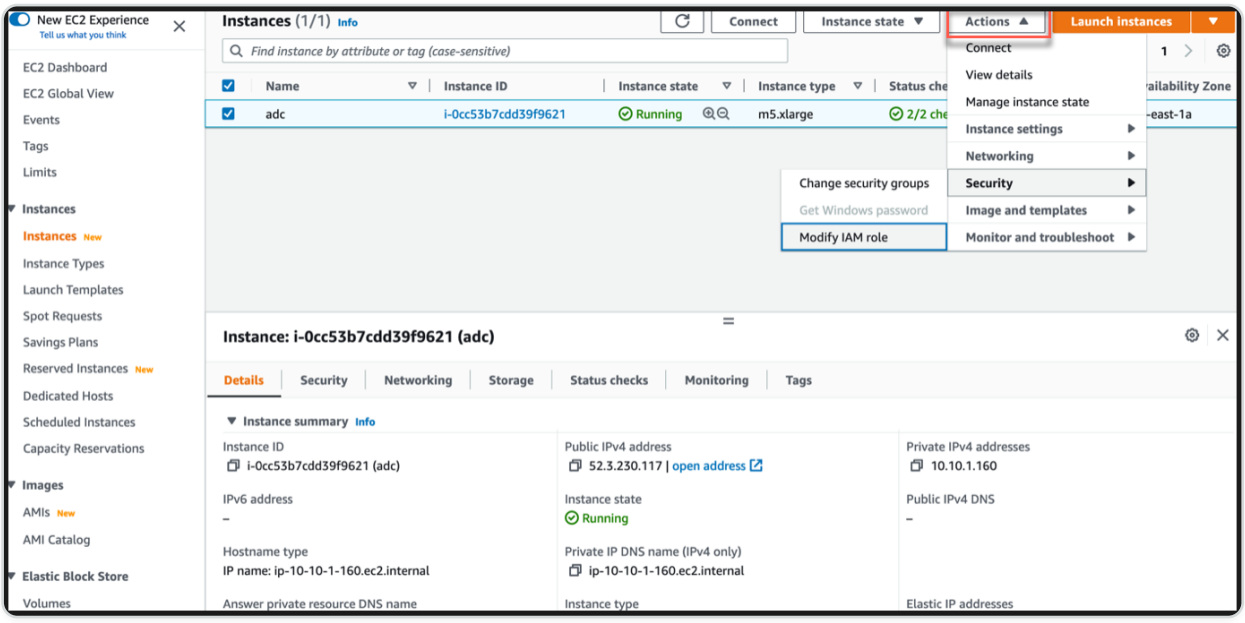
您可以按照相同的步骤创建与其它功能对应的任何 IAM 角色。

1. 登录到 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



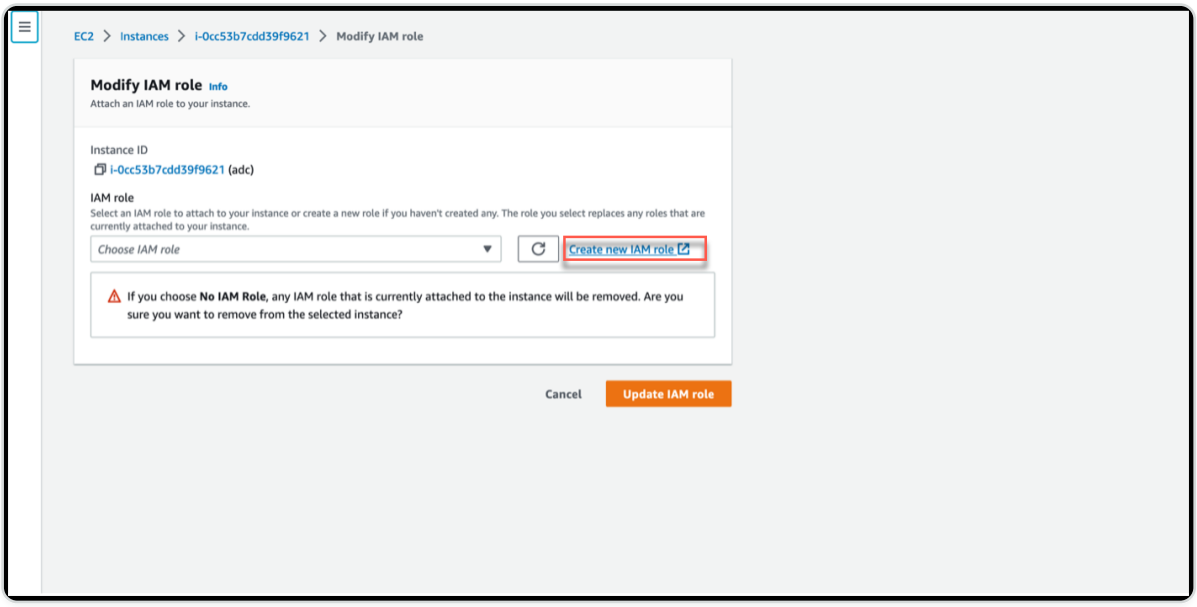
3. 导航到 **操作 > 安全 > 修改 IAM 角色**。



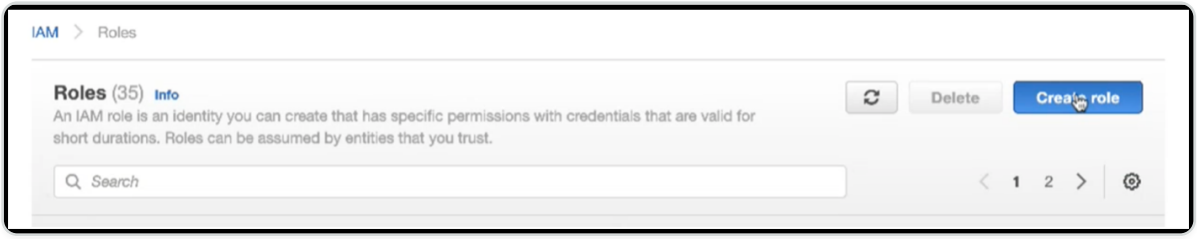
4. 在**修改 IAM 角色**页面中，您可以选择现有 IAM 角色或创建 IAM 角色。
5. 要创建 IAM 角色，请按照以下步骤操作：

   a. 在**修改 IAM 角色**页面中，单击**创建新 IAM 角色**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



b. 在**角色**页面中，单击**创建角色**。



c. 在**受信任实体类型**下选择**AWS 服务**，在**常见用例**下选择**EC2**，然后点击**下一步**。

d. 在**添加权限**页面中，点击**创建策略**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. 点击**JSON**选项卡以打开 JSON 编辑器。

f. 在 JSON 编辑器中，删除所有内容并粘贴您要使用的功能的 IAM 权限。

例如，粘贴以下用于 AWS 后端自动扩缩功能的 IAM 权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "autoscaling:*",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

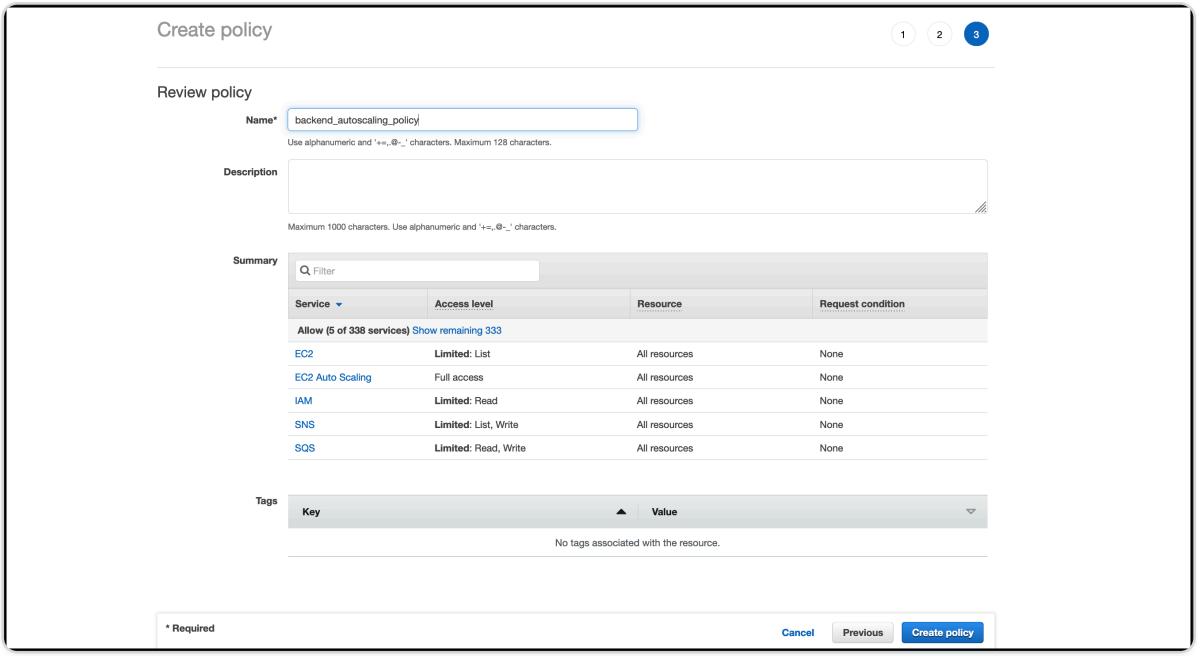
```
                "sns:CreateTopic",

                "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“Version”键值对与 AWS 自动生成的键值对相同。

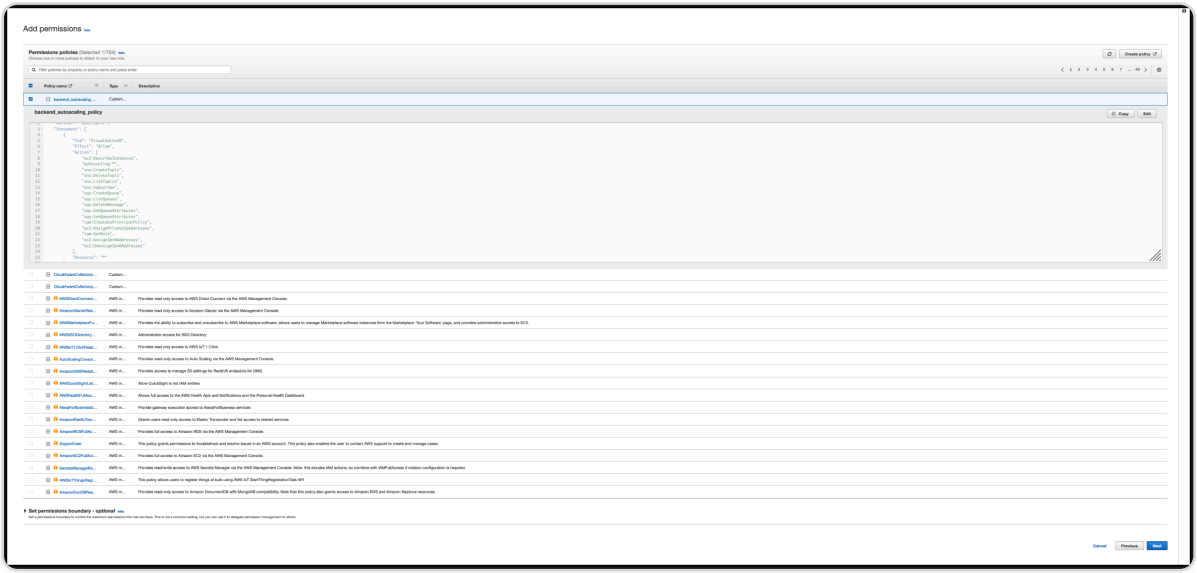
g. 点击**下一步: 审核**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

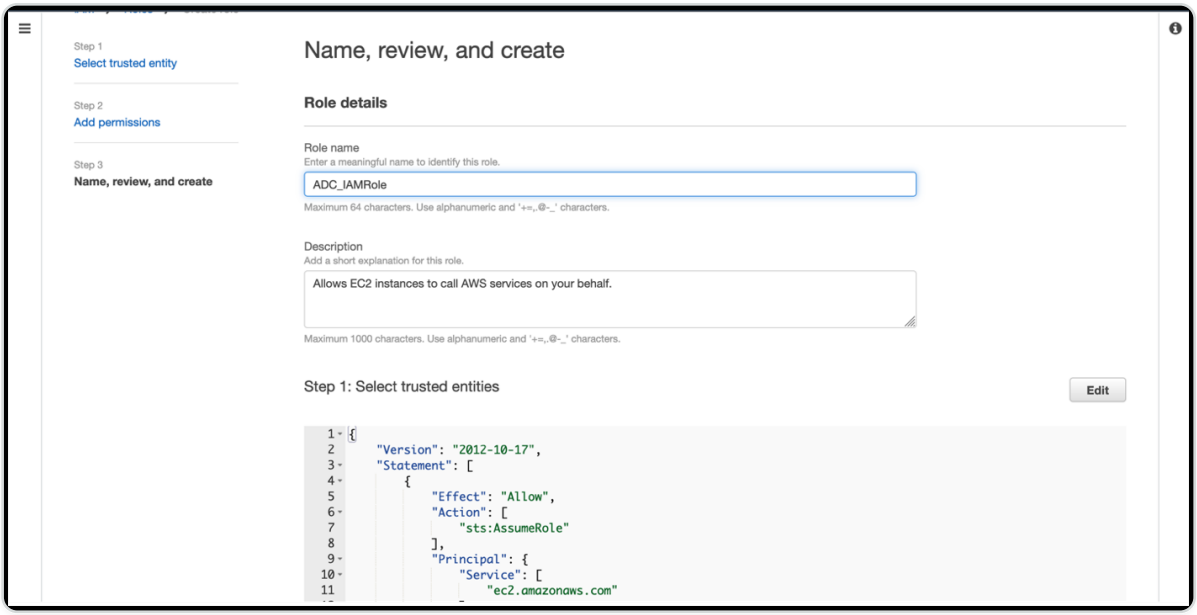
h. 在**审核策略**选项卡中，为策略指定一个有效名称，然后点击**创建策略**。



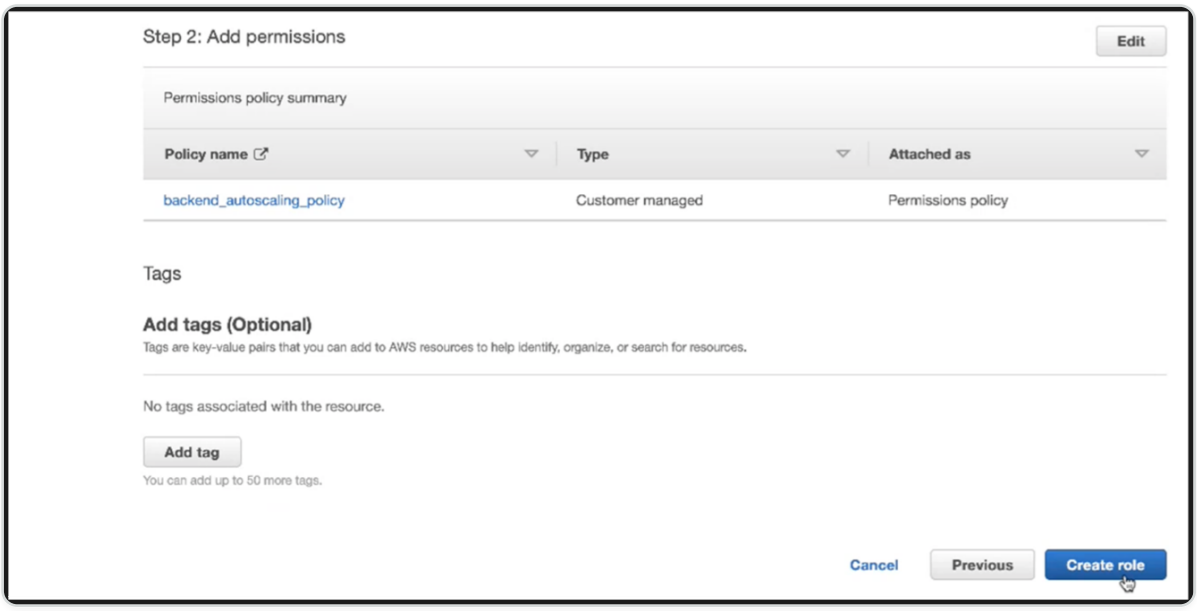
i. 在**身份访问管理**页面中，点击您创建的策略名称。展开策略以检查整个 JSON，然后点击**下一步**。



j. 在“**命名、审核和创建**”页面中，为角色指定一个有效名称。

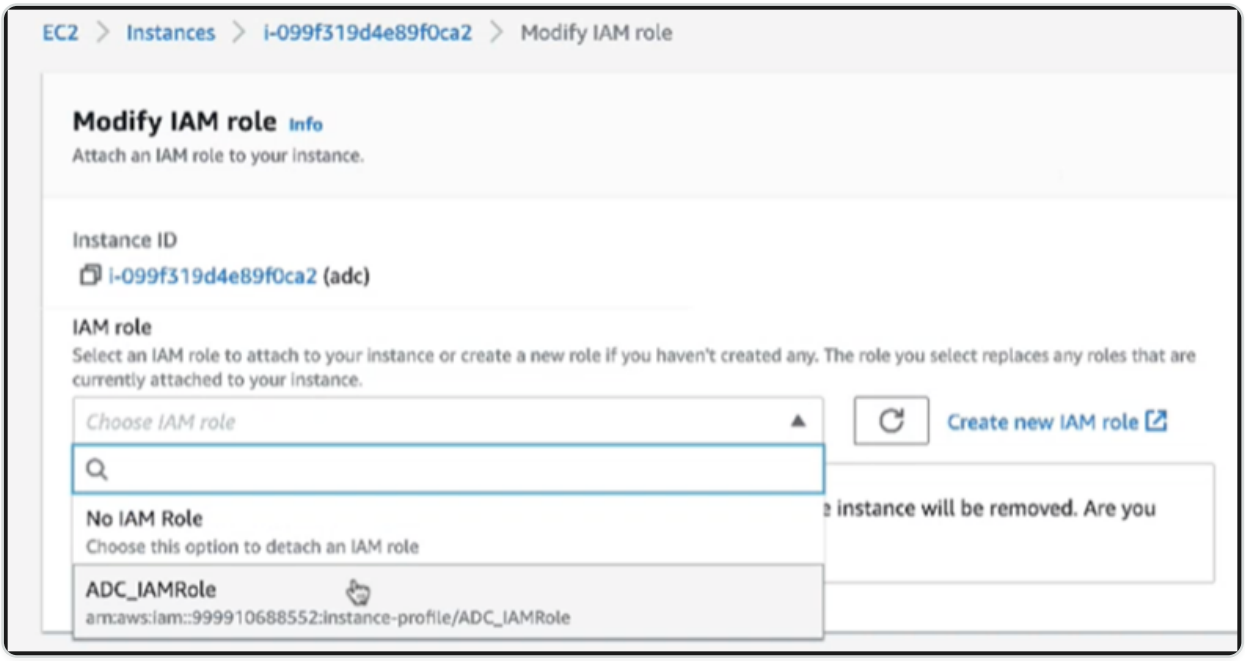


k. 单击“**创建角色**”。

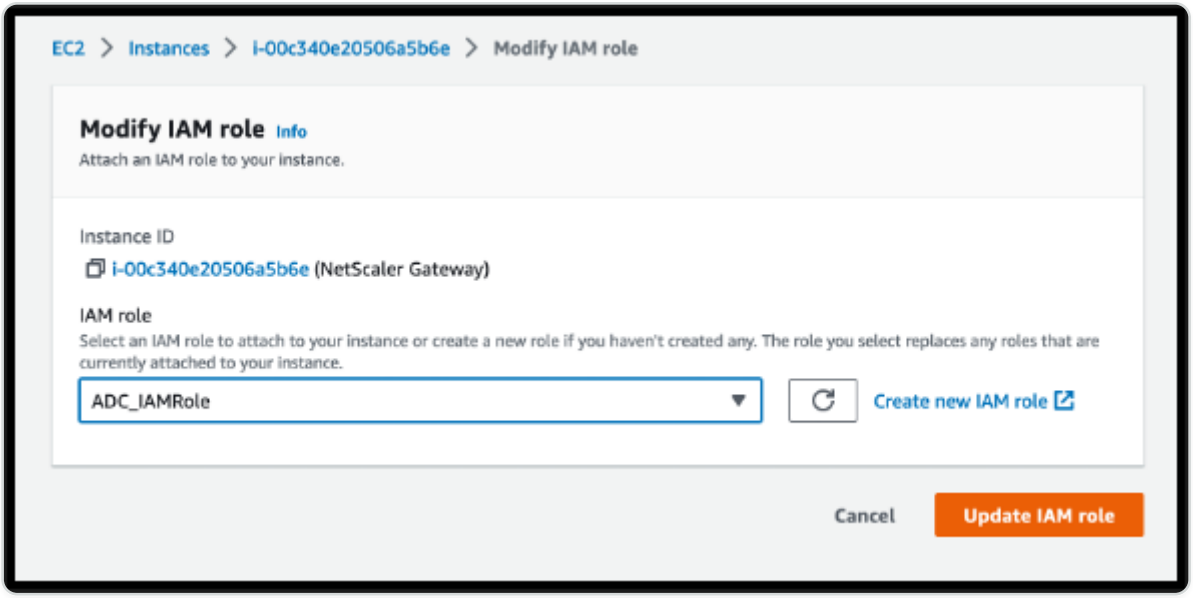


6. 重复步骤 1、2 和 3。选择“**刷新**”按钮，然后选择下拉菜单以查看您创建的角色。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. 单击“**更新 IAM 角色**”。

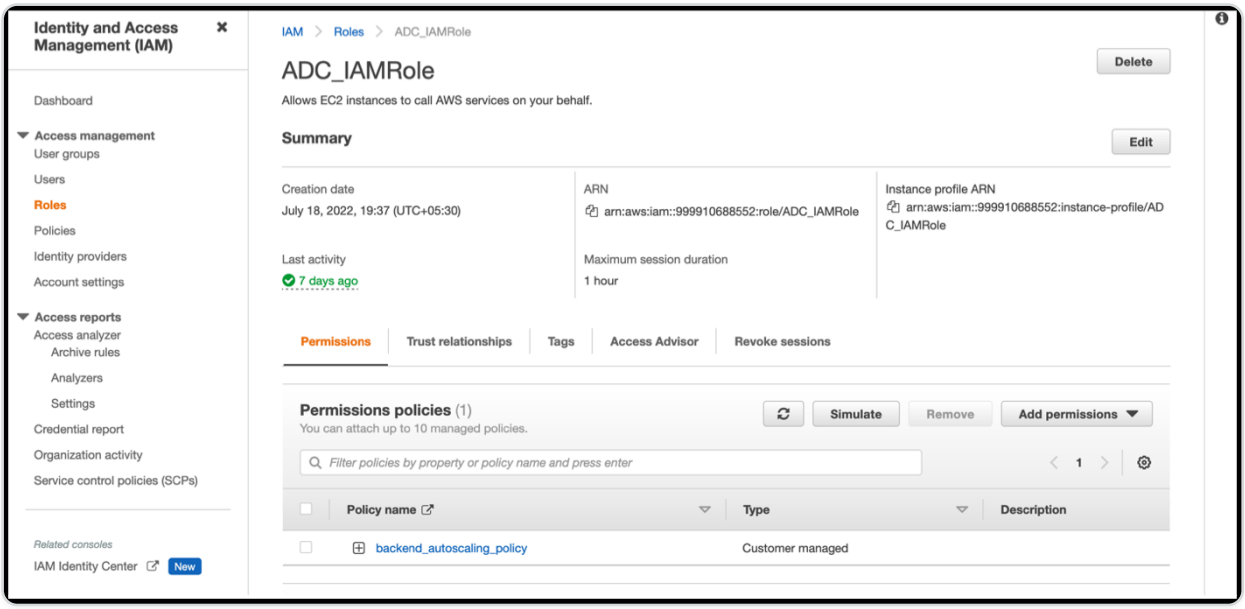


使用 IAM 策略模拟器测试 IAM 策略

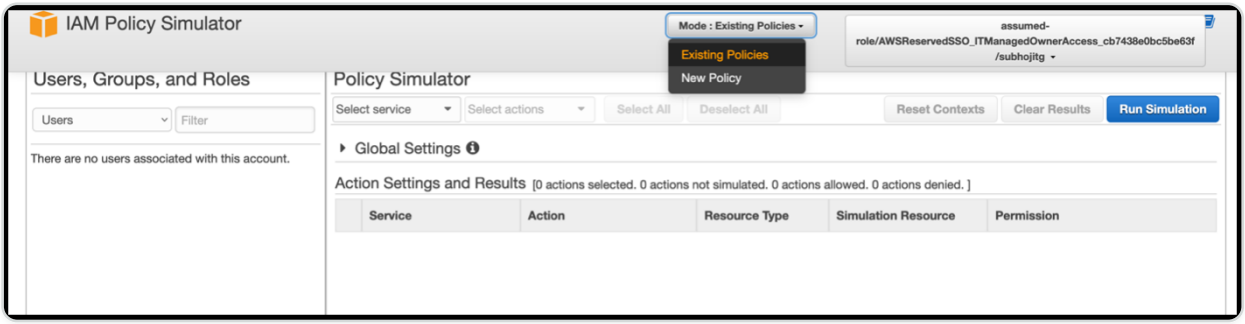
IAM 策略模拟器是一种工具，可让您在将 IAM 访问控制策略提交到生产环境之前测试其效果。它使验证和排查权限问题变得更加容易。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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**”，然后选择一个现有角色。

   选择现有角色(/en-us/vpx/media/iam-users-groups-roles.png)

4. 选择现有角色后，选择其下的现有策略。

   选择现有策略(/en-us/vpx/media/iam-users-groups-policies.png)

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。

   选择所需策略(/en-us/vpx/media/iam-policy-json.png)

6. 单击“**运行模拟**”。

   选择所需策略(/en-us/vpx/media/iam-run-simulation.png)

有关详细信息，请参阅 AWS IAM 文档。

其他参考

使用 IAM 角色向在 Amazon EC2 实例上运行的应用程序授予权限

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler VPX 实例在 AWS 上如何工作

NetScaler VPX 实例在 AWS Marketplace 中以 AMI 形式提供，可以作为 EC2 实例在 AWS VPC 中启动。NetScaler VPX AMI 实例至少需要 2 个虚拟 CPU 和 2 GB 内存。在 AWS VPC 中启动的 EC2 实例还可以提供 VPX 配置所需的多个接口、每个接口多个 IP 地址以及公共和私有 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® 建议为 AWS 上标准 VPX 实例安装配置三个网络接口。

AWS 目前仅向在 AWS VPC 中运行的实例提供多 IP 功能。VPC 中的 VPX 实例可用于对在 EC2 实例中运行的服务器进行负载均衡。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 账户在每个 AWS 区域最多可以创建 5 个 VPC 实例。您可以通过提交 Amazon 的请求表单 `<http://aws.amazon.com/contact-us/vpc-request>` 来请求更高的 VPC 限制。

图 1. AWS 架构上的 NetScaler VPX 实例部署示例

© 1997–2026 Citrix Systems, Inc. All rights reserved.

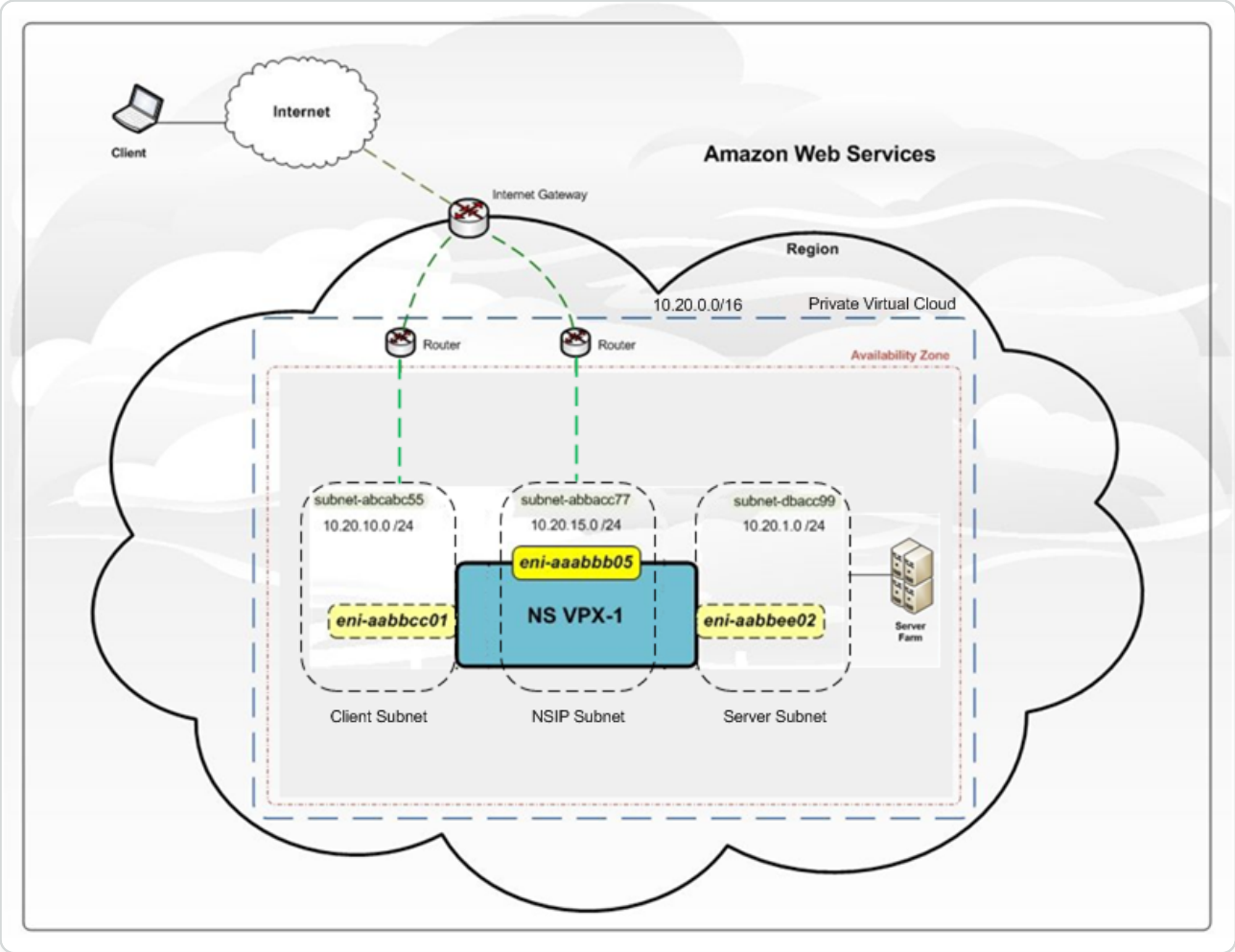


图 1 显示了具有 NetScaler VPX 部署的 AWS VPC 的简单拓扑。 AWS VPC 具有：

1. 一个 Internet 网关，用于路由进出 VPC 的流量。
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. 互联网网关与两个子网（管理和客户端）之间的网络连接。
5. 部署在 VPC 内的独立 NetScaler VPX 实例。该 VPX 实例有三个 ENI，每个子网连接一个。

在 AWS 上部署 NetScaler VPX 独立实例

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

本主题介绍了在 AWS 上部署 NetScaler VPX 实例的步骤。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在开始部署之前，请阅读以下主题：

- 先决条件
- 限制和使用指南

使用 AWS Web 控制台在 AWS 上部署 NetScaler VPX 实例

您可以通过 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. 创建互联网网关
7. 创建 NetScaler VPX 实例
8. 创建并附加更多网络接口
9. 将弹性 IP 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。要登录到您的实例，您必须创建一个密钥对，在启动实例时指定密钥对的名称，并在连接到实例时提供私钥。

当您使用 AWS 启动实例向导审查并启动实例时，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 中。VPC 允许您定义专用于您的 AWS 账户的虚拟网络。有关 AWS VPC 的更多信息，请参阅 Amazon VPC 入门。

为 NetScaler VPX 实例创建 VPC 时，请记住以下几点。

- 使用“仅包含单个公共子网的 VPC”选项在 AWS 可用区中创建 AWS VPC。
- Citrix 建议您至少创建以下类型的**三个子网**：
  - 一个用于管理流量的子网。您将管理 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 一个或多个用于客户端访问（用户到 NetScaler VPX）流量的子网，客户端通过这些子网连接到一个或多个分配给 NetScaler 负载均衡虚拟服务器的虚拟 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，您的服务器通过这些子网连接到 VPX 拥有的子网 IP (SNIP) 地址。有关 NetScaler 负载均衡和虚拟服务器、虚拟 IP 地址 (VIP) 和子网 IP 地址 (SNIP) 的更多信息，请参阅：
- 所有子网必须位于同一可用区。

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 将子网添加到您的 VPC。

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中添加规则。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，这些安全组由 AWS Marketplace 生成，并基于 Citrix 推荐的设置。但是，您可以根据自己的要求创建更多安全组。

注意：

安全组上需打开端口 22、80、443，分别用于 SSH、HTTP 和 HTTPS 访问。

步骤 5：添加路由表。

路由表包含一组称为路由的规则，用于确定网络流量的去向。VPC 中的每个子网都必须与一个路由表关联。有关如何创建路由表的更多信息，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 路由表中为可路由到 Internet 的流量提供目标，以及为已分配公共 IPv4 地址的实例执行网络地址转换 (NAT)。

为 Internet 流量创建 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 部分。

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. 在 AWS 控制面板中，转至 **计算 > EC2 > 启动实例 > AWS Marketplace**。

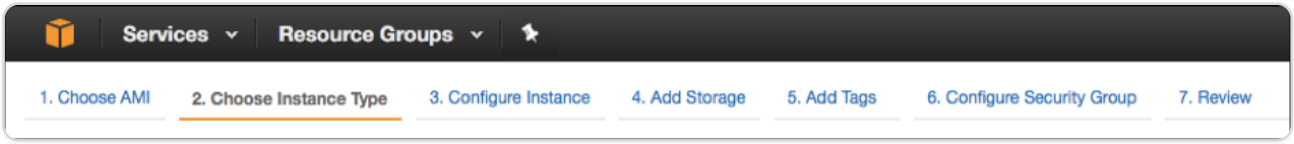
© 1997–2026 Citrix Systems, Inc. All rights reserved.

在单击“**启动实例**”之前，请通过检查“**启动实例**”下方的说明来确保您的区域正确无误。

2. 在“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“**选择**”。对于 NetScaler VPX 版本，您有以下选项：
   - 许可版本
   - NetScaler VPX Express 设备（这是一个免费的虚拟设备，可从 NetScaler 12.0 56.20 版本开始提供。）
   - 自带设备

启动实例向导随即开始。按照向导创建实例。向导会提示您：

- 选择实例类型
- 配置实例
- 添加存储
- 添加标签
- 配置安全组
- 审核



步骤 8：创建并附加更多网络接口。

为 VIP 和 SNIP 创建另外两个网络接口。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。

创建网络接口后，必须将其附加到 VPX 实例。在附加接口之前，请关闭 VPX 实例，附加接口，然后启动实例。有关如何附加网络接口的详细信息，请参阅启动实例时附加网络接口 部分。

步骤 9：分配和关联弹性 IP。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

如果将公共 IP 地址分配给 EC2 实例，则该地址仅在实例停止之前保持分配状态。之后，该地址将释放回池中。重新启动实例时，将分配新的公共 IP 地址。

相比之下，弹性 IP (EIP) 地址会一直保持分配状态，直到该地址与实例解除关联。

为管理 NIC 分配并关联弹性 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

这些步骤完成了在 AWS 上创建 NetScaler VPX 实例的过程。实例准备就绪可能需要几分钟。检查您的实例是否已通过其状态检查。您可以在“实例”页面上的“**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，您可以使用 GUI 和 SSH 客户端连接该实例。

- GUI

以下是访问 NetScaler VPX 实例的默认管理员凭据

用户名：`nsroot`

密码：ns root 账户的默认密码设置为 NetScaler VPX 实例的 AWS 实例 ID。首次登录时，系统会提示您出于安全原因更改密码。更改密码后，您必须保存配置。如果未保存配置且实例重新启动，则必须使用默认密码登录。在提示符下再次更改密码。

- 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 **连接到您的实例** 页面上的说明进行操作。

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。该模板提供启动单个 NetScaler VPX 实例的功能，或创建包含一对 NetScaler VPX 实例的高可用性环境的功能。

您可以从 AWS Marketplace 或 GitHub 启动该模板。

CloudFormation 模板需要现有的 VPC 环境，它会启动一个具有三个弹性网络接口 (ENI) 的 VPX 实例。在启动 CloudFormation 模板之前，请确保您已完成以下要求：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 一个 AWS 虚拟私有云 (VPC)
- VPC 中的三个子网：一个用于管理，一个用于客户端流量，一个用于后端服务器
- 一个 EC2 密钥对，用于启用对实例的 SSH 访问
- 一个安全组，开放 UDP 3003、TCP 3009–3010、HTTP、SSH 端口

有关如何完成先决条件的更多信息，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。

此外，您可以使用 GitHub 中提供的 Citrix CloudFormation 模板配置并启动 NetScaler VPX Express 独立实例：

`<https://github.com/citrix/citrix-adc-aws-cloudformation/tree/master/templates/standalone/>`

IAM 角色对于独立部署不是强制性的。但是，Citrix 建议您为实例创建并附加具有所需权限的 IAM 角色，以备将来之需。IAM 角色可确保在需要时，独立实例可以轻松转换为具有 SR-IOV 的高可用性节点。

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 CloudWatch 服务默认启用。如果您使用 Citrix CloudFormation 模板部署 NetScaler VPX 实例，则默认选项为“是”。如果您想禁用 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

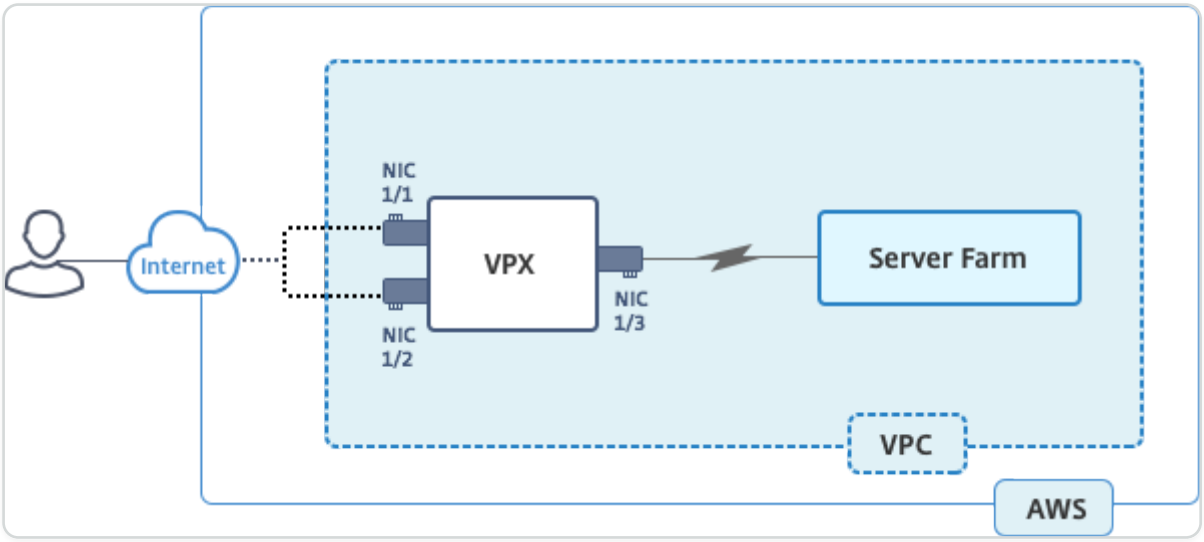
您可以使用 AWS CLI 启动实例。有关更多信息，请参阅AWS 命令行界面文档。

场景：独立实例

此场景说明了如何使用 AWS GUI 在 AWS 中部署 NetScaler VPX 独立 EC2 实例。创建一个具有三个 NIC 的独立 VPX 实例。该实例配置为负载均衡虚拟服务器，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互联网上的外部主机之间所需的通信路由。

有关部署 VPX 实例过程的更多详细信息，请参阅在 AWS 上部署 NetScaler VPX 独立实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



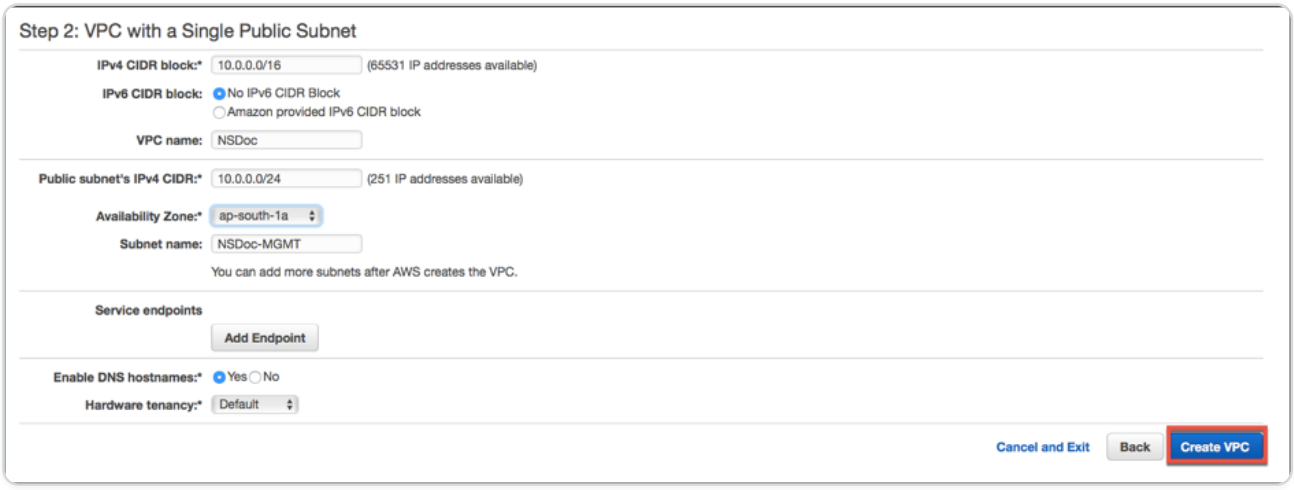
创建三个 NIC。每个 NIC 可以配置一对 IP 地址（公共和私有）。这些 NIC 用于以下目的。

NIC	用途	关联到
eth0	用于管理流量 (NSIP)	一个公共 IP 地址和一个私有 IP 地址
eth1	用于客户端流量 (VIP)	一个公共 IP 地址和一个私有 IP 地址
eth2	与后端服务器通信 (SNIP)	一个公共 IP 地址（私有 IP 地址非强制要求）

步骤 1：创建 VPC。

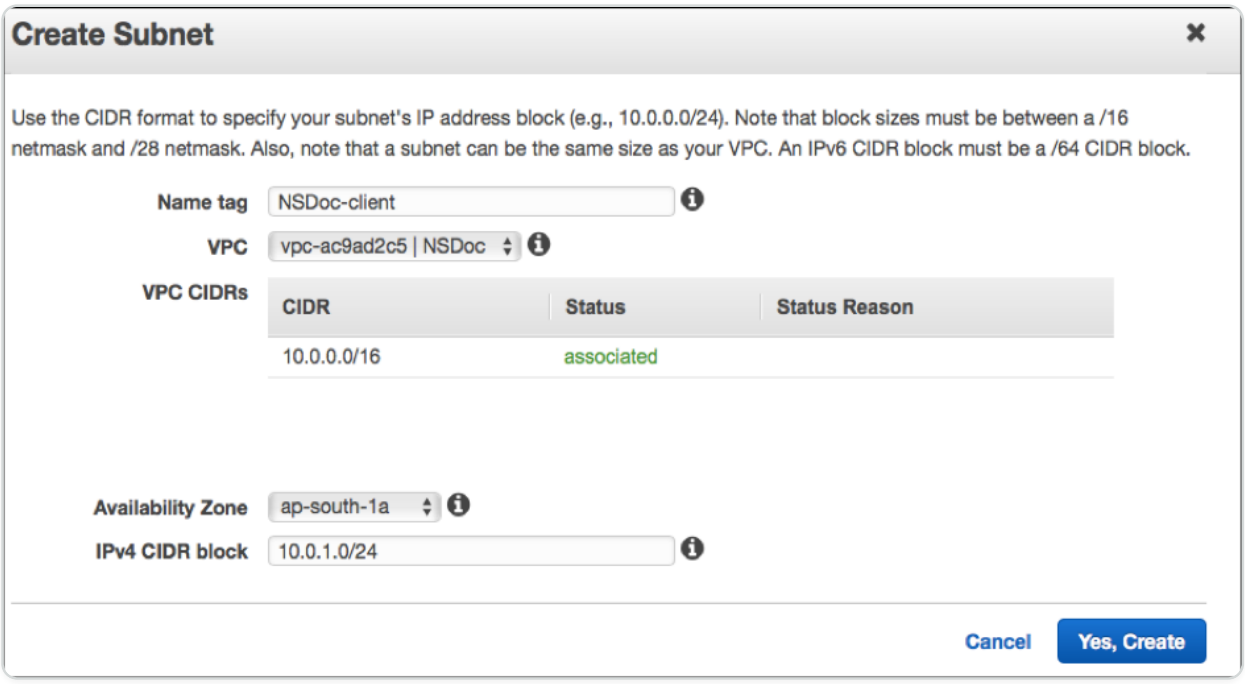
1. 登录 AWS Web 控制台，导航到 **Networking & Content Delivery \> VPC**。点击 **Start VPC Wizard**。
2. 选择 **VPC with a Single Public Subnet**，然后点击 **Select**。
3. 将 IP CIDR 块设置为 10.0.0.0/16，用于此场景。
4. 为 VPC 命名。
5. 将公共子网设置为 10.0.0.0/24。（这是管理网络）。
6. 选择一个可用区。
7. 为子网命名。
8. 点击创建 **VPC**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



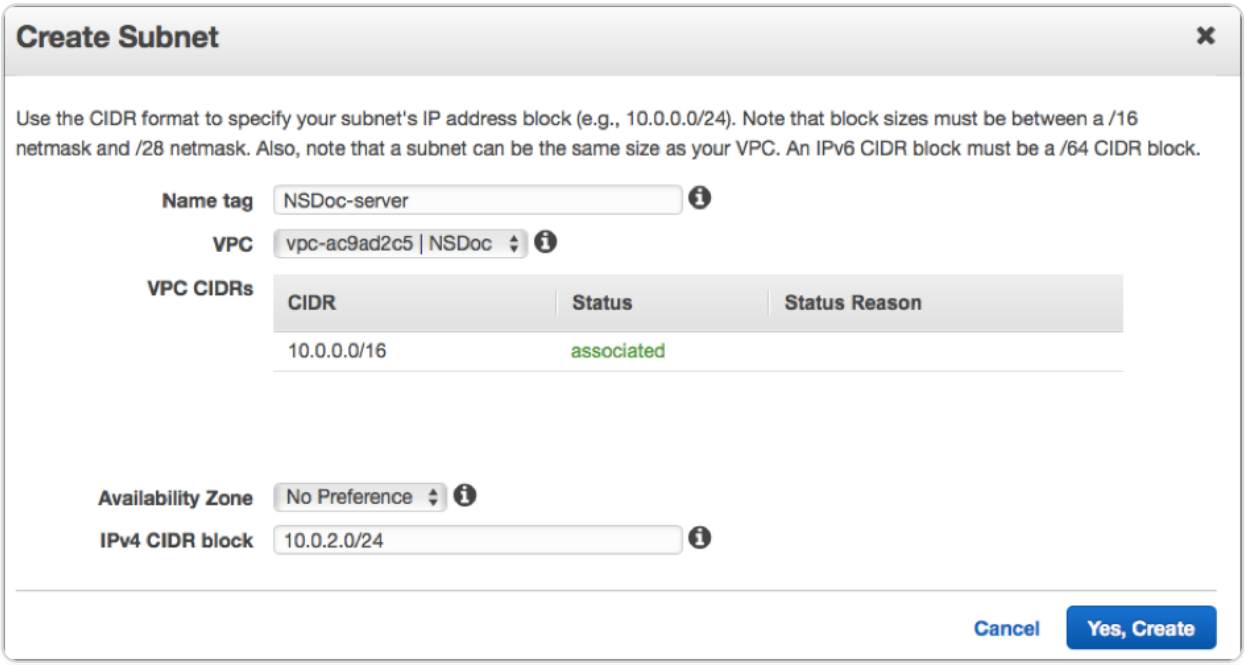
步骤 2：创建额外子网。

1. 在 `<https://console.aws.amazon.com/vpc/>` 打开 Amazon VPC 控制台。
2. 在导航窗格中，输入以下详细信息后，选择 Subnets，然后选择 Create Subnet。
   - 名称标签：为您的子网提供一个名称。
   - VPC：选择您要为其创建子网的 VPC。
   - 可用区：选择您在步骤 1 中创建 VPC 的可用区。
   - IPv4 CIDR 块：为您的子网指定一个 IPv4 CIDR 块。对于此场景，请选择 10.0.1.0/24。



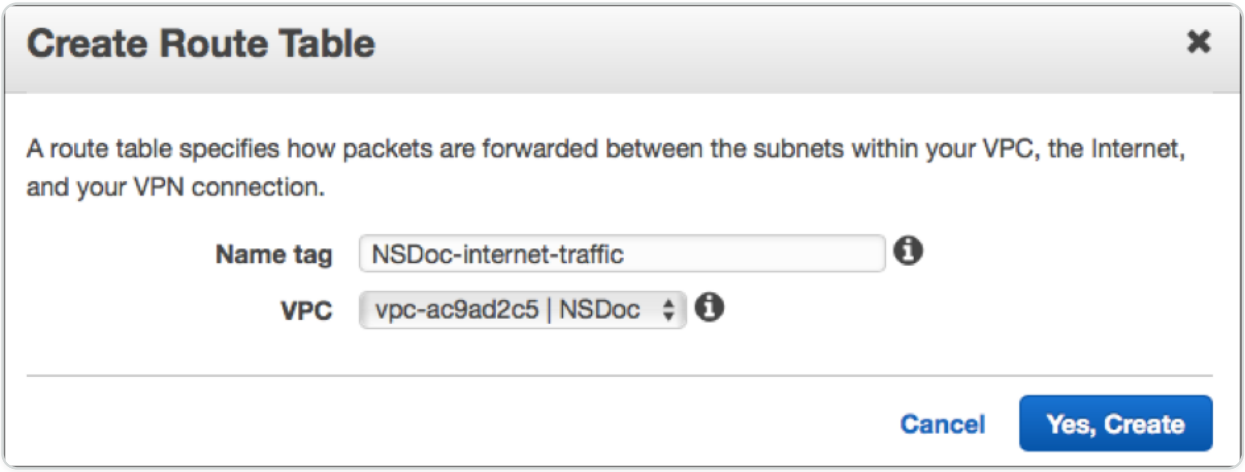
3. 重复这些步骤，再创建一个用于后端服务器的子网。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



步骤 3：创建路由表。

1. 在 `<https://console.aws.amazon.com/vpc/>` 打开 Amazon VPC 控制台。
2. 在导航窗格中，选择 **路由表** > **创建路由表**。
3. 在“创建路由表”窗口中，添加一个名称并选择您在步骤 1 中创建的 VPC。
4. 点击 **是，创建**。



路由表将分配给您为此 VPC 创建的所有子网，以便来自一个子网中实例的流量可以路由到另一个子网中的实例。

5. 点击“子网关联”，然后点击 **编辑**。
6. 点击管理和客户端子网，并点击**保存**。这将创建一个仅用于互联网流量的路由表。

   关联场景路由表(/en-us/vpx/media/routetable-associate-scenario.png)

7. 点击**路由** > **编辑** > **添加另一个路由**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. 在目标字段中添加 0.0.0.0/0，然后点击目标字段以选择 igw-\<xxxx\>，这是 VPC 向导自动创建的互联网网关。
9. 点击**保存**。

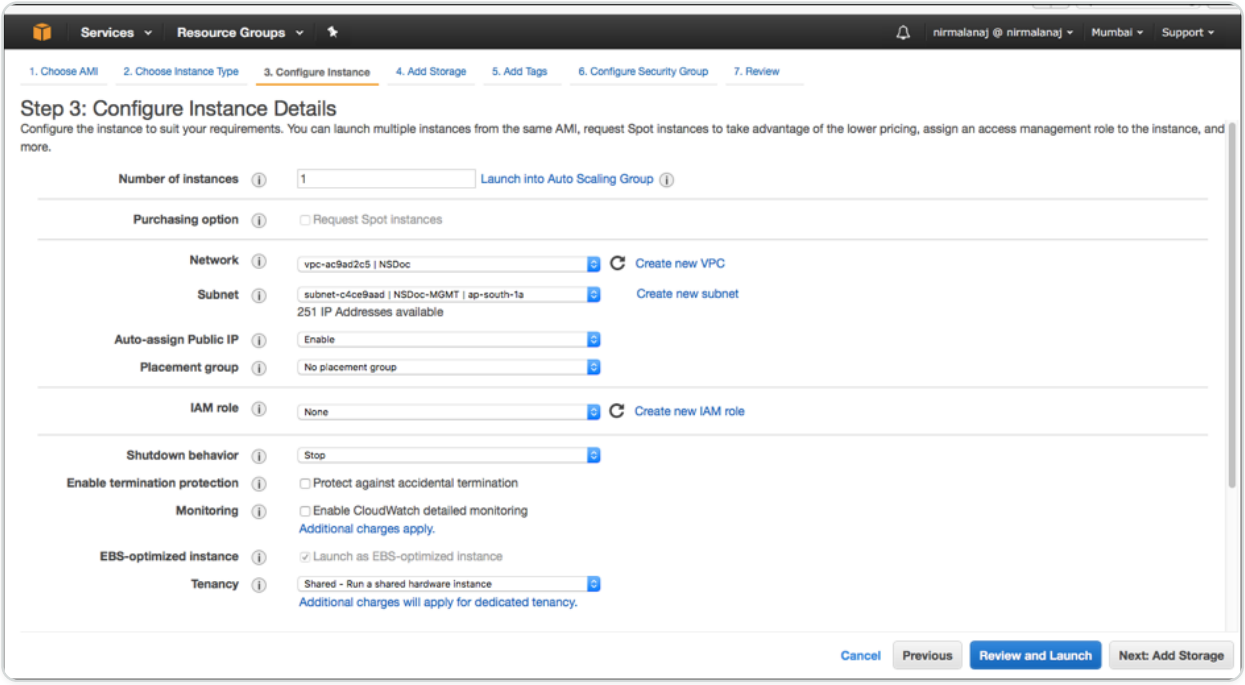
   为场景添加网关(/en-us/vpx/media/add-gateway-scenario.png)

10. 按照步骤创建用于服务器端流量的路由表。

步骤 4：创建 NetScaler VPX 实例。

1. 登录 AWS 管理控制台，并在**计算**下点击 **EC2**。
2. 点击 AWS Marketplace。在“搜索 AWS Marketplace”栏中，键入 NetScaler VPX 并按 Enter 键。将显示可用的 NetScaler VPX 版本。
3. 点击**选择**以选择所需的 NetScaler VPX 版本。EC2 实例向导将启动。
4. 在**选择实例类型**页面上，选择 **m4. 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”页面上，选择以下内容，然后点击“下一步：添加存储”。

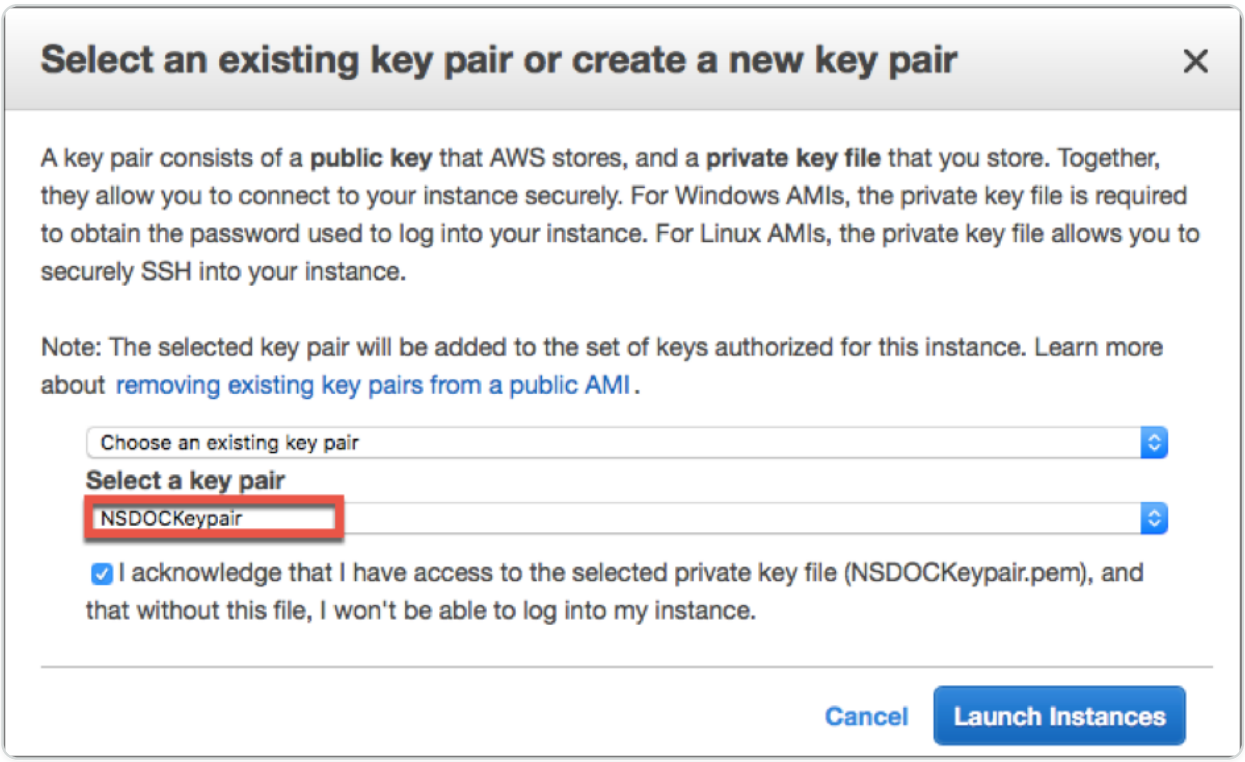
   - 实例数量：1
   - 网络：在步骤 1 中创建的 VPC
   - 子网：管理子网
   - 自动分配公有 IP：启用



6. 在“添加存储”页面上，选择默认选项，然后单击“下一步: 添加标签”。
7. 在“添加标签”页面上，为实例添加名称，然后单击“下一步: 配置安全组”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. 在“配置安全组”页面上，选择默认选项（由 AWS Marketplace 生成，并基于 Citrix® Systems 的推荐设置），然后单击“**审核和启动 > 启动**”。
9. 系统会提示您选择现有密钥对或创建新密钥对。从“选择密钥对”下拉列表中，选择您作为先决条件创建的密钥对（请参阅“先决条件”部分）。
10. 选中该复选框以确认密钥对，然后单击“启动实例”。



启动实例向导显示启动状态，实例完全启动后，它会显示在实例列表中。

要检查实例，请转到 AWS 控制台，单击 EC2 > 正在运行的实例。选择实例并添加名称。确保实例状态为“正在运行”且“状态检查”已完成。

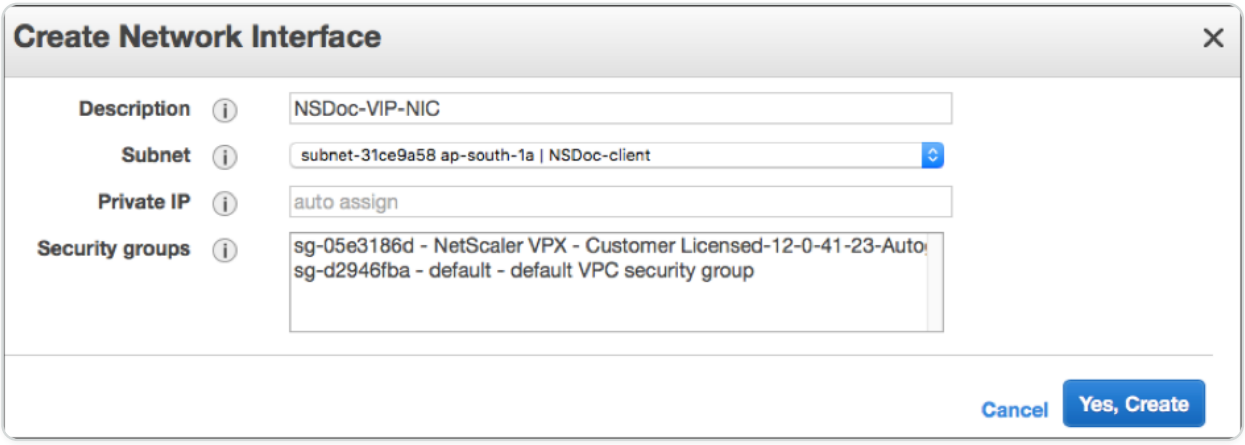
步骤 5：创建并附加更多网络接口。

创建 VPC 时，只有一个网络接口与其关联。现在，为 VPC 添加另外两个网络接口，用于 VIP 和 SNIP。

1. 在 `<https://console.aws.amazon.com/ec2/>` 处打开 Amazon EC2 控制台。
2. 在导航窗格中，选择“网络接口”。
3. 选择创建网络接口。
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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

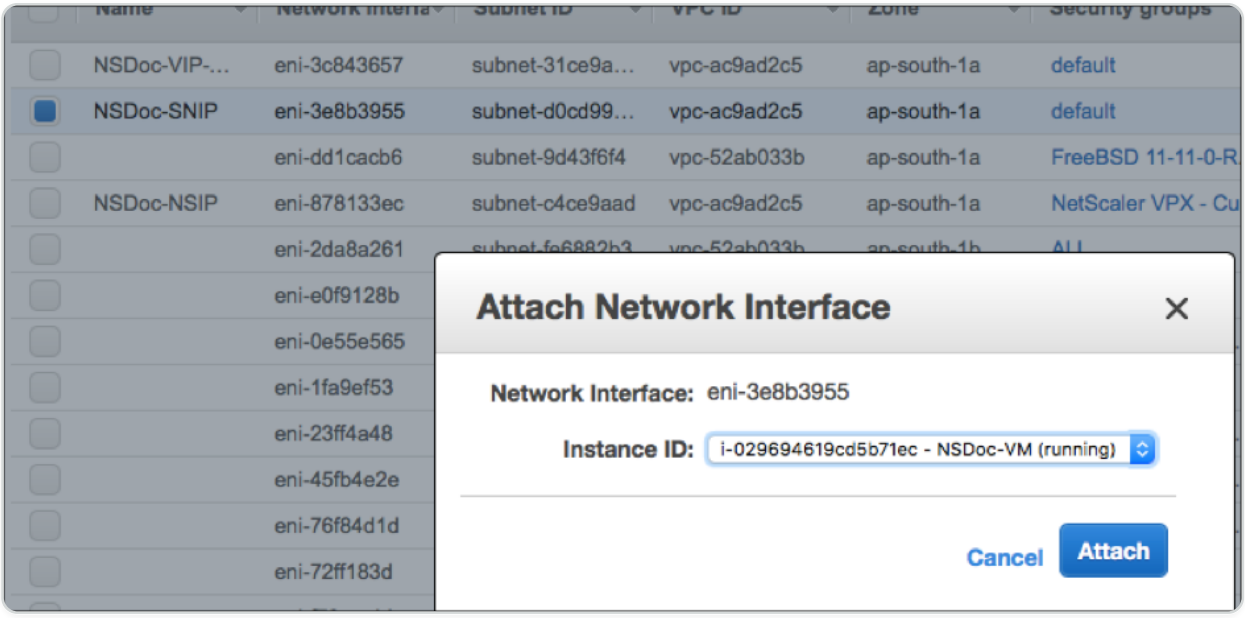
7. 对于安全组，选择该组。
8. 单击 **是，创建**。



9. 创建网络接口后，为该接口添加一个名称。
10. 重复这些步骤，为服务器端流量创建网络接口。

附加网络接口：

1. 在导航窗格中，选择网络接口。
2. 选择网络接口并选择附加。
3. 在“附加网络接口”对话框中，选择实例并选择附加。

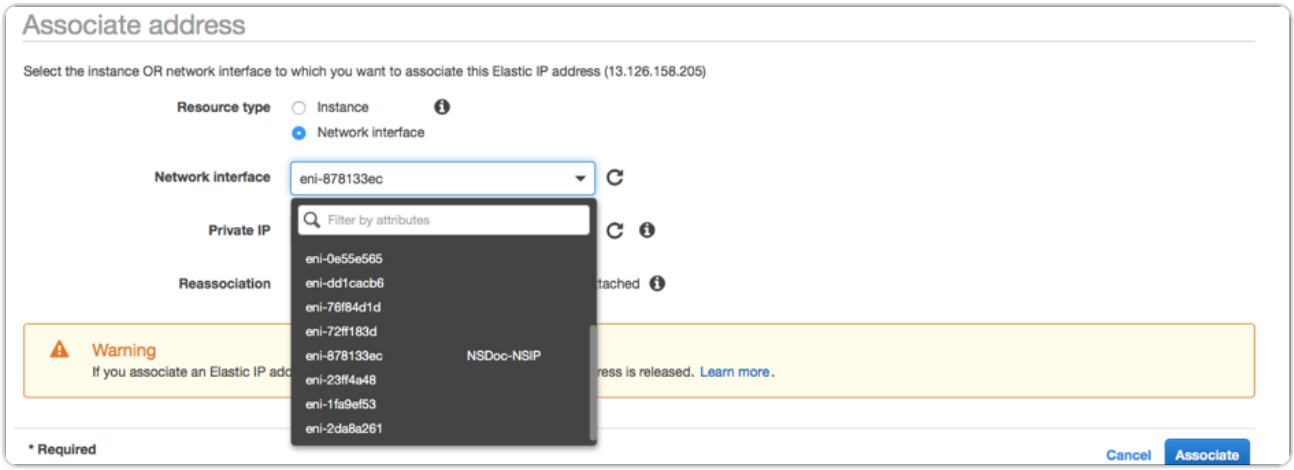


步骤 6：将弹性 IP 附加到 NSIP。

1. 从 AWS 管理控制台，转到 **网络与安全 > 弹性 IP**。
2. 检查是否有可用的空闲 EIP 进行附加。如果没有，请单击 **分配新地址**。
3. 选择新分配的 IP 地址，然后选择 **操作 > 关联地址**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 单击 **网络接口** 单选按钮。
5. 从“网络接口”下拉列表中，选择管理 NIC。
6. 从 **私有 IP** 下拉菜单中，选择 AWS 生成的 IP 地址。
7. 选中 **重新关联** 复选框。
8. 单击 **关联**。



访问 VPX 实例：

配置具有三个 NIC 的独立 NetScaler VPX 实例后，登录到 VPX 实例以完成 NetScaler 端的配置。使用以下选项：

- GUI：在浏览器中键入管理 NIC 的公共 IP。使用 `nsroot` 作为用户名，实例 ID (i-0c1ffe1d987817522) 作为密码登录。

> **注意：**
>
> 首次登录时，系统会提示您出于安全原因更改密码。更改密码后，必须保存配置。如果未保存配置且实例重新启动，则必须使用默认密码登录。在提示符下再次更改密码并保存配置。

- SSH：打开 SSH 客户端并键入：

```
ssh -i \<location of your private key\> ns root@\<public DNS of the instance\>
```

要查找公共 DNS，请单击实例，然后单击“**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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 您已配置 NetScaler VPX 设备的 BYOL 版本，有关详细信息，请参阅 `<https://support.citrix.com/s/article/CTX255959-how-to-allocate-and-install-citrix-netscaler-vpx-licenses?language=en_US>` 处的 VPX 许可指南

下载 NetScaler VPX 许可证

从 AWS Marketplace 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。

您必须执行以下操作：

1. 使用 Citrix® 网站中的许可门户生成有效许可证。
2. 将许可证上传到实例。

如果这是 **付费** Marketplace 实例，则无需安装许可证。正确的功能集和性能将自动激活。

如果您使用的 NetScaler VPX 实例型号高于 VPX 5000，则网络吞吐量可能与实例许可证中指定的吞吐量不同。但是，其他功能（例如 SSL 吞吐量和每秒 SSL 事务数）可能会有所改善。

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

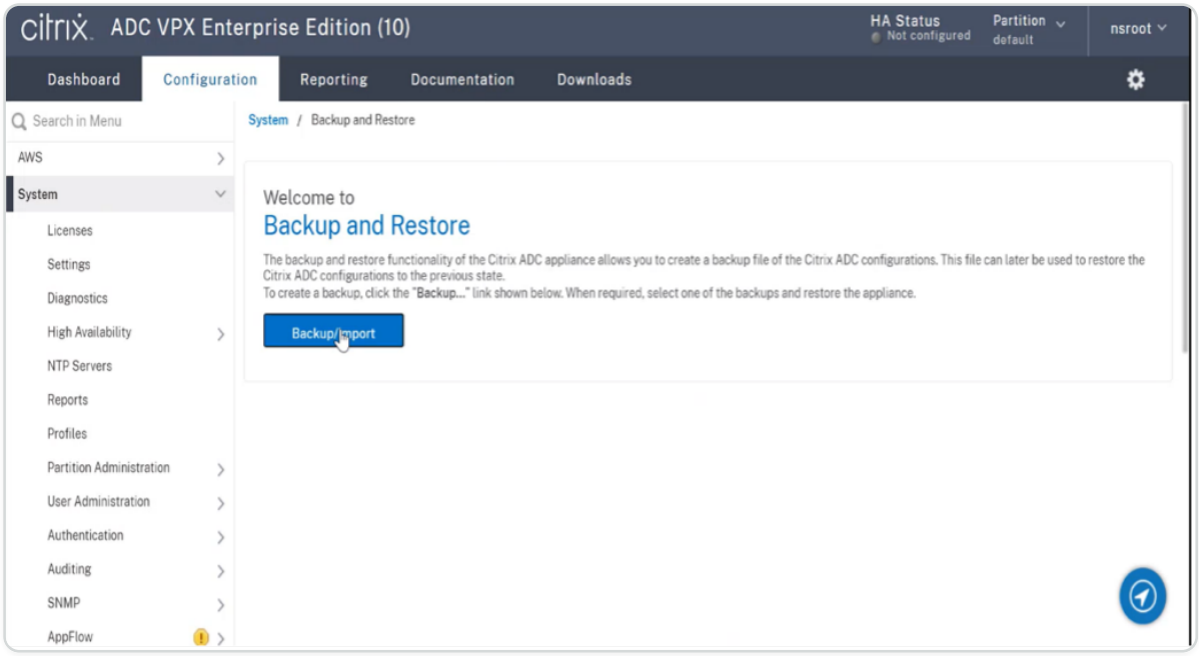
本节介绍从 AWS 订阅迁移到自带许可证 (BYOL) 的过程，反之亦然。

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 门户上完成。

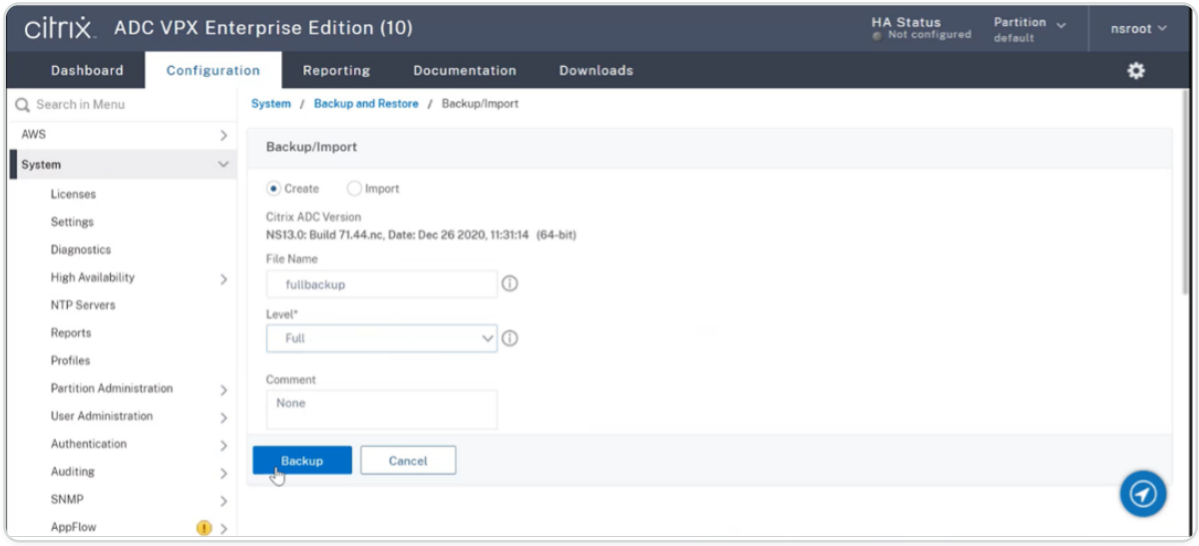
1. 使用 NetScaler VPX - 客户许可 在与旧 EC2 实例相同的可用区中创建 BYOL EC2 实例，该旧实例具有相同的安全组、IAM 角色和子网。新的 EC2 实例必须只有一个 ENI 接口。
2. 要使用 NetScaler GUI 备份旧 EC2 实例上的数据，请按照以下步骤操作。
   a. 导航到 **系统 > 备份和恢复**。
   b. 在 **Welcome** 页面中，单击 **Backup/Import** 以启动该过程。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



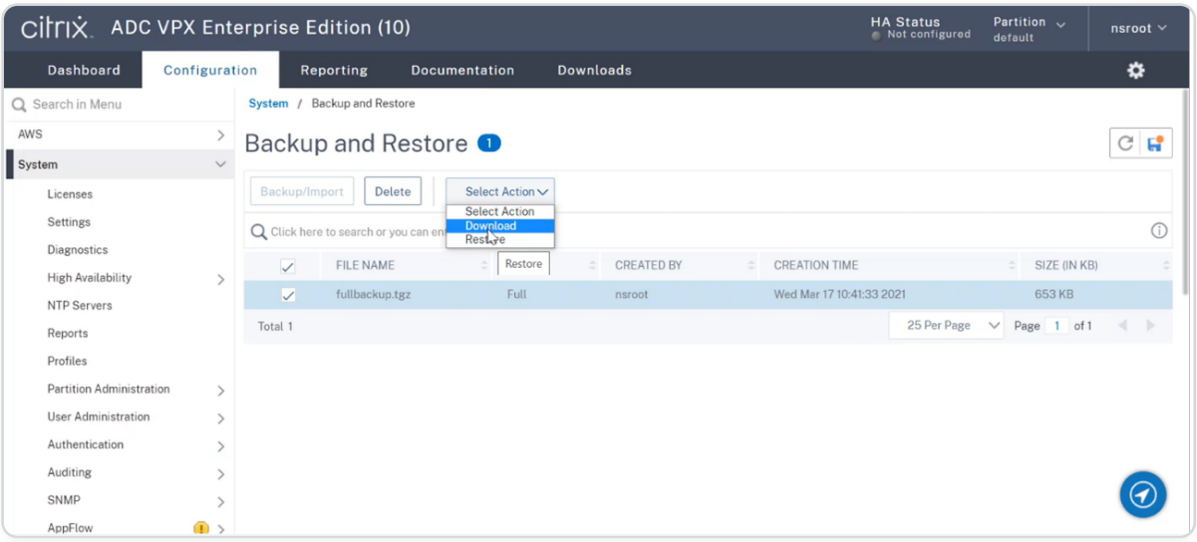
c. 在 **Backup/Import** 页面中，填写以下详细信息：

- **名称** – 备份文件的名称。
- **级别** – 选择备份级别为 **Full**。
- **注释** – 提供备份的简要说明。



d. 单击 **Backup**。备份完成后，您可以选择该文件并将其下载到本地计算机。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

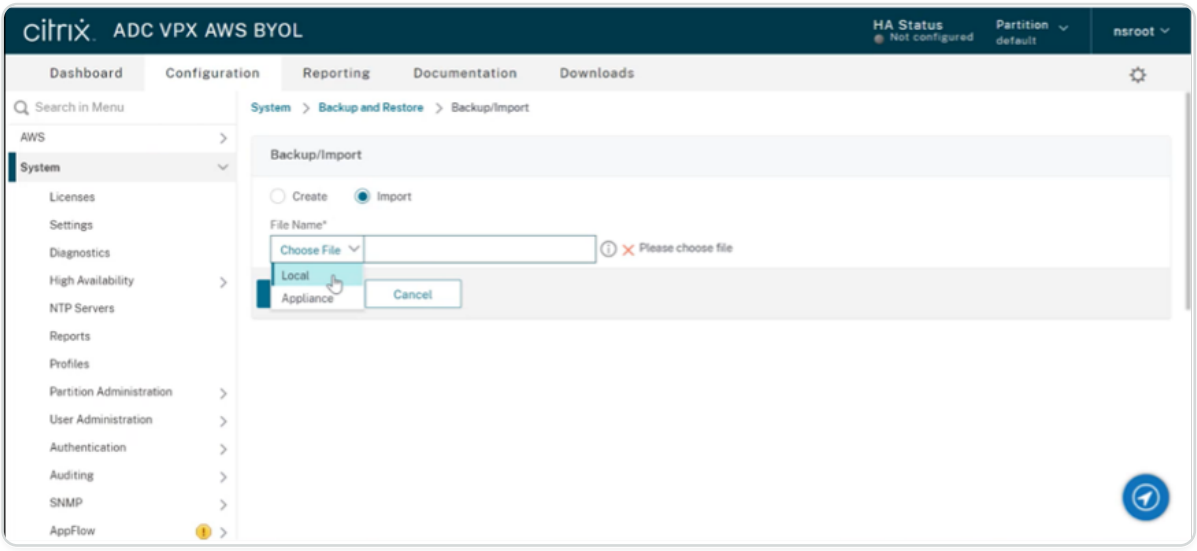


3. 要使用 NetScaler GUI 在新的 EC2 实例上恢复数据，请按照以下步骤操作：

   a. 导航到 **系统 > 备份和恢复**。

   b. 单击 **Backup/Import** 以启动该过程。

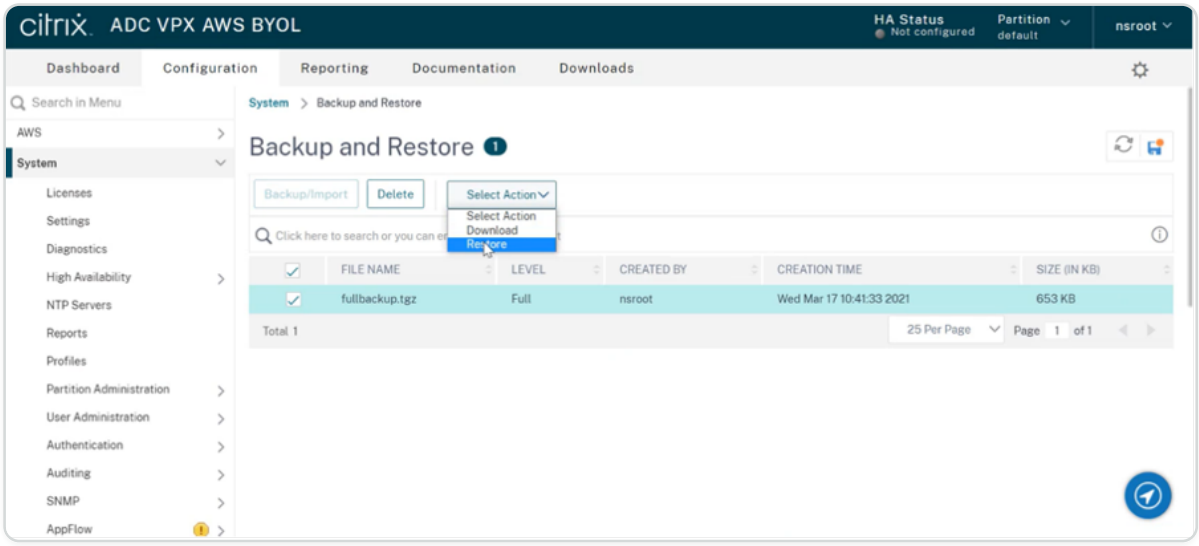
   c. 选择 **Import** 选项并上传备份文件。



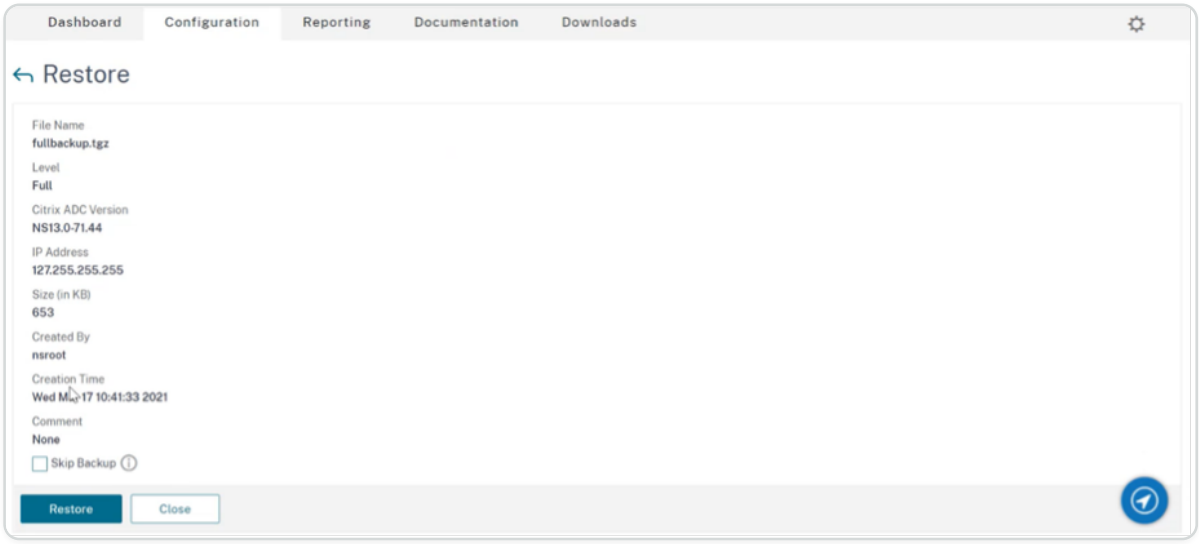
   d. 选择文件。

   e. 从**选择操作**下拉菜单中，选择**恢复**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



f. 在**恢复**页面上，验证文件详细信息，然后单击**恢复**。



g. 恢复后，重新启动 EC2 实例。

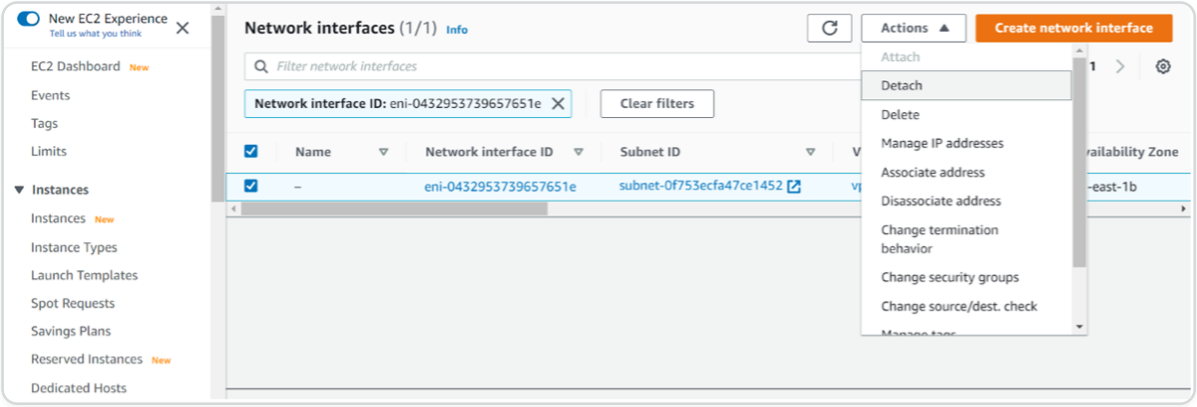
4. 将所有接口（绑定 NSIP 地址的管理接口除外）从旧 EC2 实例移动到新 EC2 实例。要将网络接口从一个 EC2 实例移动到另一个 EC2 实例，请按照以下步骤操作：

   a. 在 **AWS Portal** 中，停止旧 EC2 实例和新 EC2 实例。

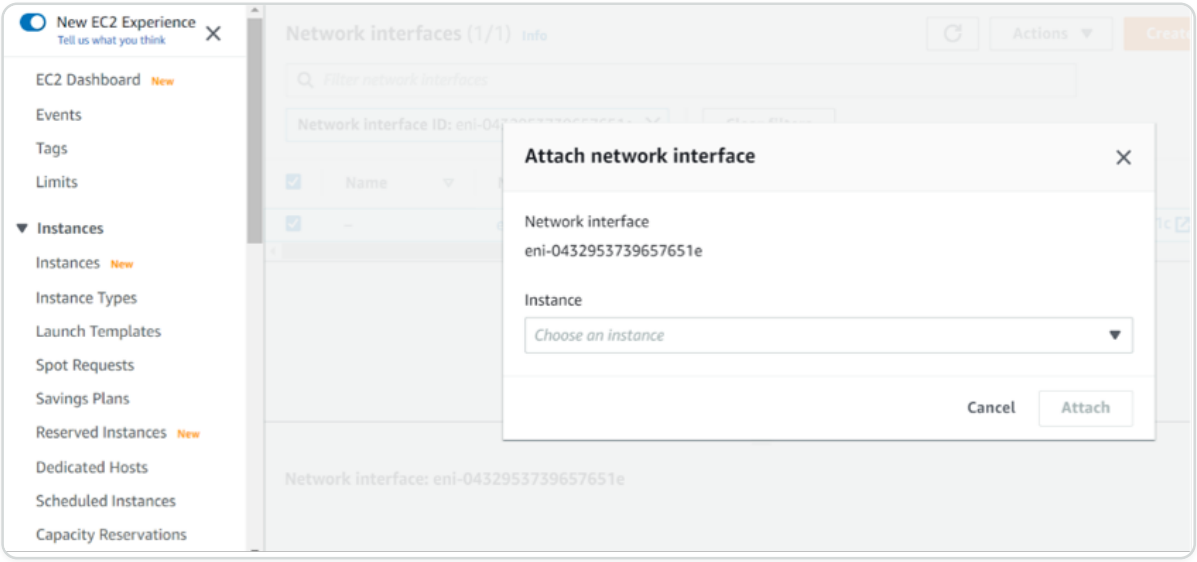
   b. 导航到**网络接口**，并选择连接到旧 EC2 实例的网络接口。

   c. 通过单击**操作 > 分离**来分离 EC2 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



d. 通过单击**操作 > 附加**将网络接口附加到新的 EC2 实例。输入必须附加网络接口的 EC2 实例名称。



e. 对所有其他已附加的接口执行**步骤 1** 到**步骤 4**。请务必遵循顺序并保持接口顺序。也就是说，首先分离接口 2 并附加它，然后分离接口 3 并附加它，依此类推。

5. 无法从旧 EC2 实例分离管理接口。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，请按照以下步骤操作：

   a. 在 **AWS Portal** 中，确保新旧 EC2 实例都处于 **停止** 状态。

   b. 导航到 **网络接口**，然后选择附加到旧 EC2 实例的管理网络接口。

   c. 单击 **操作 > 管理 IP 地址**，并记下所有已分配的辅助 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 IP 地址**。

   g. 输入在 **步骤 3** 中记下的 IP 地址。

   h. 选中 **允许重新分配辅助私有 IP 地址** 复选框。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. 单击 **保存**。

在 AWS 中移动 IP 地址(/en-us/vpx/media/aws-move-ip-address.png)

6. 启动新的 EC2 实例并验证配置。所有配置迁移完成后，您可以根据需要删除或保留旧的 EC2 实例。
7. 如果任何 EIP 地址附加到旧 EC2 实例的 NSIP 地址，请将旧实例的 NSIP 地址移动到新实例的 NSIP 地址。
8. 如果要恢复到旧实例，请在新旧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，请按照以下步骤操作：
   - 使用 Citrix 网站中的许可门户生成有效许可证。
   - 将许可证上传到实例。

注意：

当您将 BYOL 实例迁移到订阅实例（付费市场实例）时，无需安装许可证。正确的特性集和性能将自动激活。

限制

管理接口无法移动到新的 EC2 实例。因此，Citrix 建议您手动配置管理接口。有关更多信息，请参阅前面过程中的**步骤 5**。将创建一个新的 EC2 实例，它是旧 EC2 实例的精确副本，但只有 NSIP 地址具有新的 IP 地址。

在不同可用区中对服务器进行负载均衡

VPX 实例可用于对在同一可用区中运行的服务器进行负载均衡，或在：

- 同一 AWS VPC 中的不同可用区 (AZ)
- 不同的 AWS 区域
- VPC 中的 AWS EC2

为了使 VPX 实例能够对在 VPX 实例所在的 AWS VPC 外部运行的服务器进行负载均衡， 请将实例配置为使用 EIP 通过 Internet 网关路由流量，具体如下：

1. 通过使用 NetScaler CLI 或 GUI，在 NetScaler VPX 实例上配置 SNIP。
2. 通过为服务器端流量创建面向公众的子网，启用流量路由出 AZ。
3. 使用 AWS GUI 控制台，将 Internet 网关路由添加到路由表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 将您更新的路由表与服务器端子网关联。
5. 将 EIP 与映射到 NetScaler SNIP 地址的服务器端私有 IP 地址关联。

AWS 上高可用性如何工作

您可以在 AWS 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，另一个配置为辅助节点时，主节点接受连接并管理服务器。辅助节点监控主节点。如果由于任何原因主节点无法接受连接，则辅助节点将接管。

在 AWS 中，VPX 实例支持以下部署类型：

- 同一区域内的高可用性
- 跨不同区域的高可用性

注意：

为了使高可用性正常工作，请确保两个 NetScaler VPX 实例都附加了 IAM 角色，并将弹性 IP (EIP) 地址分配给 NSIP。如果 NSIP 可以通过 NAT 实例访问互联网，则无需在 NSIP 上分配 EIP。

同一区域内的高可用性

在同一区域内的高可用性部署中，两个 VPX 实例必须具有相似的网络配置。

请遵循以下两条规则：

规则 1. 一个 VPX 实例上的任何 NIC 必须与另一个 VPX 中对应的 NIC 位于同一子网中。两个实例都必须具有：

- 同一子网上的管理接口（称为管理子网）
- 同一子网上的客户端接口（称为客户端子网）
- 同一子网上的服务器接口（称为服务器子网）

规则 2. 两个实例上的管理 NIC、客户端 NIC 和服务器 NIC 的顺序必须相同。 例如，不支持以下场景。

VPX 实例 1

NIC 0: 管理 NIC 1: 客户端 NIC 2: 服务器

VPX 实例 2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NIC 0: 管理

NIC 1: 服务器

NIC 2: 客户端

在此场景中，实例 1 的 NIC 1 位于客户端子网中，而实例 2 的 NIC 1 位于服务器子网中。为了使 HA 正常工作，两个实例的 NIC 1 必须位于客户端子网或服务器子网中。

从 13.0 41.xx 开始，可以通过在故障转移后将附加到主 HA 节点的 NIC（客户端和服务器端 NIC）的辅助私有 IP 地址迁移到辅助 HA 节点来实现高可用性。在此部署中：

- 两个 VPX 实例具有相同数量的 NIC，并根据 NIC 枚举进行子网映射。
- 每个 VPX NIC 都有一个额外的私有 IP 地址，除了第一个 NIC（它对应于管理 IP 地址）。这个额外的私有 IP 地址在 AWS Web 控制台中显示为主私有 IP 地址。在我们的文档中，我们将此额外 IP 地址称为虚拟 IP 地址)。
- 虚拟 IP 地址不得在 NetScaler 实例上配置为 VIP 和 SNIP。
- 必须根据需要创建其他辅助私有 IP 地址，并将其配置为 VIP 和 SNIP。
- 在故障转移时，新的主节点会查找已配置的 SNIP 和 VIP，并将其从附加到先前主节点的 NIC 移动到新主节点上对应的 NIC。
- NetScaler 实例需要 IAM 权限才能使 HA 正常工作。将以下 IAM 权限添加到添加到每个实例的 IAM 策略中。

`"iam:GetRole"` `"ec2:DescribeInstances"` `"ec2:DescribeNetworkInterfaces"` `"ec2:AssignPrivateIpAddresses"`

注意：

`unassignPrivateIpAddress` 不是必需的。

此方法比传统方法更快。在旧方法中，HA 依赖于主节点的 AWS 弹性网络接口迁移到辅助节点。

对于传统方法，需要以下策略：

`"iam:GetRole"` `"ec2:DescribeInstances"` `"ec2:DescribeAddresses"` `"ec2:AssociateAddress"` `"ec2:DisassociateAddress"`

有关更多信息，请参阅在 AWS 上部署高可用性对。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

跨不同区域的高可用性

您可以在两个不同的子网或两个不同的 AWS 可用区中配置两个 NetScaler VPX 实例，作为独立网络配置 (INC) 模式下的高可用性主动-被动对。发生故障转移时，主实例 VIP 的 EIP（弹性 IP）会迁移到辅助实例，辅助实例将接管成为新的主实例。在故障转移过程中，AWS API 会执行以下操作：

- 检查附加了 `IPSets` 的虚拟服务器。
- 从虚拟服务器正在侦听的两个 IP 地址中，查找具有关联公共 IP 的 IP 地址。其中一个直接附加到虚拟服务器，另一个通过 IP 集附加。
- 将公共 IP (EIP) 重新关联到属于新主 VIP 的私有 IP。

对于跨不同区域的 HA，需要以下策略：

`"iam:GetRole"` `"ec2:DescribeInstances"` `"ec2:DescribeAddresses"` `"ec2:AssociateAddress"` `"ec2:DisassociateAddress"`

有关更多信息，请参阅跨 AWS 可用区的高可用性。

开始部署之前

在 AWS 上开始任何 HA 部署之前，请阅读以下文档：

- 先决条件
- 限制和使用准则
- 在 AWS 上部署 NetScaler VPX 实例
- 高可用性

故障排除

要排查 AWS 云中 NetScaler VPX 实例 HA 故障转移期间的任何故障，请检查存储在 `/var/log/` 位置的 `cloud-ha-daemon.log` 文件。

在同一 AWS 可用区中部署 VPX HA 对

注意：

从 NetScaler 13.1 版本 27.x 开始，同一 AWS 可用区中的 VPX HA 对支持 IPv6 地址。

您可以在 AWS 上将两个 NetScaler VPX 实例配置为 HA 对，在同一 AWS 区域中，两个 VPX 实例位于同一子网。HA 是通过在故障转移后将附加到主 HA 节点的 NIC（客户端和服务器端 NIC）的辅

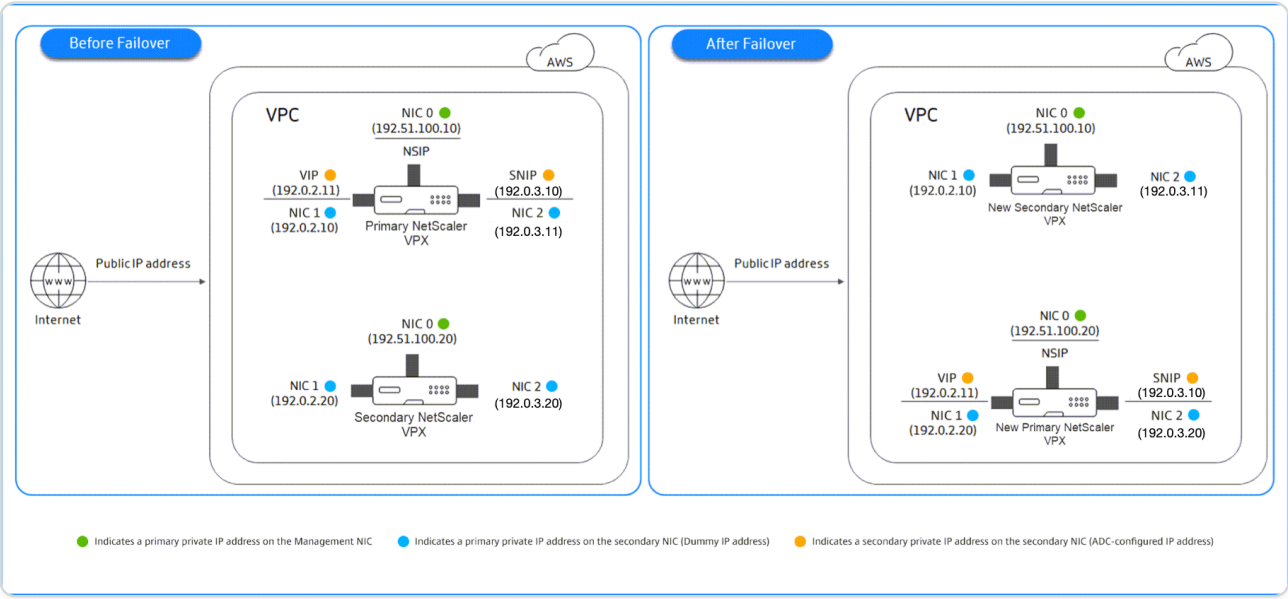
© 1997–2026 Citrix Systems, Inc. All rights reserved.

助私有 IP 地址迁移到辅助 HA 节点来实现的。与辅助私有 IP 地址关联的所有弹性 IP 地址也会被迁移。

NetScaler VPX HA 对在同一 AWS 可用区中同时支持 IPv4 和 IPv6 地址。

下图描述了通过迁移辅助私有 IP 地址实现的 HA 故障转移场景。

图 1. AWS 上的 NetScaler VPX HA 对，使用私有 IP 迁移



在开始阅读本文档之前，请阅读以下文档：

- 先决条件
- 限制和使用指南
- 在 AWS 上部署 NetScaler VPX 实例
- 高可用性

如何在同一区域中部署 VPX HA 对

以下是在同一区域中部署 VPX HA 对的步骤摘要：

1. 在 AWS 上创建两个 VPX 实例，每个实例有三个 NIC
2. 将 AWS 辅助私有 IP 地址分配给主节点的 VIP 和 SNIP
3. 使用 AWS 辅助私有 IP 地址在主节点上配置 VIP 和 SNIP
4. 在两个节点上配置 HA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

步骤 1. 使用相同的 VPC 创建两个 VPX 实例（主节点和辅助节点），每个实例有三个 NIC（以太网 0、以太网 1、以太网 2）

按照 (/zh-cn/vpx/13-1/deploy-aws/launch-vpx-for-aws-ami.html#deploy-a-citrix-adc-vpx-instance-on-aws-by-using-the-aws-web-console) 中“使用 AWS Web 控制台在 AWS 上部署 NetScaler VPX 实例”中给出的步骤操作。

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）分配私有 IP 地址

AWS 控制台会自动将主私有 IP 地址分配给已配置的 NIC。为 VIP 和 SNIP 分配更多私有 IP 地址，这些地址称为辅助私有 IP 地址。

要将私有 IP 地址分配给网络接口，请按照以下步骤操作：

1. 在 `<https://console.aws.amazon.com/ec2/>` 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 **网络接口**，然后选择附加到实例的网络接口。
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. 输入一个在实例子网范围内的特定 IPv4 地址，或者将此字段留空，让 Amazon 为您选择一个 IP 地址。
   c. （可选）选择 **允许重新分配**，以允许在辅助私有 IP 地址已分配给另一个网络接口时重新分配它。
6. 对于 IPv6 地址：
   a. 选择 **分配新 IP**。
   b. 输入一个在实例子网范围内的特定 IPv6 地址，或者将此字段留空，让 Amazon 为您选择一个 IP 地址。
   c. （可选）选择 **允许重新分配**，以允许在主或辅助私有 IP 地址已分配给另一个网络接口时重新分配它。
7. 选择 **是 > 更新**。

在 **实例描述** 下，会显示已分配的私有 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

在 IPv4 HA 对部署中，您只能在接口上分配辅助 IPv4 地址，并将其用作 VIP 和 SNIP 地址。但在 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. 在主节点上配置 VIP 和 SNIP，使用辅助私有 IP 地址

使用 SSH 访问主节点。打开 SSH 客户端并输入：

```
ssh -i <location of your private key> nsroot@<public DNS of the instance>
```

接下来，配置 VIP 和 SNIP。

对于 VIP，输入：

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

对于 SNIP，输入：

```
add ns ip <IPAddress> <netmask> -type SNIP
```

键入 `save config` 以保存。

要查看已配置的 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 HA

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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 HA 节点，请键入 `show ha node`。

发生故障转移时，在先前的主节点上配置为 VIP 和 SNIP 的辅助私有 IP 地址将迁移到新的主节点。

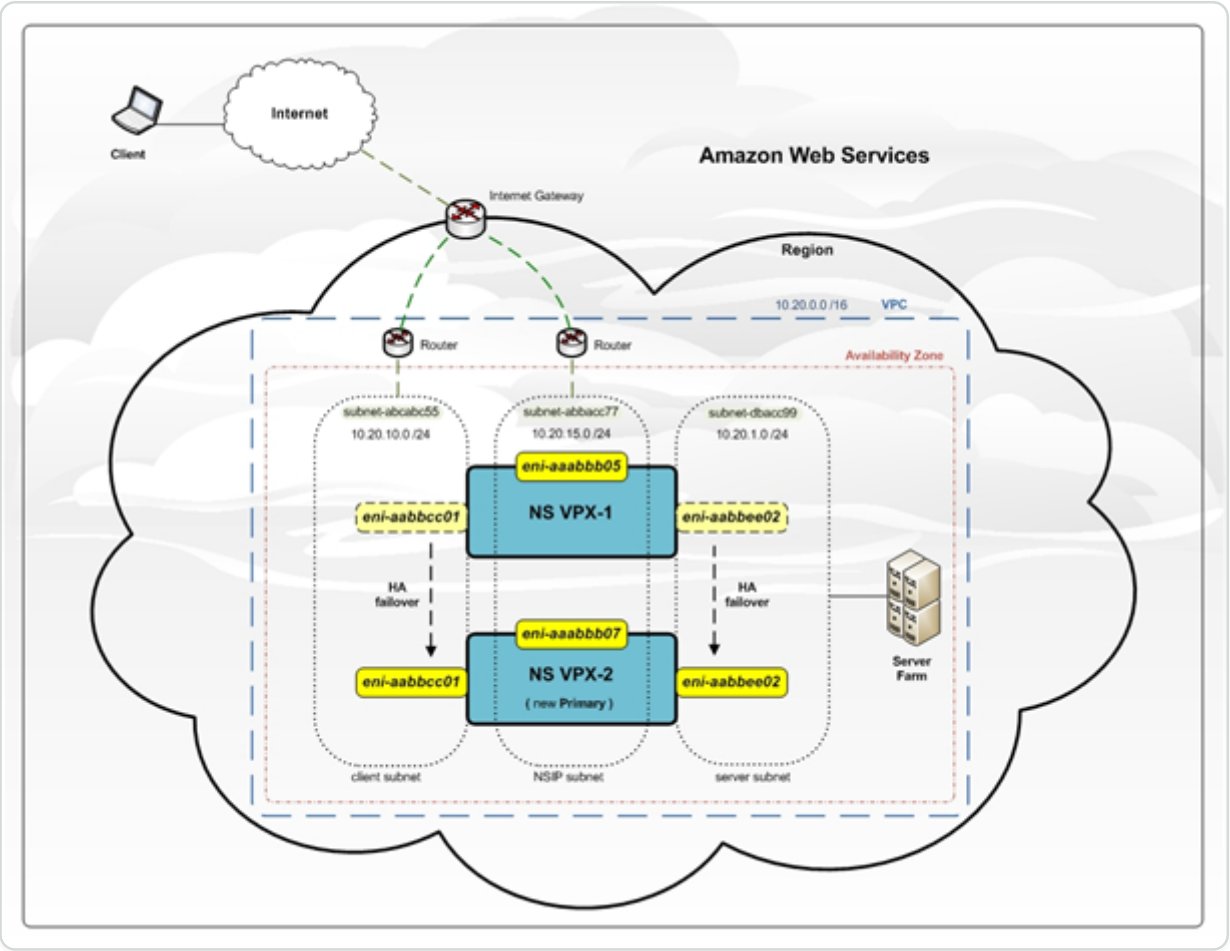
要强制节点进行故障转移，请键入 `force HA` failover。

部署 VPX HA 对的旧方法

在 13.0 41.x 版本之前，同一区域内的 HA 是通过 AWS 弹性网络接口 (ENI) 迁移实现的。但是，此方法正在逐渐弃用。

下图显示了 AWS 上 NetScaler VPX 实例的 HA 部署架构示例。

图 1. AWS 上的 NetScaler VPX HA 对，使用 ENI 迁移



© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以使用以下选项之一，在 AWS 上将两个 VPX 实例部署为 HA 对：

- 使用 AWS 管理控制台手动创建具有 IAM 角色的实例，然后在其上配置 HA。
- 或者使用 Citrix CloudFormation 模板自动执行高可用性部署。

CloudFormation 模板显著减少了创建 HA 对所需的步骤，并且它会自动创建一个 IAM 角色。本节介绍如何使用 Citrix CloudFormation 模板部署 NetScaler VPX HA（主动-被动）对。

在将两个 NetScaler VPX 实例部署为 HA 对时，请记住以下几点。

注意事项

- AWS 上的 HA 要求主节点至少有两个 ENI（一个用于管理，另一个用于数据流量），辅助节点有一个管理 ENI。但是，出于安全考虑，请在主节点上创建三个 ENI，因为此设置允许您隔离私有网络和公共网络（推荐）。
- 辅助节点始终有一个 ENI 接口（用于管理），主节点最多可以有四个 ENI。
- 高可用性对中每个 VPX 实例的 NSIP 地址必须配置在实例的默认 ENI 上。
- Amazon 不允许 AWS 中有任何广播/多播数据包。因此，在 HA 设置中，当主 VPX 实例发生故障时，数据平面 ENI 会从主 VPX 实例迁移到辅助 VPX 实例。
- 由于默认（管理）ENI 无法移动到另一个 VPX 实例，因此请勿将默认 ENI 用于客户端和服务器流量（数据平面流量）。
- /var/log/ns.log 中的消息 AWSCONFIG IOCTL NSAPI_HOTPLUG_INTF success output 0 表示两个数据 ENI 已成功附加到辅助实例（新的主实例）。
- 由于 AWS 分离/附加 ENI 机制，故障转移可能需要长达 20 秒。
- 发生故障转移时，故障实例始终会重新启动。
- 心跳数据包仅在管理接口上接收。
- 主 VPX 实例和辅助 VPX 实例的配置文件会同步，包括 `nsroot` 密码。HA 配置同步后，辅助节点的 `nsroot` 密码将设置为与主节点相同。
- 要访问 AWS API 服务器，VPX 实例必须分配有公共 IP 地址，或者必须在 VPC 子网级别正确设置路由以指向 VPC 的互联网网关。
- 命名服务器/DNS 服务器在 VPC 级别使用 DHCP 选项进行配置。
- Citrix CloudFormation 模板不会在不同可用区之间创建 HA 设置。
- Citrix CloudFormation 模板不会创建 INC 模式。
- AWS 调试消息可在 VPX 实例上的日志文件 /var/log/ns.log 中找到。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 Citrix CloudFormation 模板部署高可用性对

在启动 CloudFormation 模板之前，请确保完成以下要求：

- 一个 VPC
- VPC 中的三个子网
- 一个安全组，其中打开了 UDP 3003、TCP 3009–3010、HTTP、SSH 端口
- 一个密钥对
- 创建一个互联网网关
- 编辑客户端和管理网络的路由表，使其指向互联网网关

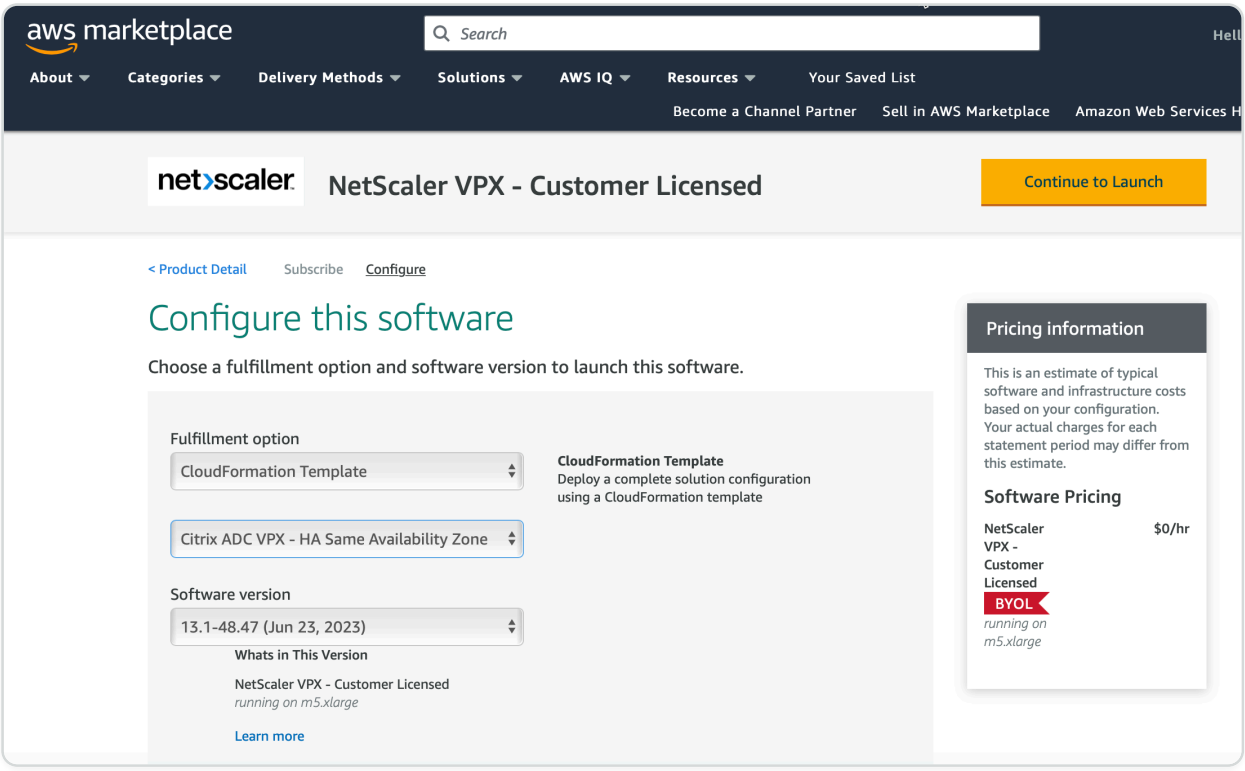
注意

Citrix CloudFormation 模板会自动创建一个 IAM 角色。现有 IAM 角色不会出现在模板中。

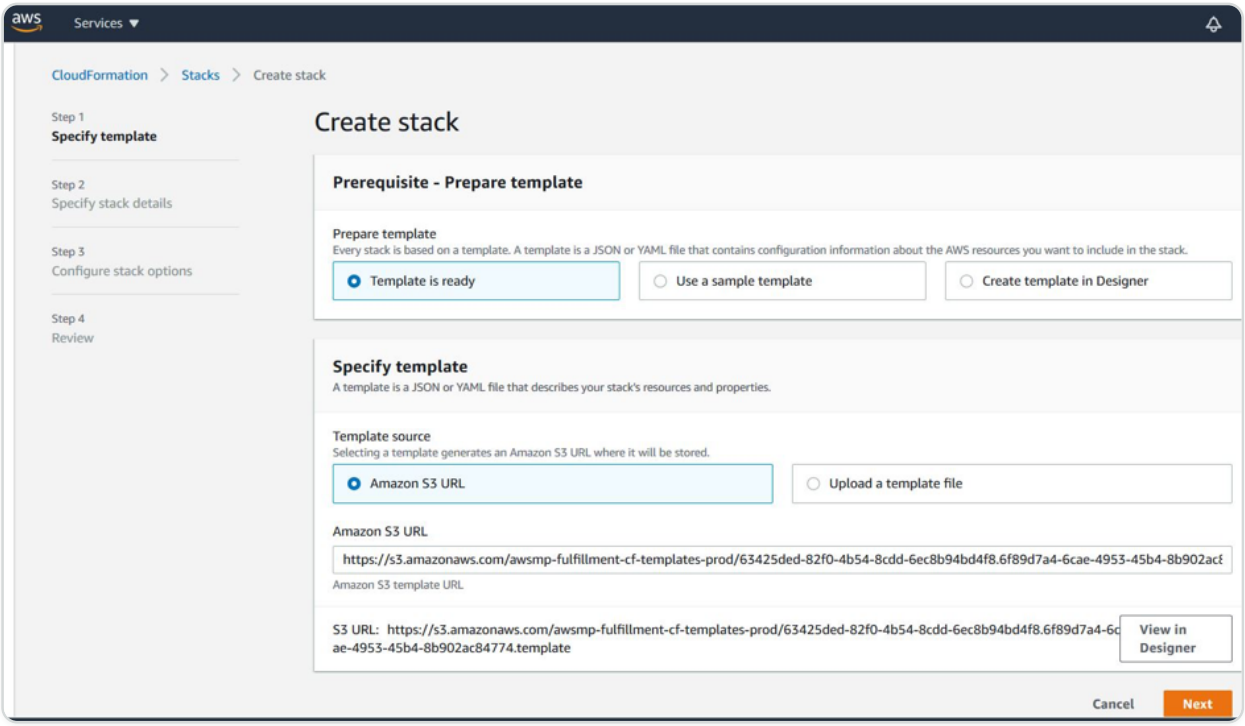
启动 Citrix CloudFormation 模板：

1. 使用您的 AWS 凭据登录到 AWS Marketplace。
2. 在搜索字段中，键入 **NetScaler VPX** 以搜索 NetScaler AMI，然后单击 **Go**。
3. 在搜索结果页面上，单击所需的 NetScaler VPX 产品。
4. 单击“**定价**”选项卡，转到“**定价信息**”。
5. 选择区域和“**履行选项**”为“**NetScaler VPX – 客户许可**”。
6. 单击“**继续订阅**”。
7. 检查“**订阅**”页面中的详细信息，然后单击“**继续配置**”。
8. 选择“**交付方法**”为“**CloudFormation 模板**”。
9. 选择所需的 CloudFormation 模板。
10. 选择“**软件版本**”和“**区域**”，然后单击“**继续启动**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



11. 在“**选择操作**”下，选择“**启动 CloudFormation**”，然后单击“**启动**”。 出现“**创建堆栈**”页面。
12. 单击“**下一步**”。



13. 出现“**指定堆栈详细信息**”页面。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“**网络配置**”下，执行以下操作：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - 选择“**管理子网**”、“**客户端子网**”和“**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“**主管理 IP**”、“**辅助管理 IP**”、“**客户端 IP**”和“**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。
  - 为“**VPCTenancy**”选择“**default**”。

- 在“**NetScaler 配置**”下，执行以下操作：
  - 为“**实例类型**”选择“**m5.xlarge**”。
  - 从“**密钥对**”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“**否**”。

    有关 CloudWatch 指标的更多信息，请参阅 (#monitor-your-instances-using-amazon-cloudWatch)。

- 在“**可选配置**”下，执行以下操作：
  - 默认情况下，**是否应将公有 IP (EIP) 分配给管理接口？** 选项设置为 **否**。
  - 默认情况下，**是否应将公有 IP (EIP) 分配给客户端接口？** 选项设置为 **否**。

指定堆栈详细信息(/en-us/vpx/media/cloudformation-specify-stack-details.png)

14. 单击 **下一步**。
15. 出现 **配置堆栈选项** 页面。这是一个可选页面。

    配置堆栈选项(/en-us/vpx/media/configure-stack-options.png)

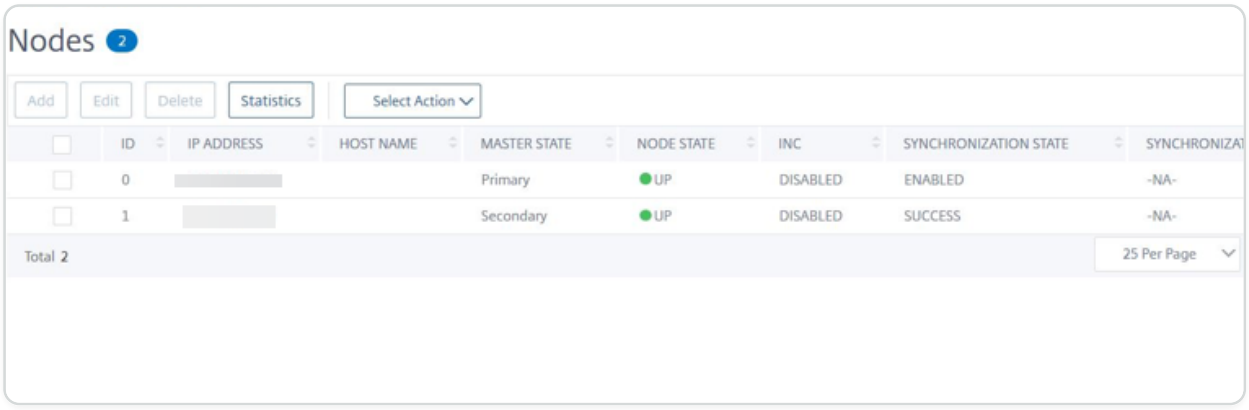
16. 单击 **下一步**。
17. 出现 **选项** 页面。（这是一个可选页面。）单击 **下一步**。
18. 出现 **审核** 页面。请花点时间查看设置，并在必要时进行任何更改。
19. 选中 **我确认 AWS CloudFormation 可能会创建 IAM 资源。** 复选框，然后单击 **创建堆栈**。
20. 出现 **CREATE-IN-PROGRESS** 状态。请等待状态变为 **CREATE-COMPLETE**。如果状态未变为 **COMPLETE**，请检查 **事件** 选项卡以了解失败原因，并使用正确的配置重新创建实例。

    CloudFormation 堆栈完成(/en-us/vpx/media/cloudformation-stack-complete.png)

21. 创建 IAM 资源后，导航到 **EC2 管理控制台 > 实例**。您会发现创建了两个具有 IAM 角色的 VPX 实例。主节点和辅助节点均创建了三个私有 IP 地址和三个网络接口。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

22. 使用用户名 `nsroot` 和实例 ID 作为密码登录主节点。从 GUI 导航到 **系统 > 高可用性 > 节点**。NetScaler VPX 已通过 CloudFormation 模板配置为 HA 对。
23. NetScaler VPX HA 对出现。



使用 Amazon CloudWatch 监控您的实例

您可以使用 Amazon CloudWatch 服务来监控一组 NetScaler VPX 指标，例如 CPU 和内存利用率以及吞吐量。CloudWatch 实时监控在 AWS 上运行的资源和应用程序。您可以通过 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

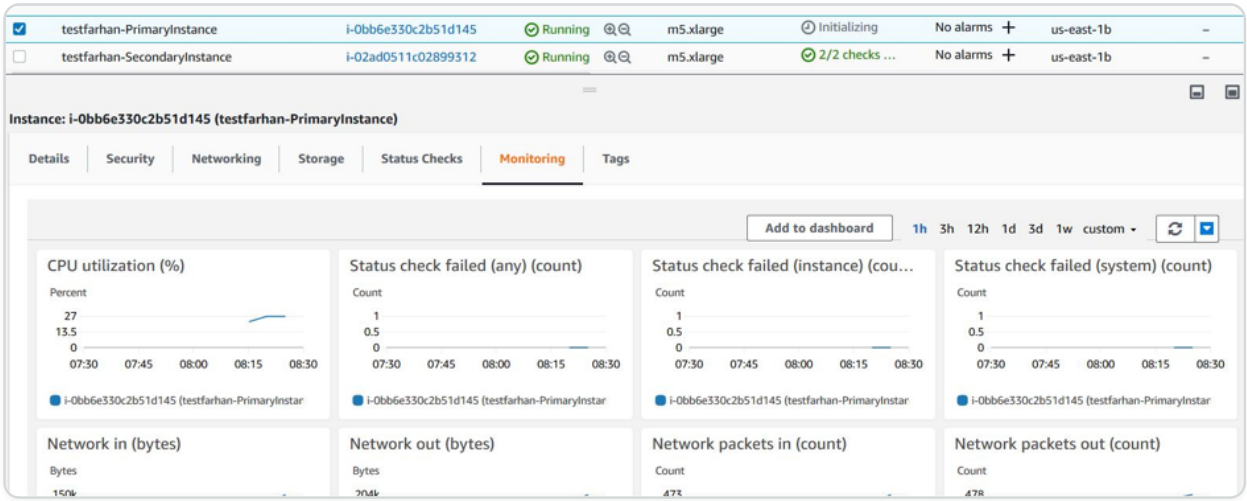
- 如果您使用 AWS Web 控制台在 AWS 上部署 NetScaler VPX 实例，则 CloudWatch 服务默认启用。
- 如果您使用 Citrix CloudFormation 模板部署 NetScaler VPX 实例，则默认选项为“是”。如果您想禁用 CloudWatch 服务，请选择“否”。
- 指标适用于 CPU（管理和数据包 CPU 使用率）、内存和吞吐量（入站和出站）。

如何查看 CloudWatch 指标

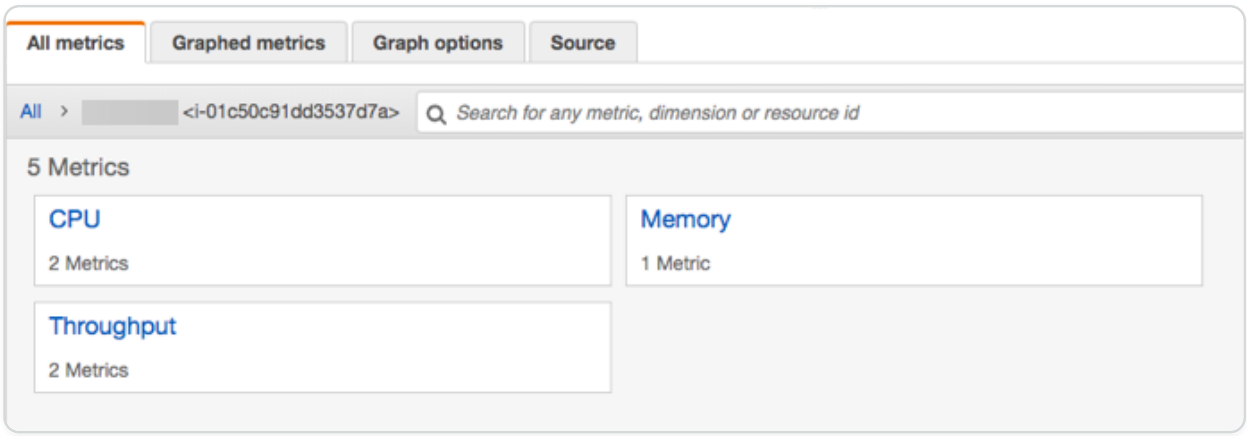
要查看实例的 CloudWatch 指标，请按照以下步骤操作：

1. 登录到 **AWS 管理控制台 > EC2 > 实例**。
2. 选择实例。
3. 单击 **监控**。
4. 单击 **查看所有 CloudWatch 指标**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

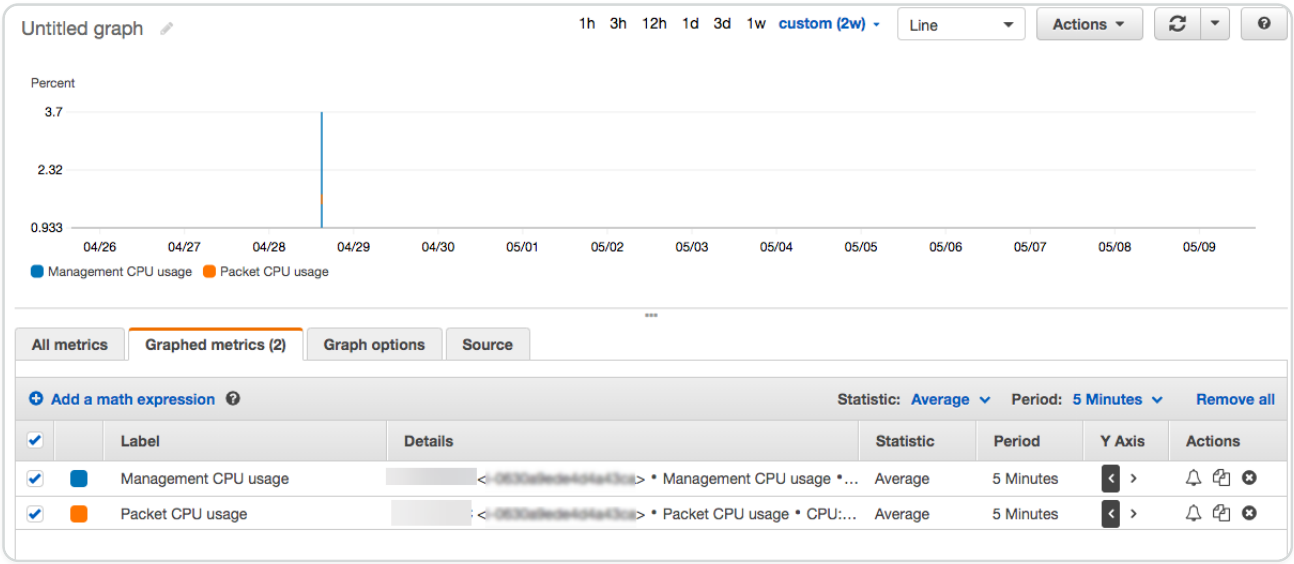


5. 在“所有指标”下，单击您的实例 ID。



6. 单击您要查看的指标，设置持续时间（按分钟、小时、天、周、月）。
7. 单击**图形化指标**以查看使用情况统计信息。使用**图表选项**自定义图表。

图。CPU 使用率的图形化指标



© 1997–2026 Citrix Systems, Inc. All rights reserved.

在高可用性设置中配置 SR-IOV

对高可用性设置中 SR-IOV 接口的支持从 NetScaler 12.0 57.19 版本开始提供。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 上的高可用性如何工作

跨不同 AWS 可用区的高可用性

您可以将两个 NetScaler VPX 实例配置在两个不同的子网或两个不同的 AWS 可用区中，作为独立网络配置 (INC) 模式下的高可用性主动-被动对。如果由于任何原因，主节点无法接受连接，则辅助节点将接管。

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
  - 先决条件
  - 限制和使用指南
- VPX 高可用性对可以位于同一可用区中的不同子网中，也可以位于两个不同的 AWS 可用区中。
- Citrix® 建议您为管理 (NSIP)、客户端流量 (VIP) 和后端服务器 (SNIP) 使用不同的子网。
- 高可用性必须设置为独立网络配置 (INC) 模式，才能使故障转移正常工作。
- 这两个实例必须打开端口 3003 以进行 UDP 流量，因为该端口用于心跳。
- 两个节点的管理子网必须能够访问互联网或通过内部 NAT 访问 AWS API 服务器，以便 REST API 正常运行。
- IAM 角色必须具有 E2 权限用于公共 IP 或弹性 IP (EIP) 迁移，以及 EC2 路由表权限用于私有 IP 迁移。

您可以通过以下方式部署跨 AWS 可用区的高可用性：

- 使用弹性 IP 地址
- 使用私有 IP 地址

© 1997–2026 Citrix Systems, Inc. All rights reserved.

其他参考

有关适用于 AWS 的 NetScaler Application Delivery Management (ADM) 的更多信息，请参阅在 AWS 上安装 NetScaler ADM 代理。

在不同 AWS 区域部署具有弹性 IP 地址的 VPX 高可用性对

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 可用区中配置两个 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。

具有跨不同 AWS 区域的 EIP 地址的 HA 如何工作

发生故障转移时，主实例 VIP 的 EIP 将迁移到辅助实例，辅助实例将接管成为新的主实例。在故障转移过程中，AWS API 将执行以下操作：

1. 检查已附加 `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，查找具有关联公共 IP 的 IP 地址。其中一个直接附加到虚拟服务器，另一个通过 IP 集附加。
3. 将公共 IP (EIP) 重新关联到属于新主 VIP 的私有 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，您可以在 AWS 中创建安全组以限制 IP 访问。对于高可用性，您可以根据部署情况从 EIP 切换到私有 IP 移动解决方案。

如何在不同 AWS 区域部署具有弹性 IP 地址的 VPX 高可用性对

以下是在两个不同子网或两个不同 AWS 可用区中部署 VPX 对的步骤摘要。

1. 创建 Amazon 虚拟私有云。
2. 在两个不同的可用区或同一可用区但不同子网中部署两个 VPX 实例。
3. 配置高可用性
   a. 在两个实例中以 INC 模式设置高可用性。
   b. 在两个实例中添加一个 (/zh-cn/citrix-adc/13-1/load-balancing/load-balancing-customizing/multi-ip-virtual-servers.html)。
   c. 将两个实例中的 IP 集绑定到 VIP。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. 在主实例中添加一个虚拟服务器。

对于步骤 1 和 2，请使用 AWS 控制台。对于步骤 3，请使用 NetScaler VPX GUI 或 CLI。

步骤 1. 创建一个 Amazon 虚拟私有云 (VPC)。

步骤 2. 在两个不同的可用区或在同一可用区但不同子网中部署两个 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. 在两个实例中以 INC 模式设置高可用性。

   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>` 指的是辅助节点的管理 NIC 的私有 IP 地址

   `<prim_ip>` 指的是主节点的管理 NIC 的私有 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. 在两个实例上将 IP 集绑定到 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>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

您可以将 IP 集绑定到主 VIP 或辅助 VIP。但是，如果您将 IP 集绑定到主 VIP，则使用辅助 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：

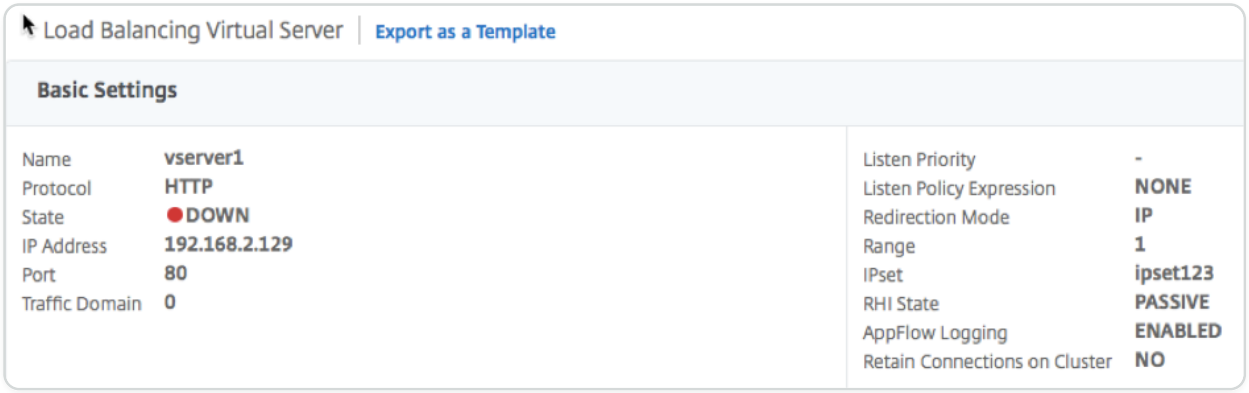
   ```
   add <server_type> vserver <vserver_name> <protocol> <primary_vip> <port> -ipset \<ipset_name>
   ```

使用 GUI 配置高可用性

1. 在两个实例上以 INC 模式设置高可用性
2. 使用用户名 `nsroot` 和实例 ID 作为密码登录主节点。
3. 从 GUI 中，导航到 **配置** > **系统** > **高可用性**。点击 **添加**。
4. 在 **远程节点 IP 地址** 字段中，添加辅助节点的管理网卡的私有 IP 地址。
5. 在自节点上选择 **启用 NIC（独立网络配置）** 模式。
6. 在 **远程系统登录凭据** 下，添加辅助节点的用户名和密码，然后点击 **创建**。
7. 在辅助节点中重复这些步骤。
8. 在两个实例上添加 IP 集并将 IP 集绑定到 VIP 集。
9. 从 GUI 中，导航到 **系统** > **网络** > **IP 地址** > **添加**。
10. 添加 IP 地址、子网掩码、IP 类型（虚拟 IP）所需的值，然后点击 **创建**。
11. 导航到 **系统** > **网络** > **IP 集** > **添加**。添加 IP 集名称并点击 **插入**。
12. 在 IPV4 页面中，选择虚拟 IP 并点击 **插入**。点击 **创建** 以创建 IP 集。
13. 在主实例中添加虚拟服务器

    从 GUI 中，导航到 **配置** > **流量管理** > **虚拟服务器** > **添加**。

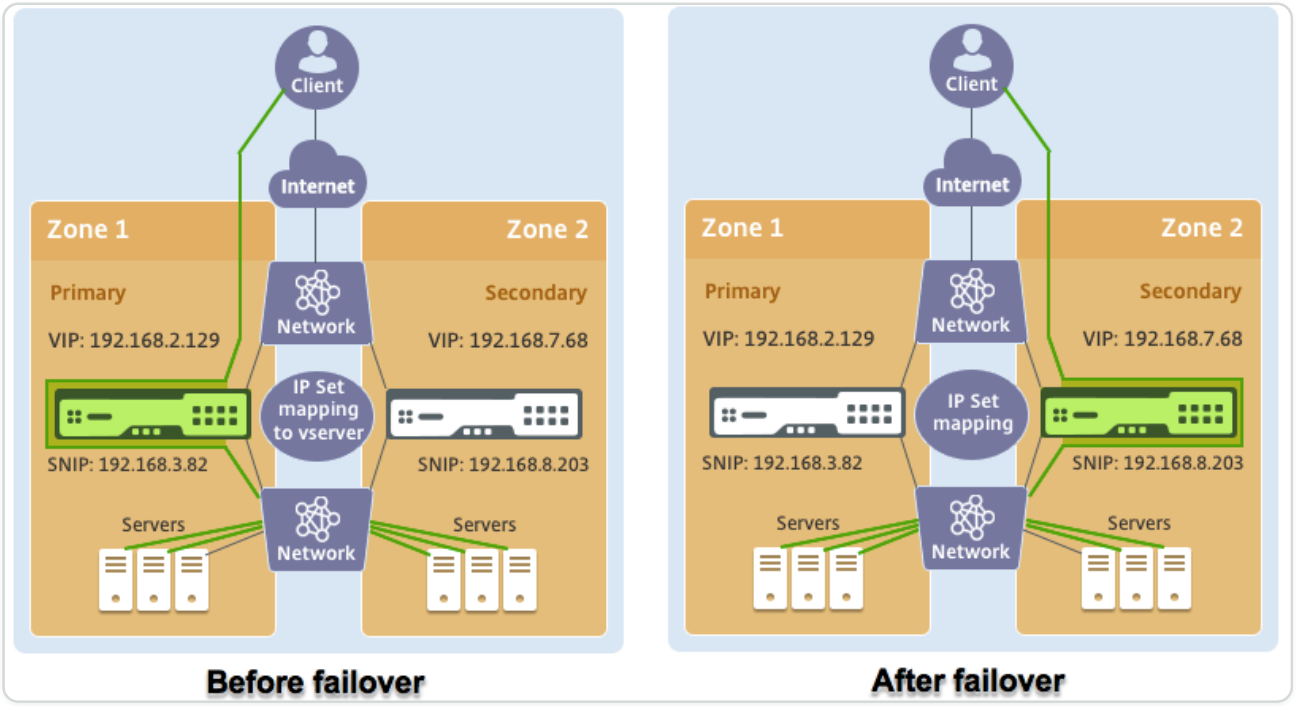
© 1997–2026 Citrix Systems, Inc. All rights reserved.



场景

在此场景中，将创建一个 VPC。在该 VPC 中，将在两个可用区中创建两个 VPX 实例。每个实例有三个子网 - 一个用于管理，一个用于客户端，一个用于后端服务器。一个 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



对于此场景，请使用 CLI 配置高可用性。

1. 在两个实例上以 INC 模式设置高可用性。

   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 指的是辅助节点管理 NIC 的私有 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在辅助节点上：

```
add ha node 1 192.168.1.108 -inc enabled
```

此处，192.168.1.108 指的是主节点管理 NIC 的私有 IP 地址。

2. 添加一个 IP 集并将该 IP 集绑定到两个实例上的 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
   ```

   在辅助设备上：

   ```
   add ipset ipset123
   ```

   ```
   add ns ip 192.168.7.68 255.255.255.0 -type VIP
   ```

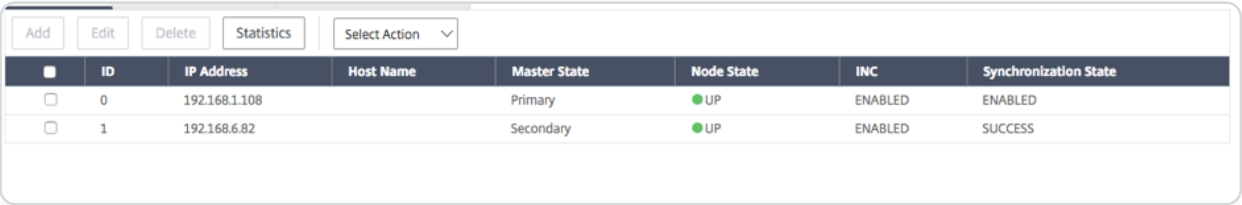
   ```
   bind ipset ipset123 192.168.7.68
   ```

3. 在主实例上添加一个虚拟服务器。

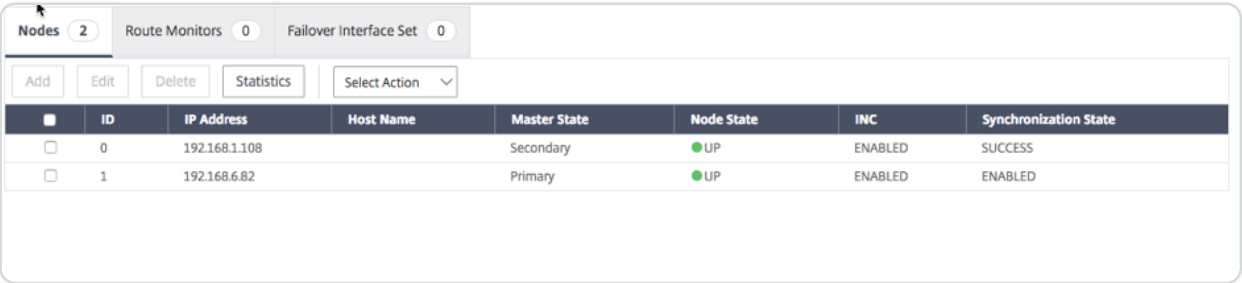
   以下命令：

   ```
   add lbvserver vserver1 http 192.168.2.129 80 -ipset ipset123
   ```

4. 保存配置。



5. 强制故障转移后，辅助设备成为新的主设备。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

在不同 AWS 区域部署具有私有 IP 地址的 VPX 高可用性对

您可以在 INC 模式下，使用私有 IP 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。此解决方案可以轻松地与现有的多区域 具有弹性 IP 地址的 VPX 高可用性对集成。因此，您可以同时使用这两种解决方案。

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：

此部署从 NetScaler 13.0 版本 build 67.39 及更高版本开始支持。此部署与 AWS Transit Gateway 兼容。

使用 AWS 非共享 VPC 的具有私有 IP 地址的高可用性对

先决条件

确保与您的 AWS 账户关联的 IAM 角色具有以下 IAM 权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DeleteRoute",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "ec2:CreateRoute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "iam:SimulatePrincipalPolicy",
                "iam:GetRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

使用 AWS 非共享 VPC 部署具有私有 IP 地址的 VPX HA 对

以下是使用私有 IP 地址在两个不同子网或两个不同 AWS 可用区上部署 VPX 对的步骤摘要。

1. 创建 Amazon 虚拟私有云。
2. 在两个不同的可用区中部署两个 VPX 实例。
3. 配置高可用性
   a. 在两个实例中以 INC 模式设置高可用性。
   b. 在 VPC 中添加指向客户端接口的相应路由表。
   c. 在主实例中添加一个虚拟服务器。

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两个 VPX 实例，并使用相同数量的 ENI（网络接口）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 是 192.168.0.0/16，则要配置 ADC VIP 地址，您可以从以下 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。您可以选择除 VPC 子网 (192.168.0.0/16) 之外的任何子网。

步骤 4. 从 VPC 路由表添加指向主节点客户端接口 (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 **路由表**，然后选择路由表。
3. 选择 **操作**，然后单击 **编辑路由**。
4. 要添加路由，请选择 **添加路由**。对于 **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，选择主节点客户端接口的 ENI。

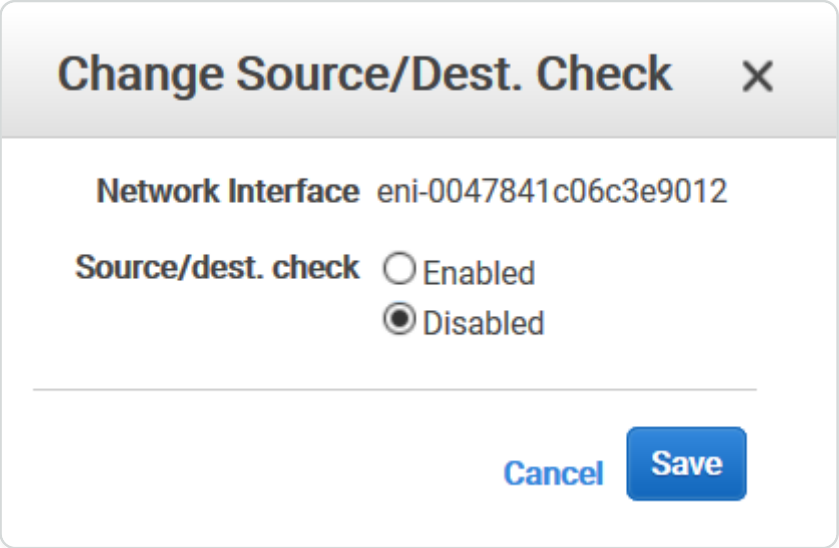
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

您必须在主实例的客户端 ENI 上禁用 **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 **网络接口**。
3. 选择主客户端接口的网络接口，然后选择 **操作**，并单击 **更改源/目标检查**。
4. 在对话框中，选择 **禁用**，然后单击 **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. 在两个实例中以 INC 模式设置高可用性。

   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\> 指的是辅助节点的管理网卡的私有 IP 地址。

   \<prim_ip\> 指的是主节点的管理网卡的私有 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 在主实例上添加一个虚拟服务器。您必须从所选子网中添加它，例如 10.10.10.0/24。

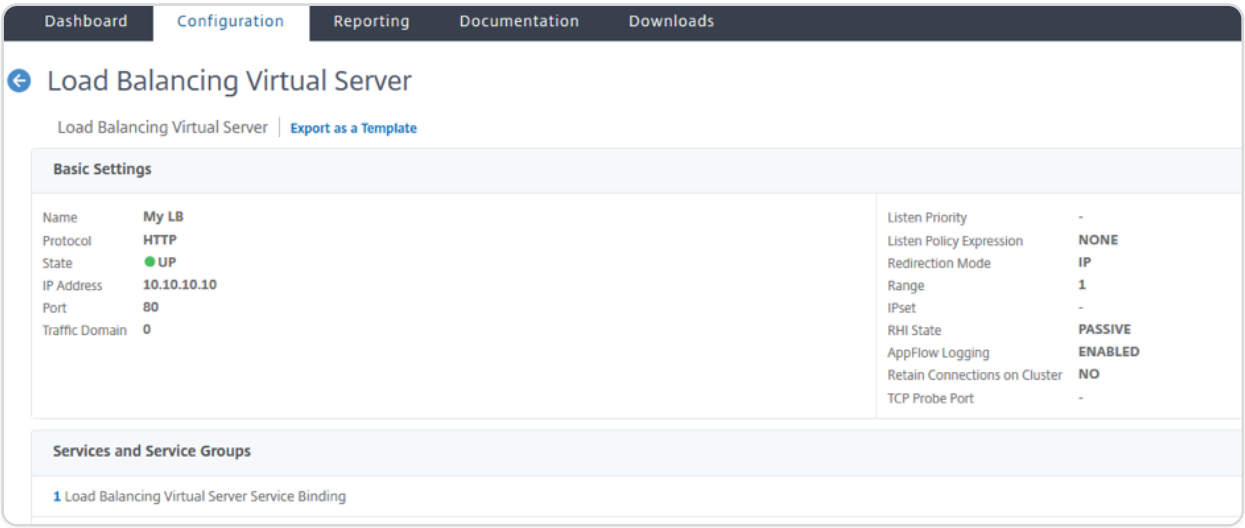
   键入以下命令：

```
add \<server\_type\> vserver \<vserver\_name\> \<protocol\>
\<primary\_vip\> \<port\>
```

使用 GUI 配置高可用性

1. 在两个实例上以 INC 模式设置高可用性
2. 使用用户名 `nsroot` 并将实例 ID 作为密码登录到主节点。
3. 导航到 **Configuration** > **System** > **High Availability**，然后单击 **Add**。
4. 在 **Remote Node IP address** 字段中，添加辅助节点的管理网卡的私有 IP 地址。
5. 在自节点上选择 **Turn on NIC (Independent Network Configuration)** 模式。
6. 在 **Remote System Login Credential** 下，添加辅助节点的用户名和密码，然后单击 **Create**。
7. 在辅助节点中重复这些步骤。
8. 在主实例中添加一个虚拟服务器

   导航到 **配置** > **流量管理** > **虚拟服务器** > **添加**。



使用 AWS 共享 VPC 部署具有私有 IP 地址的 VPX 高可用性对

在 AWS 共享 VPC 模型中，拥有 VPC 的账户（所有者）与其他账户（参与者）共享一个或多个子网。因此，您拥有一个 VPC 所有者账户和一个参与者账户。子网共享后，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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关 AWS 共享 VPC 的信息，请参阅 AWS 文档。

注意：

使用 AWS 共享 VPC 部署具有私有 IP 地址的 VPX 高可用性对的配置步骤与 使用 AWS 非共享 VPC 部署具有私有 IP 地址的 VPX 高可用性对 相同，但有以下例外：

- VPC 中指向客户端接口的路由表必须从 *VPC 所有者账户* 添加。

先决条件

- 确保 AWS 参与者账户中与 NetScaler VPX 实例关联的 IAM 角色具有以下 IAM 权限：

```
"Version": "2012-10-17",

    "Statement": [

        {

            "Sid": "VisualEditor0",

            "Effect": "Allow",

            "Action": [

                "ec2:DisassociateAddress",

                "iam:GetRole",

                "iam:SimulatePrincipalPolicy",

                "ec2:DescribeInstances",

                "ec2:DescribeAddresses",

                "ec2:ModifyNetworkInterfaceAttribute",

                “ec2:AssociateAddress”,

                "sts:AssumeRole"

        ],
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "Resource": "*"
        }
    ]
}
```

注意：

AssumeRole 允许 NetScaler VPX 实例承担由 VPC 所有者账户创建的跨账户 IAM 角色。

- 确保 VPC 所有者账户使用跨账户 IAM 角色向参与者账户提供以下 IAM 权限：

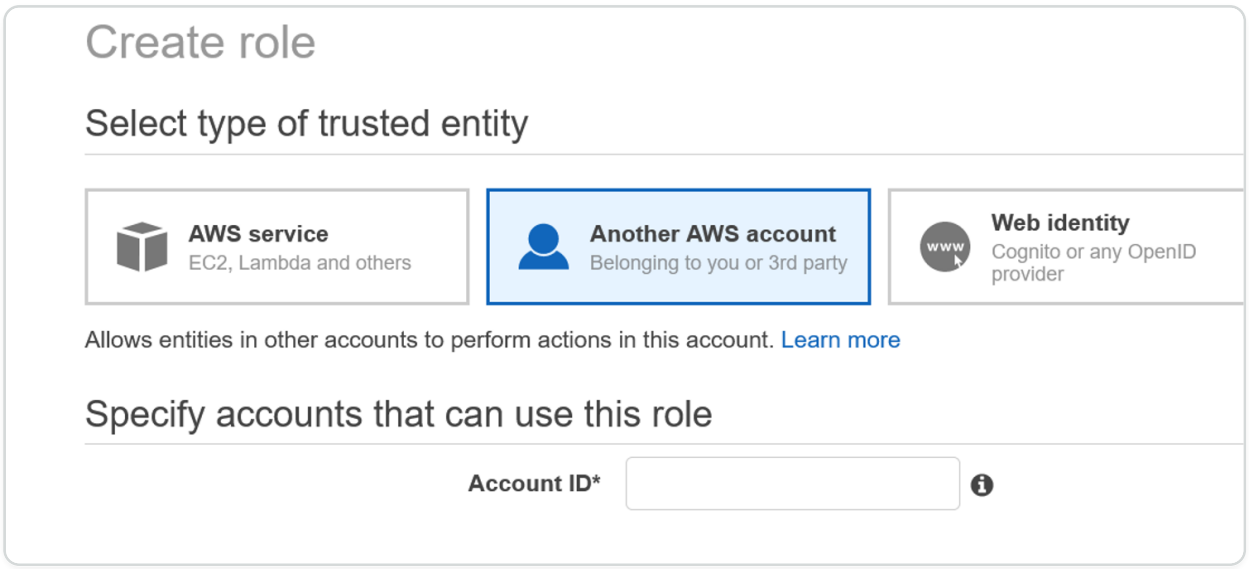
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeRouteTables"
            ],
            "Resource": "*"
        }
    ]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

创建跨账户 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 账户**。



4. 输入您要授予管理员访问权限的参与者账户的 12 位账户 ID 号。

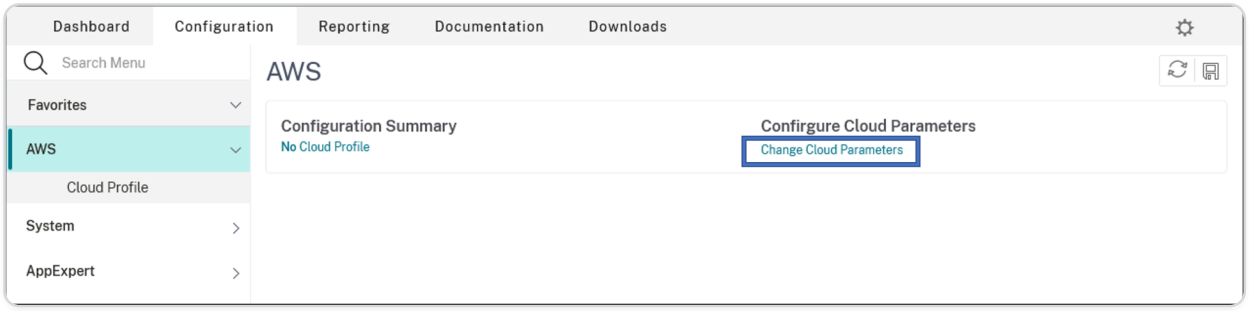
使用 NetScaler CLI 设置跨账户 IAM 角色

以下命令使 NetScaler VPX 实例能够承担 VPC 所有者账户中存在的跨账户 IAM 角色。

```
set cloud awsParam -roleARN <string>
```

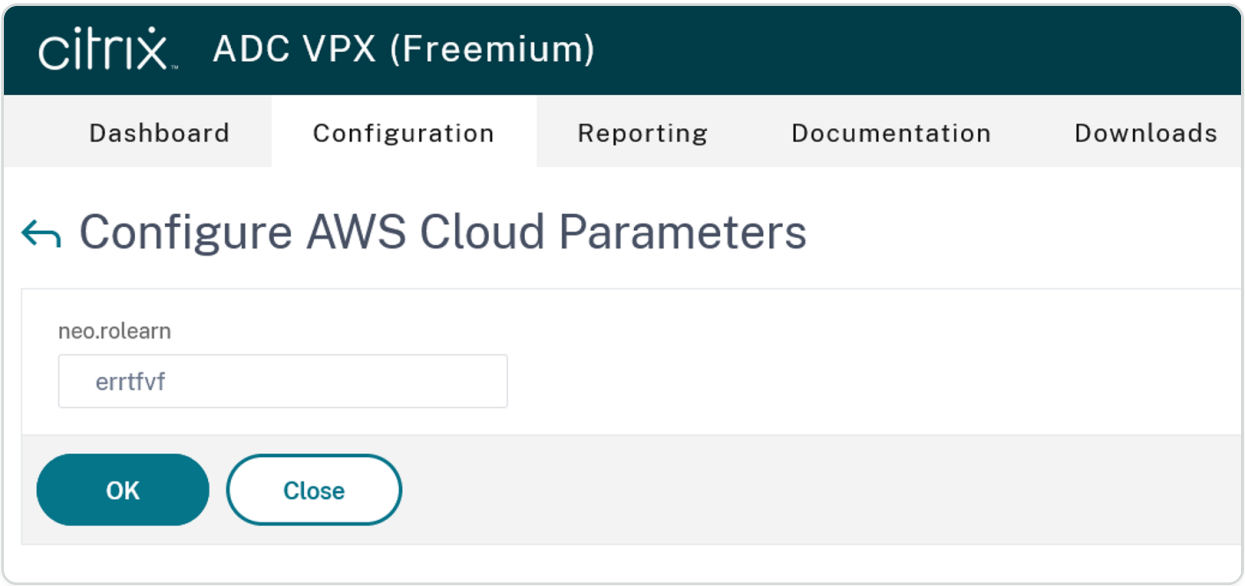
使用 NetScaler GUI 设置跨账户 IAM 角色

1. 登录 NetScaler 设备并导航到 **Configuration > AWS > Change cloud parameters**。



2. 在 **Configure AWS Cloud Parameters** 页面中，输入 **RoleARN** 字段的值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

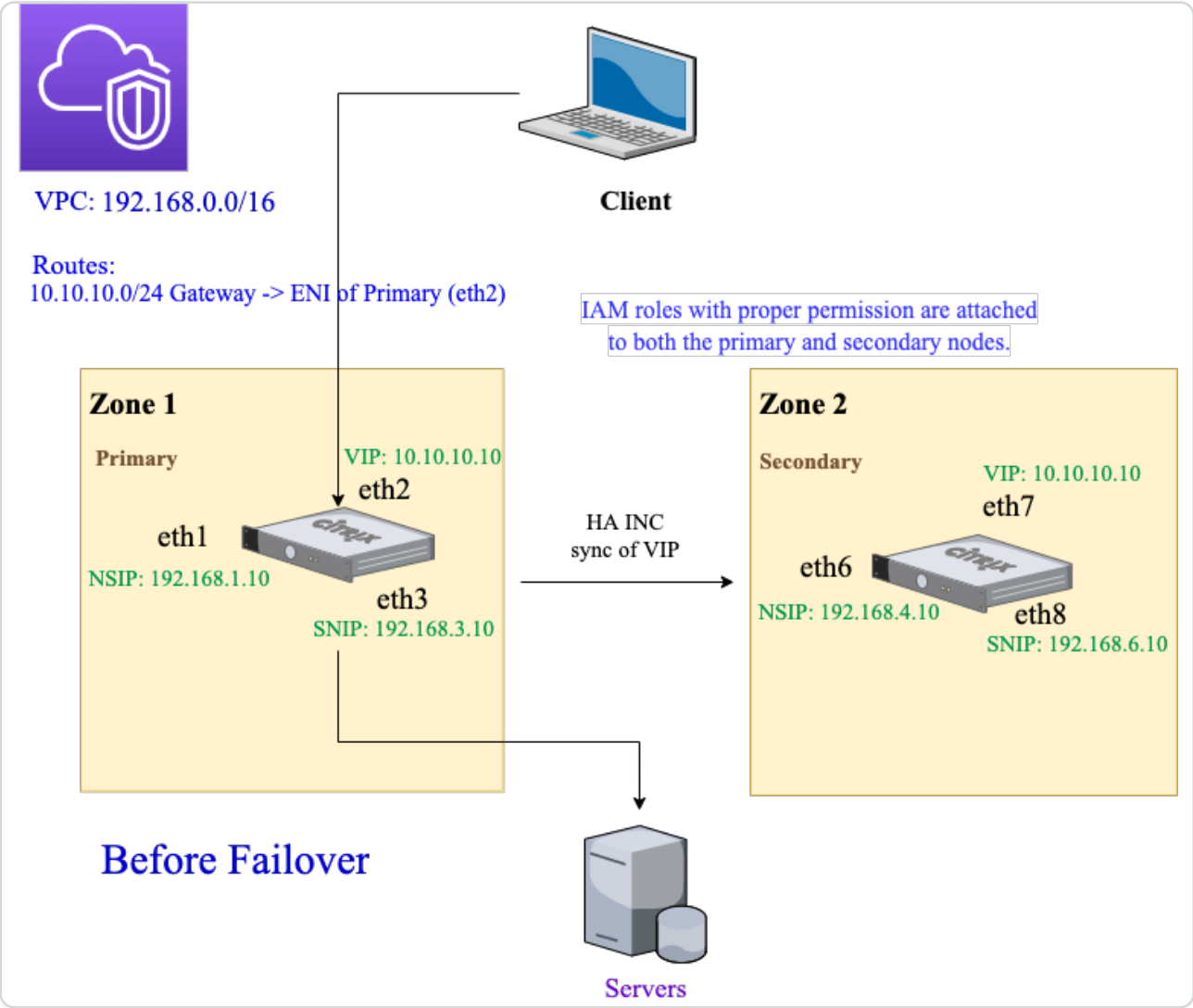


场景

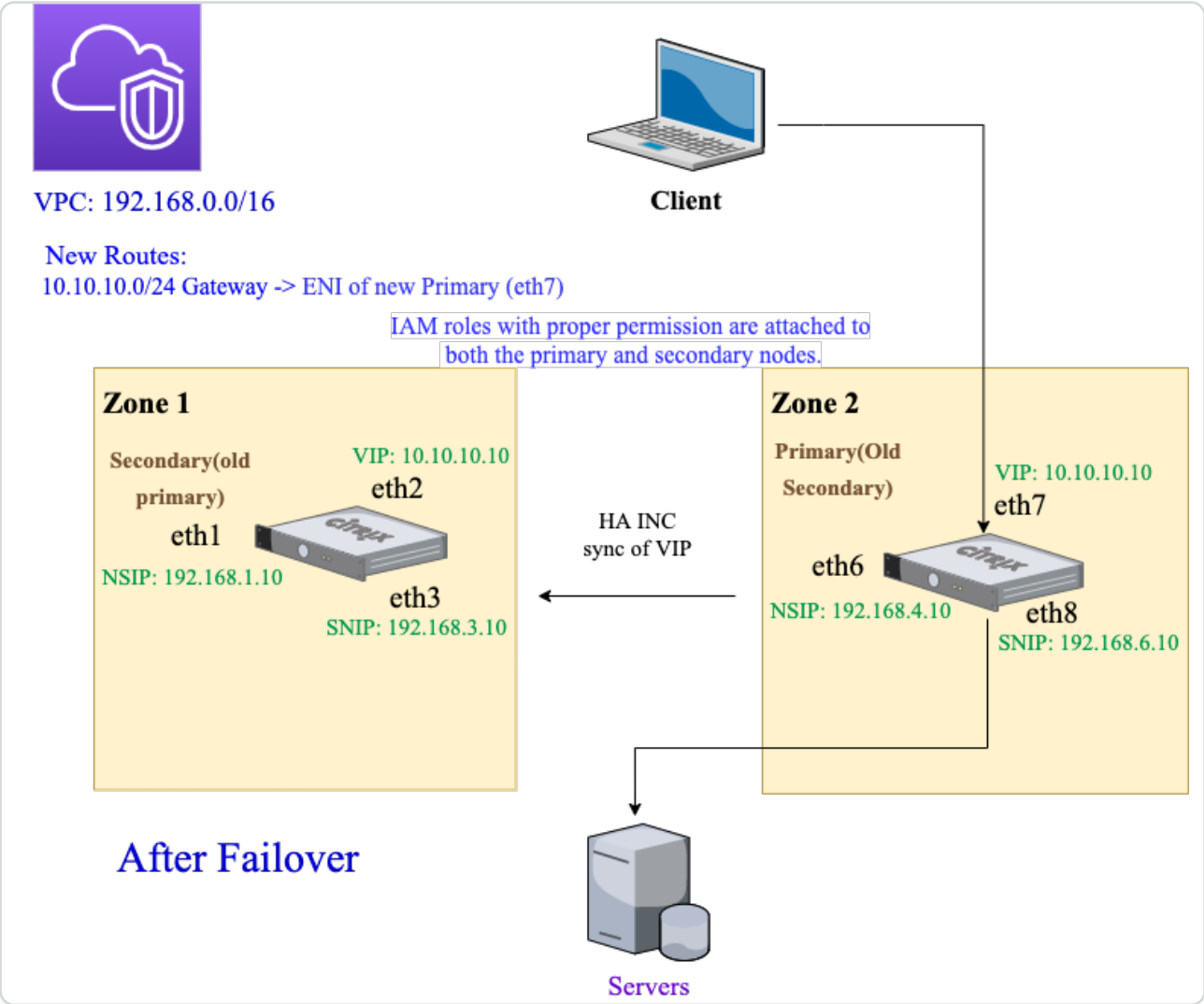
在此场景中，将创建一个 VPC。在该 VPC 中，在两个可用区中创建了两个 VPX 实例。每个实例有三个子网 - 一个用于管理，一个用于客户端，一个用于后端服务器。

以下图表说明了 AWS 上 INC 模式下的 NetScaler VPX 高可用性设置。自定义子网 10.10.10.10 不属于 VPC，用作 VIP。因此，10.10.10.10 子网可以在可用区之间使用。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



对于此场景，请使用 CLI 配置高可用性。

1. 在两个实例上以 INC 模式设置高可用性。

   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 指的是辅助节点的管理 NIC 的私有 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 指的是主节点的管理 NIC 的私有 IP 地址。

2. 在主实例上添加一个虚拟服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

键入以下命令：

```
add lbvserver vserver1 http 10.10.10.10 80
```

3. 保存配置。
4. 强制故障转移后：
   - 辅助实例成为新的主实例。
   - 指向主 ENI 的 VPC 路由迁移到辅助客户端 ENI。
   - 客户端流量恢复到新的主实例。

用于 HA 私有 IP 解决方案的 AWS Transit Gateway 配置

您需要 AWS Transit Gateway 才能使私有 VIP 子网在内部网络、AWS VPC、区域和本地网络中可路由。VPC 必须连接到 AWS Transit Gateway。在 AWS Transit Gateway 路由表内为 VIP 子网或 IP 池创建静态路由，并将其指向 VPC。

AWS 传输网关(/en-us/vpx/media/aws-transit-gateway.png)

要配置 AWS Transit Gateway，请按照以下步骤操作：

1. 打开 Amazon VPC 控制台。
2. 在导航窗格中，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**。

   AWS Transit Gateway 路由表(/en-us/vpx/media/aws-transit-gateway-route-table.png)
4. 创建静态路由，其中 CIDR 指向您的私有 VIPS 子网，附件指向包含 NetScaler VPX 的 VPC。

   创建静态路由(/en-us/vpx/media/tg-create-static-route.png)
5. 单击 **创建静态路由**，然后选择 **关闭**。

故障排除

如果在跨多区域 HA 配置 HA 私有 IP 解决方案时遇到任何问题，请检查以下关键点进行故障排除：

- 主节点和辅助节点都具有相同的 IAM 权限集。
- 主节点和辅助节点均已启用 INC 模式。
- 主节点和辅助节点具有相同数量的接口。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 创建实例时，请在两个节点上遵循相同的接口连接顺序。在主节点上，如果先连接客户端接口，后连接服务器接口。那么，在辅助节点上也请遵循相同的顺序。如果存在任何不匹配，请按正确的顺序分离并重新连接接口。
- 如果流量不通，请确保首次在主节点的客户端接口上禁用“源/目标检查”。
- 确保 cloudhadaemon 命令 (`ps -aux | grep cloudha`) 正在 Shell 中运行。
- 确保 NetScaler 固件版本为 13.0 build 70.x 或更高版本。
- 对于故障转移过程中的问题，请检查位于以下位置的日志文件：/var/log/cloud-ha-daemon.log

在 AWS Outposts 上部署 NetScaler VPX 实例

AWS Outposts 是部署在您站点的 AWS 计算和存储容量池。Outposts 在您的本地位置提供 AWS 基础设施和服务。AWS 作为 AWS 区域的一部分，对这些容量进行操作、监控和管理。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。

您可以在 Outposts 上创建子网，并在创建 AWS 资源（例如 EC2 实例、EBS 卷、ECS 集群和 RDS 实例）时指定它们。Outposts 子网中的实例使用私有 IP 地址与 AWS 区域中的其他实例通信，所有这些都在同一个 Amazon Virtual Private Cloud (VPC) 中。

有关更多信息，请参阅 AWS Outposts 用户指南。

AWS Outposts 的工作原理

AWS Outposts 旨在通过 Outposts 与 AWS 区域之间持续稳定的连接来运行。为了实现与区域以及本地环境中本地工作负载的连接，您必须将 Outpost 连接到您的本地网络。您的本地网络必须提供回区域和互联网的 WAN 访问。互联网还必须提供对本地网络（您的本地工作负载或应用程序所在的位置）的 LAN 或 WAN 访问。

先决条件

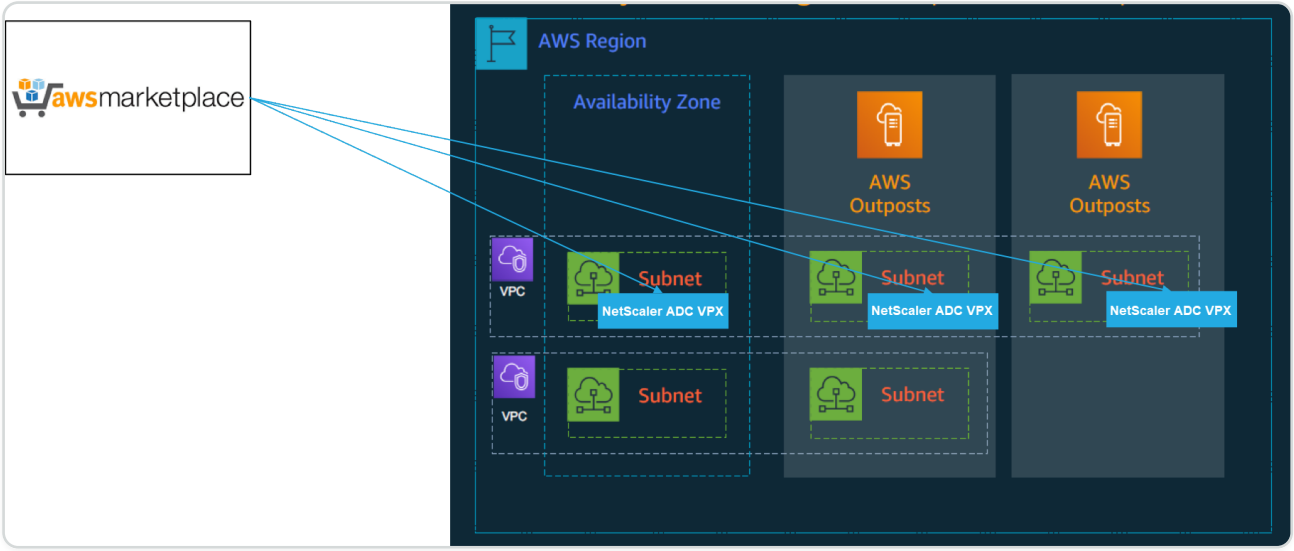
- 您必须在您的站点安装 AWS Outposts。
- AWS Outposts 的计算和存储容量必须可用。

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

下图描述了在 Outposts 上部署 NetScaler VPX 实例的简单过程。AWS Marketplace 中存在的 NetScaler AMI 也部署在 Outposts 中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



登录 AWS Web 控制台并完成以下步骤，以在您的 AWS Outposts 上部署 NetScaler VPX EC2 实例。

1. 创建密钥对。
2. 创建一个虚拟私有云 (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. 创建一个互联网网关。
7. 使用 AWS EC2 服务创建一个 NetScaler VPX 实例。 从 AWS 控制面板，导航到 **计算 > EC2 > 启动实例 > AWS Marketplace**。
8. 创建并附加更多网络接口。
9. 将弹性 IP 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。

有关同一可用区部署中的高可用性，请参阅 在 AWS 上部署高可用性对。

在包含 AWS Outposts 的混合云上部署 NetScaler VPX 实例

您可以在包含 AWS Outposts 的 AWS 环境中的混合云上部署 NetScaler VPX 实例。您可以使用 NetScaler 全局服务器负载均衡 (GSLB) 解决方案简化应用程序交付机制。GSLB 解决方案将应用程序流量分发到使用 AWS 区域和 AWS Outposts 基础设施构建的混合云中的多个数据中心。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler GSLB 支持主动-主动和主动-被动两种部署类型，以应对不同的用例。除了这些灵活的部署选项和应用程序交付机制之外，NetScaler 还保护整个网络和应用程序组合，无论应用程序是原生部署在 AWS 云上还是 AWS Outposts 上。

下图说明了在包含 AWS 的混合云中使用 NetScaler 设备进行应用程序交付。

混合云 AWS Outpost(/en-us/vpx/media/hybrid-cloud-aws-outpost-citrix.png)

在主动-主动部署中，NetScaler 在分布式环境中全局引导流量。环境中的所有站点通过度量交换协议 (MEP) 交换有关其可用性和资源运行状况的度量。NetScaler 设备使用此信息在站点之间进行流量负载平衡，并根据 GSLB 配置中指定的定义方法（轮询、最少连接和静态邻近性）将客户端请求发送到最合适的 GSLB 站点。

您可以使用主动-主动 GSLB 部署来：

- 优化资源利用率，所有节点都处于活动状态。
- 通过将请求引导至离每个用户最近的站点来增强用户体验。
- 以用户定义的速率将应用程序迁移到云。

您可以将主动-被动 GSLB 部署用于：

- 灾难恢复
- 云爆发

参考

- 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 Gateway

您可以在 AWS API Gateway 前部署 NetScaler 设备，以保护 API 网关免受外部威胁。NetScaler Web App Firewall (WAF) 可以防御 OWASP 十大威胁和零日攻击。NetScaler Web App Firewall 在所有 ADC 外形规格上使用单一代码库。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，并以单一许可证形式提供。NetScaler Web App Firewall 为您提供以下功能：

- 简化配置
- 僵尸程序管理

© 1997–2026 Citrix Systems, Inc. All rights reserved.

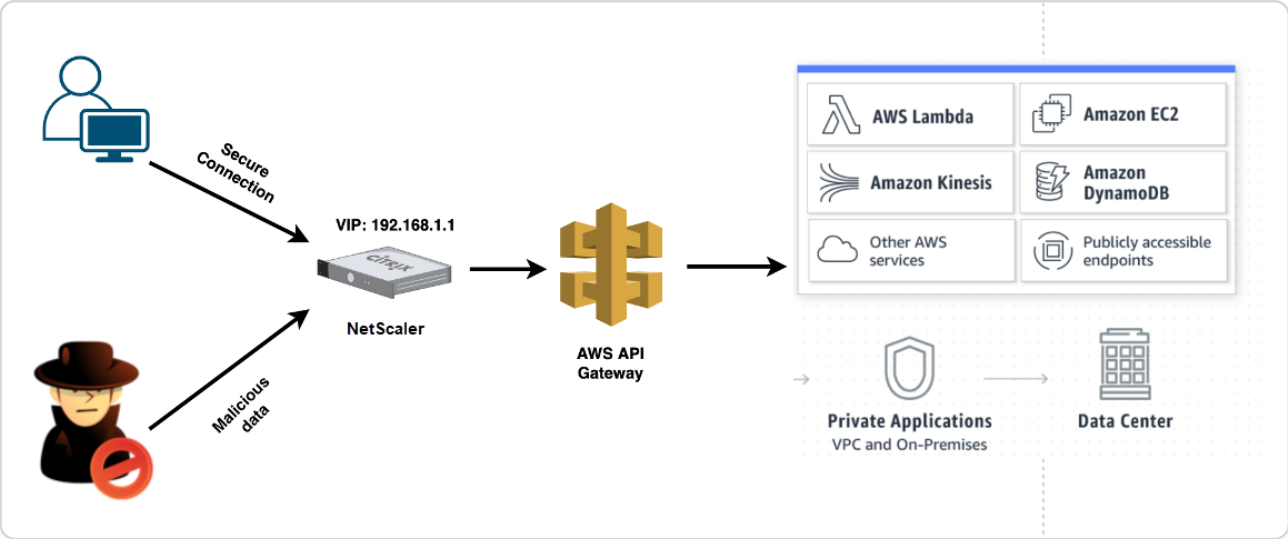
- 整体可见性
- 整合来自多个来源的数据并在统一屏幕中显示数据

除了 API 网关保护之外，您还可以使用其他 NetScaler 功能。有关详细信息，请参阅 (/zh-cn/citrix-adc/13-1/)。此外，为了避免数据中心故障转移并最大限度地缩短停机时间，您可以将 ADC 部署在可用区内或跨可用区的高可用性配置中。您还可以使用或配置具有自动缩放功能的集群。

以前，AWS API Gateway 不支持保护其背后应用程序所需的防护措施。如果没有 Web Application Firewall (WAF) 保护，API 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 网关前面。



假设有一个针对 AWS Lambda 服务的真实 API 请求。此请求可以是 Amazon API Gateway 文档 中提到的任何 API 服务。如上图所示，流量流如下：

1. 客户端向 AWS Lambda 函数 (XYZ) 发送请求。此客户端请求发送到 NetScaler 虚拟服务器 (192.168.1.1)。
2. 虚拟服务器检查数据包并检查是否存在任何恶意内容。
3. NetScaler 设备触发重写策略以更改客户端请求中的主机名和 URL。例如，您想将 `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，则恶意请求将到达 NetScaler 设备。
7. NetScaler 设备检查数据包并根据配置的操作丢弃数据包。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 地址为 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。有关更多信息，请参阅 配置 Web App Firewall。
3. 启用重写策略以更改域名。例如，您希望将传入的对“restapi.citrix.com”域名的负载平衡器请求重写为后端 AWS API Gateway 的“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
```

在前面示例的步骤 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”，并将 URL 替换为“default/lambda/XYZ”。

以下过程描述了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 登录到 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"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，请参阅配置重写以更改 NetScaler 设备上客户端请求中的主机名和 URL。

NetScaler 功能和特性

NetScaler 设备除了保护部署外，还可以根据用户要求增强请求。NetScaler 设备提供以下主要功能。

- **负载均衡 API 网关：** 如果您有多个 API 网关，可以使用 NetScaler 设备对多个 API 网关进行负载均衡，并定义 API 请求的行为。
  - 有多种负载均衡方法可用。例如，“最少连接”方法可避免 API 网关限制过载，“自定义负载”方法可在特定 API 网关上保持特定负载，等等。有关详细信息，请参阅负载均衡算法。
  - SSL 卸载的配置不会中断流量。
  - 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：您可以拥有自己的 SSL 虚拟服务器，并使用自己的签名证书和算法。
  - 备份虚拟服务器：如果 API 网关无法访问，您可以将请求发送到备份虚拟服务器以进行进一步操作。
  - 还有许多其他负载均衡功能可用。有关详细信息，请参阅在 NetScaler 设备上负载均衡流量。
- **身份验证、授权和审计：** 您可以定义自己的身份验证方法，如 LDAP、SAML、RADIUS，并授权和审计 API 请求。
- **响应程序：** 您可以在关机期间将 API 请求重定向到其他 API 网关。
- **速率限制：** 您可以配置速率限制功能，以避免 API 网关过载。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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，为您的 AWS API 流量提供更好的可用性。
- **REST API：** 支持 REST API，可用于自动化云生产环境中的工作。
- **监控数据：** 监控并记录数据以供参考。

NetScaler 设备提供了更多功能，可与 AWS API 网关集成。有关更多信息，请参阅 NetScaler 文档。

添加后端 AWS 自动扩缩服务

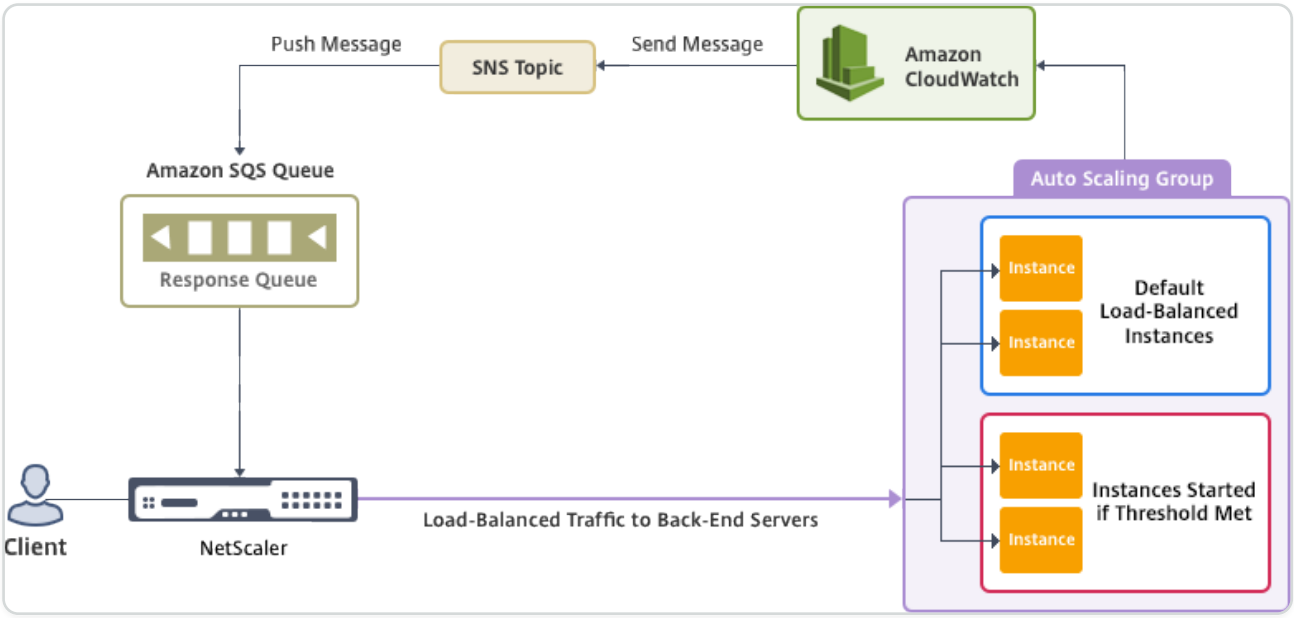
在云中高效托管应用程序涉及根据应用程序需求轻松且经济高效地管理资源。为了满足不断增长的需求，您必须向上扩展网络资源。无论需求是否减弱，您都需要缩减规模以避免闲置资源造成不必要的成本。为了通过在任何给定时间仅部署所需数量的实例来最大程度地降低运行应用程序的成本，您必须持续监控流量、内存和 CPU 使用情况等。然而，手动监控流量很麻烦。为了使应用程序环境能够动态地向上或向下扩展，您必须在必要时自动化监控流量以及向上和向下扩展资源的过程。

NetScaler VPX 实例与 AWS 自动扩缩服务集成，提供以下优势：

- **负载平衡和管理**：根据需求自动配置服务器以进行扩缩。VPX 实例自动检测后端子网中的 Autoscale™ 组，并允许用户选择 Autoscale 组以平衡负载。所有这些都通过在 VPX 实例上自动配置虚拟和子网 IP 地址来完成。
- **高可用性**：检测跨多个可用区并进行服务器负载平衡的 Autoscale 组。
- **更好的网络可用性**：VPX 实例支持：
  - 通过使用 VPC 对等连接，在不同 VPC 上的后端服务器
  - 位于相同放置组中的后端服务器
  - 位于不同可用区中的后端服务器
- **优雅连接终止**：通过使用优雅超时功能，在缩减活动发生时，优雅地移除自动扩缩服务器，避免客户端连接丢失。

图表：带有 NetScaler VPX 实例的 AWS 自动扩缩服务

© 1997–2026 Citrix Systems, Inc. All rights reserved.



此图表说明了 AWS 自动扩缩服务如何与 NetScaler VPX 实例（负载平衡虚拟服务器）兼容。有关更多信息，请参阅以下 AWS 主题。

- 自动扩缩组
- CloudWatch
- 简单通知服务 (SNS)
- 简单队列服务 (Amazon SQS)

开始之前

在使用 Autoscaling 与您的 NetScaler VPX 实例之前，您必须完成以下任务。

1. 阅读以下主题：
   - 先决条件
   - 限制和使用指南
2. 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：

Citrix 建议使用 CloudFormation 模板在 AWS 上创建 NetScaler VPX 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix® 建议您创建三个接口：一个用于管理 (NSIP)，一个用于面向客户端的 LB 虚拟服务器 (VIP)，一个用于子网 IP (NSIP)。

3. 创建 AWS 自动扩缩组。如果您没有现有的自动扩缩配置，则必须：

   a) 创建启动配置

   b) 创建自动扩缩组

   c) 验证自动扩缩组

   有关更多信息，请参阅 `<http://docs.aws.amazon.com/autoscaling/latest/userguide/GettingStartedTutorial.html>`。

4. 在 AWS 自动扩缩组中，您必须至少指定一个缩减策略。NetScaler VPX 实例仅支持步进扩缩策略。自动扩缩组不支持简单扩缩策略和目标跟踪扩缩策略。

将 AWS 自动扩缩服务添加到 NetScaler VPX 实例

您可以使用 GUI 通过单击将自动扩缩服务添加到 VPX 实例。完成以下步骤以将自动扩缩服务添加到 VPX 实例：

1. 使用您的 `nsroot` 凭据登录到 VPX 实例。
2. 首次登录 NetScaler VPX 实例时，您会看到默认的“云配置文件”页面。从下拉菜单中选择 AWS 自动扩缩组，然后单击“**创建**”以创建云配置文件。如果您想稍后创建云配置文件，请单击“**跳过**”。

   创建云配置文件时需要注意的事项：默认情况下，CloudFormation 模板会创建并附加以下 IAM 角色。

```
{



    "Version": "2012-10-17",

    "Statement": \[



     {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "Action": \[


                "ec2:DescribeInstances",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DetachNetworkInterface",

                "ec2:AttachNetworkInterface",

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:RebootInstances",

                "autoscaling:\*",

                "sns:\*",

                "sqs:\*"


            “iam: SimulatePrincipalPolicy”

            “iam: GetRole”


            \],


            "Resource": "\*",

            "Effect": "Allow"


        }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

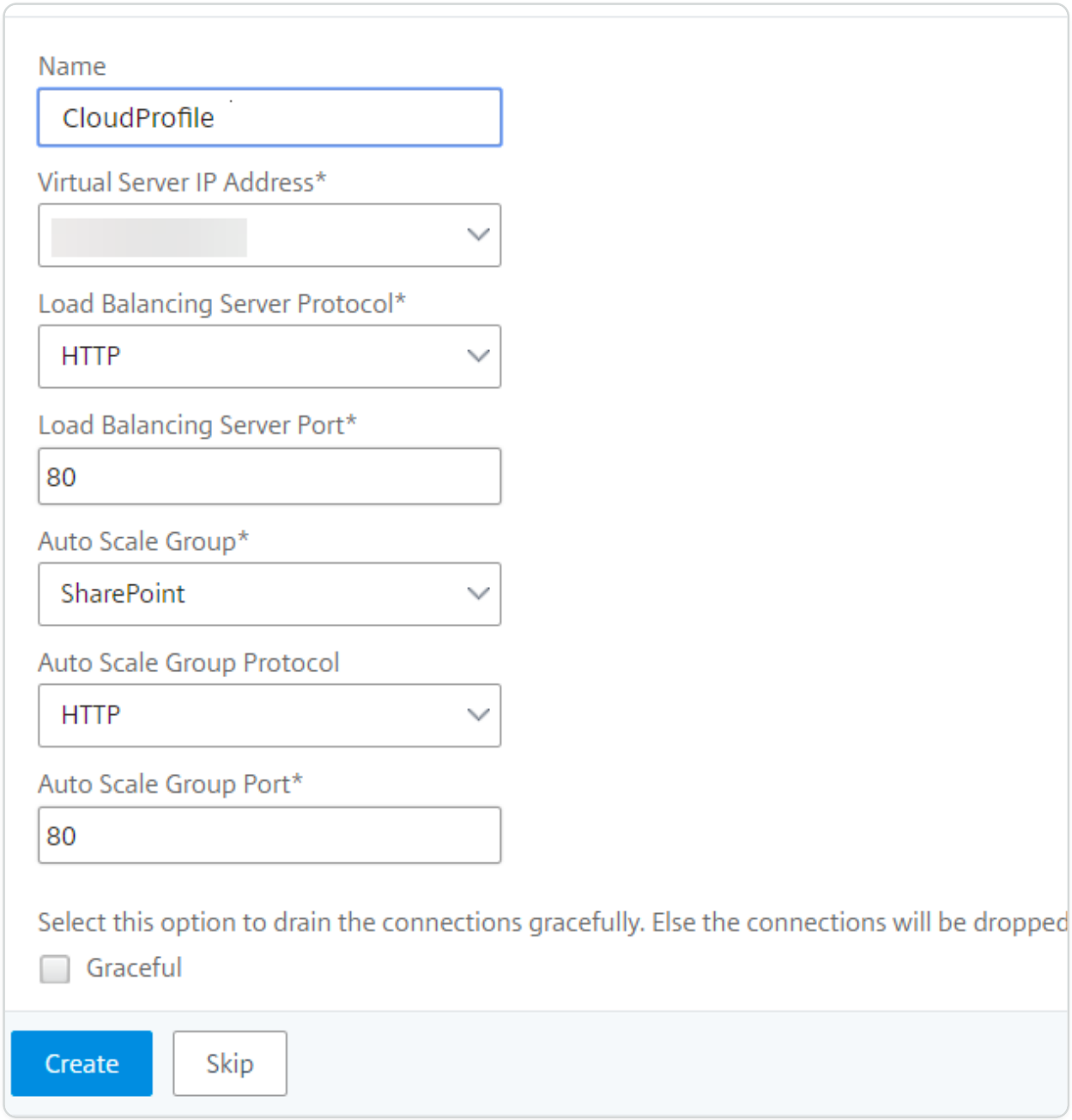
```
    \]


}
```

确保实例的 IAM 角色具有适当的权限。

- 虚拟服务器 IP 地址将从 VPX 实例可用的空闲 IP 地址自动填充。`<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html#ManageMultipleIP>`
- 自动扩缩组将从您的 AWS 账户上配置的自动扩缩组预填充。`<http://docs.aws.amazon.com/autoscaling/latest/userguide/AutoScalingGroup.html>`。
- 在选择自动扩缩组协议和端口时，请确保您的服务器侦听这些协议和端口，并且您在服务组中绑定了正确的监视器。默认情况下，使用 TCP 监视器。
- 对于 SSL 协议类型的自动扩缩，在创建云配置文件后，由于缺少证书，负载均衡虚拟服务器或服务组将处于关闭状态。您可以手动将证书绑定到虚拟服务器或服务组。
- 选择“优雅超时”选项以优雅地移除自动扩缩服务器。如果未选择此选项，则在负载下降后，自动扩缩组中的服务器会立即被移除，这可能会导致现有连接客户端的服务中断。选择“优雅”并设置超时意味着在缩减事件中，VPX 实例不会立即移除服务器，而是将其中一个服务器标记为优雅删除。在此期间，实例不允许新连接到此服务器。现有连接将一直提供服务，直到超时发生，超时后，VPX 实例将移除该服务器。

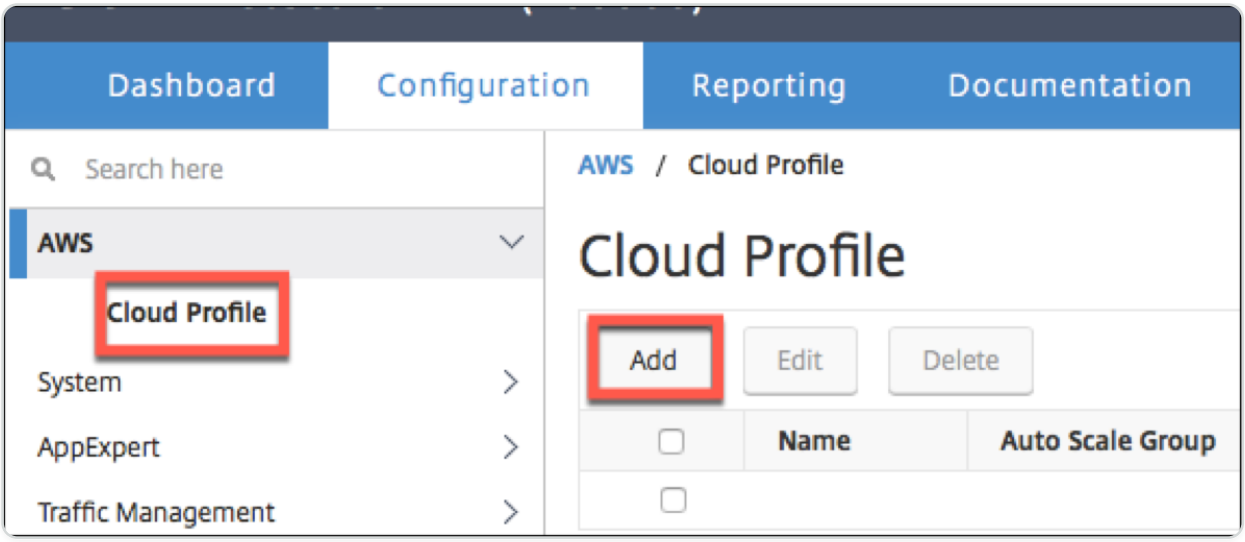
图示： 默认云配置文件页面

© 1997–2026 Citrix Systems, Inc. All rights reserved.

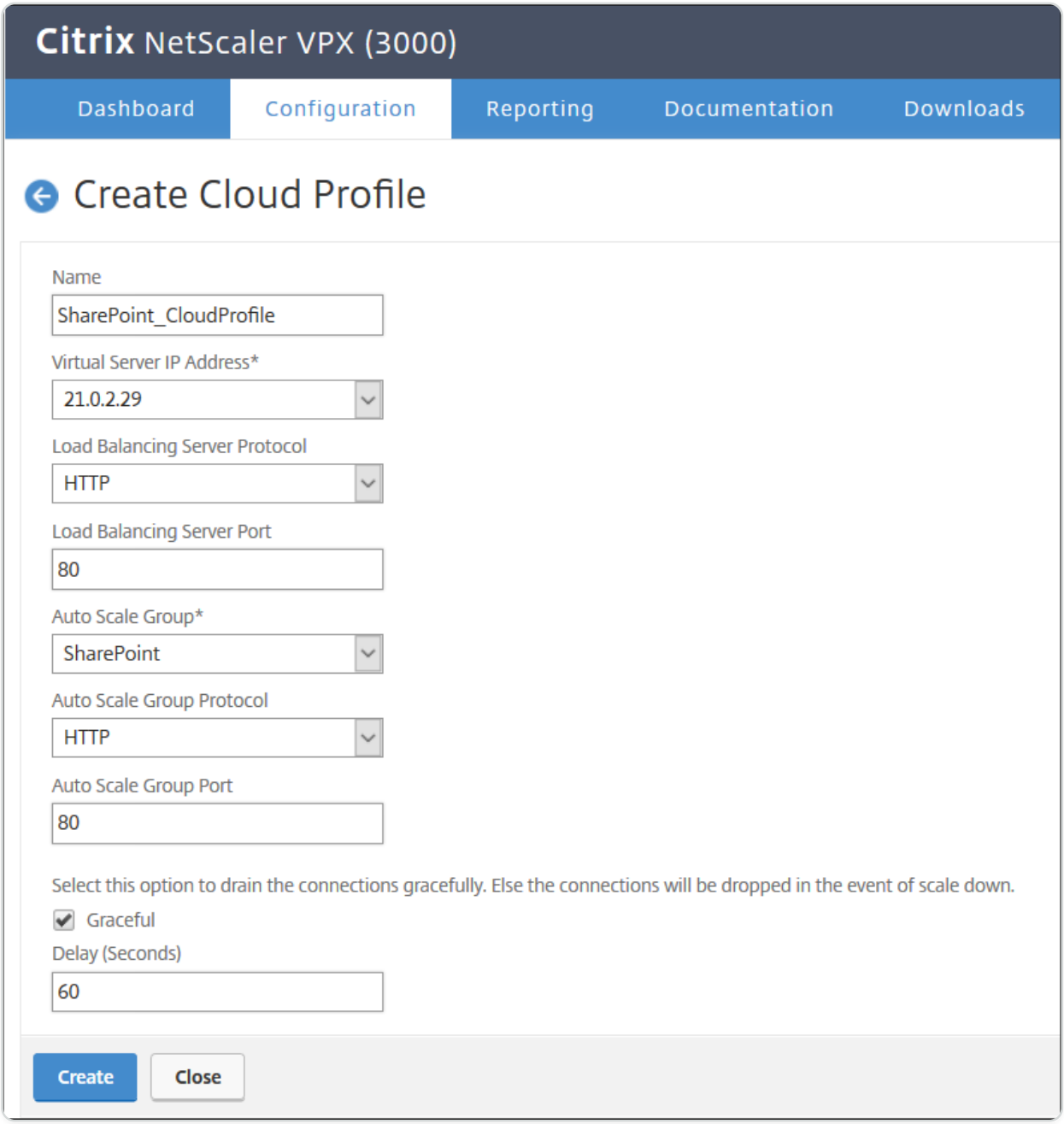


3. 首次登录后，如果要创建云配置文件，请在 GUI 上转到“**系统 > AWS > 云配置文件**”，然后单击“**添加**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



“**创建云配置文件**”配置页面随即出现。

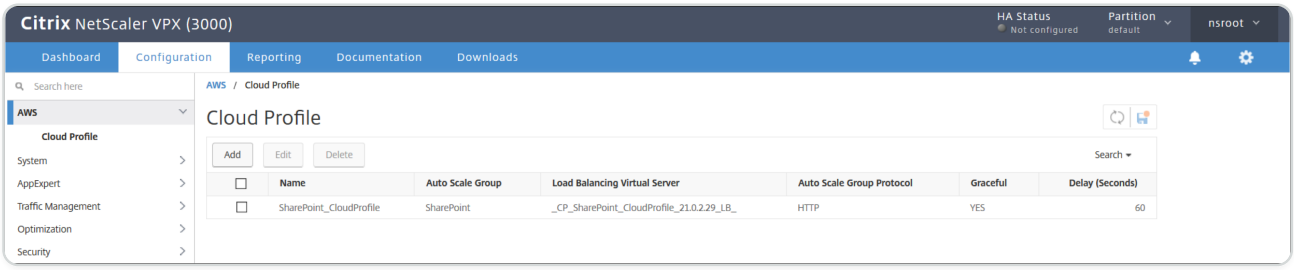


© 1997–2026 Citrix Systems, Inc. All rights reserved.

云配置文件会创建一个 NetScaler 负载平衡虚拟服务器以及一个服务组，其成员是自动扩缩组的服务器。您的后端服务器必须可通过在 VPX 实例上配置的 SNIP 访问。

注意：

从 NetScaler 13.1-42.x 版本开始，您可以为不同的服务（使用不同的端口）创建不同的云配置文件，在 AWS 中使用相同的自动扩缩组 (ASG)。因此，NetScaler VPX 实例在公有云中支持具有相同自动扩缩组的多个服务。

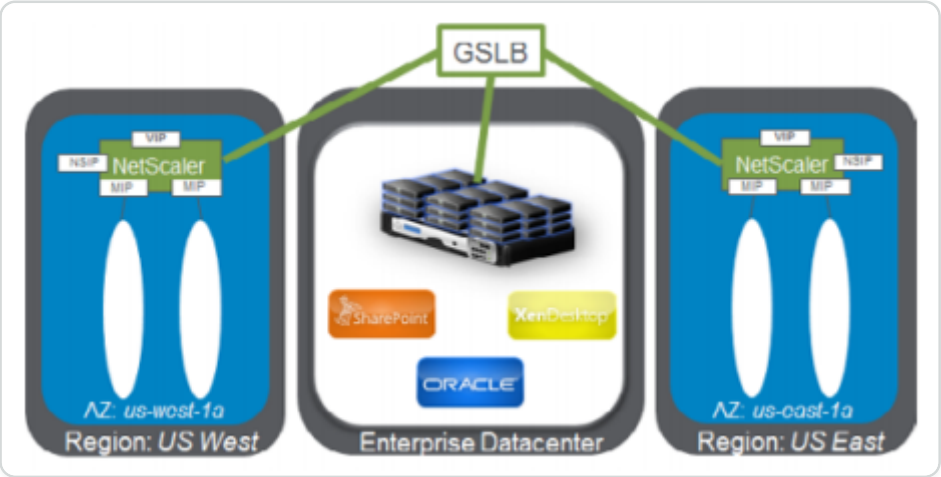


注意：

要在 AWS 控制台中查看自动扩缩相关信息，请转到“**EC2**”>“**控制面板**”>“**自动扩缩**”>“**自动扩缩组**”。

在 AWS 上部署 NetScaler GSLB

在 AWS 上为 NetScaler 设置 GSLB 主要包括配置 NetScaler，以将流量负载均衡到 NetScaler 所属 VPC 之外的服务器，例如位于不同可用区中的另一个 VPC 内，或位于本地数据中心。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

DBS 概述

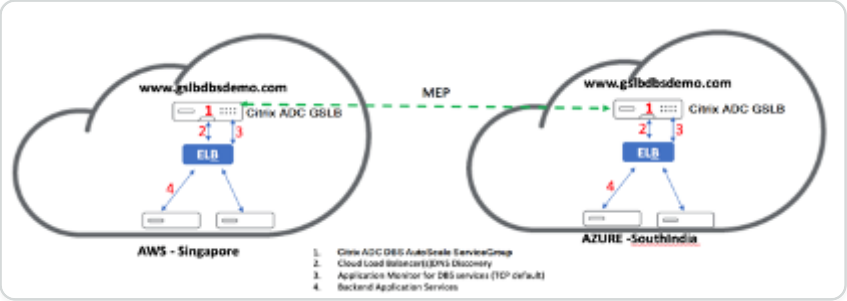
NetScaler GSLB 支持使用 DBS（基于域的服务）用于云负载均衡器，允许使用云负载均衡器解决方案自动发现动态云服务。此配置允许 NetScaler 在 Active-Active 环境中实施全局服务器负载均衡域名服务 (GSLB DBS)。DBS 允许通过 DNS 发现来扩展 AWS 环境中的后端资源。

本节介绍 AWS AutoScaling 环境中 NetScaler 之间的集成。文档的最后一部分详细介绍了设置一对 NetScaler ADC HA 对的能力，该 HA 对可跨越特定于 AWS 区域的两个不同可用区 (AZ)。

基于域名的服务 (DBS) 与 ELB

GSLB DBS 利用用户弹性负载均衡器 (ELB) 的 FQDN 动态更新 GSLB 服务组，以包含在 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根据网络需求或 CPU 利用率进行扩展配置。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，而无需在每次在 AWS 中创建和删除实例时手动更新 NetScaler。NetScaler GSLB 服务组的 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 自动扩展组件与云负载均衡器：



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，因为这些实体各自所需的规则集不同。为简洁起见，本示例采用合并的安全组配置。

为确保正确配置虚拟防火墙，请参阅 您的 VPC 的安全组。

1. 登录用户 **AWS 资源组**，然后导航到 **EC2 > NETWORK & SECURITY > 安全组**。
2. 单击 **创建安全组** 并提供名称和描述。此安全组包含 NetScaler 和 Linux 后端 Web 服务器。
3. 从以下屏幕截图添加入站端口规则。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

建议限制源 IP 访问以实现精细强化。有关更多信息，请参阅 Web 服务器规则。

4. Amazon Linux 后端 Web 服务

   a. 登录用户 **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。

5. NetScaler 配置

   a. 登录用户 **AWS 资源组**，然后导航到 **EC2 > 实例**。

   b. 单击 **启动实例** 并使用以下详细信息配置 **Amazon AMI** 实例。

6. 弹性 IP 配置

注意：

如果需要降低成本，NetScaler 也可以使用单个弹性 IP 运行，方法是不为 NSIP 分配公共 IP。相反，将弹性 IP 附加到 SNIP，除了 GSLB 站点 IP 和 ADNS IP 之外，该 SNIP 还可以用于设备的管理访问。

   a. 登录到用户 **AWS 资源组**，然后导航到 **EC2 > 网络与安全 > 弹性 IP**。

   b. 单击 **分配新地址** 以创建弹性 IP 地址。

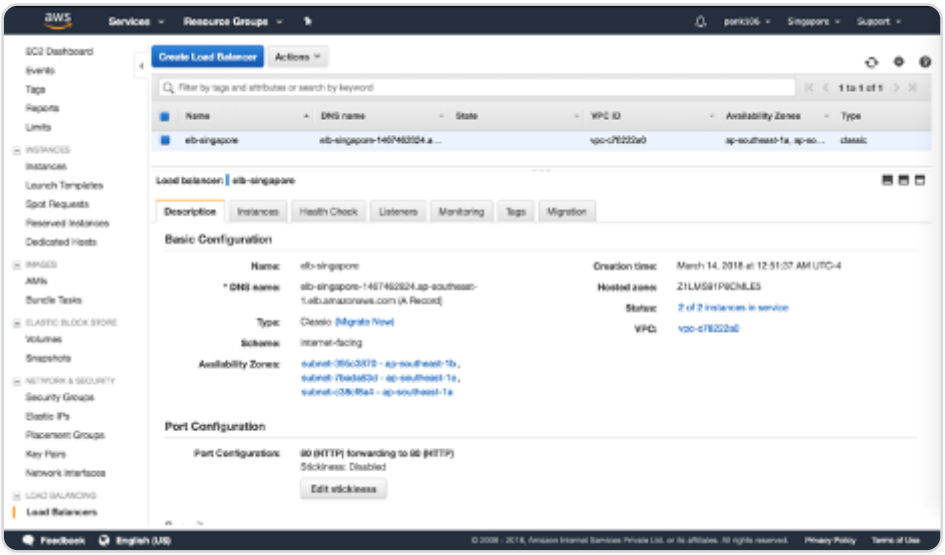
   c. 配置弹性 IP 以指向 AWS 中用户正在运行的 NetScaler 实例。

   d. 配置第二个弹性 IP，并再次将其指向用户正在运行的 NetScaler 实例。

7. 弹性负载均衡器

   a. 登录到用户 **AWS 资源组**，然后导航到 **EC2 > 负载均衡 > 负载均衡器**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. 单击 **创建负载均衡器** 以配置经典负载均衡器。

用户弹性负载均衡器允许用户对其后端 Amazon Linux 实例进行负载均衡，同时还能够对根据需求启动的其他实例进行负载均衡。

配置基于域名的全局服务器负载均衡服务

有关流量管理配置，请参阅 配置基于域的 NetScaler GSLB 服务。

部署类型

三网卡部署

- 典型部署
  - GSLB 样式手册
  - 使用 ADM
  - 使用 GSLB（Route53 带域名注册）
  - 许可 - 池化/市场
- 用例
  - 三网卡部署用于实现数据和管理流量的真正隔离。
  - 三网卡部署还可提高 ADC 的规模和性能。
  - 三网卡部署用于吞吐量通常为 1 Gbps 或更高的网络应用程序，建议采用三网卡部署。

CFT 部署

如果客户正在自定义或自动化其部署，他们将使用 CloudFormation 模板进行部署。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

部署步骤

以下是部署步骤：

1. GSLB 的三网卡部署
2. 许可
3. 部署选项

GSLB 的三网卡部署

NetScaler VPX 实例在 AWS Marketplace 中作为 Amazon Machine Image (AMI) 提供，并且可以在 AWS VPC 中作为 Elastic Compute Cloud (EC2) 实例启动。NetScaler VPX 上支持的 AMI 允许的最低 EC2 实例类型是 m4.large。NetScaler VPX AMI 实例至少需要 2 个虚拟 CPU 和 2 GB 内存。在 AWS VPC 中启动的 EC2 实例还可以提供 VPX 配置所需的多个接口、每个接口的多个 IP 地址以及公共和私有 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 建议为 AWS 安装上的标准 VPX 实例配置三个网络接口。

AWS 目前仅向在 AWS VPC 中运行的实例提供多 IP 功能。VPC 中的 VPX 实例可用于对在 EC2 实例中运行的服务器进行负载均衡。Amazon VPC 允许用户创建和控制虚拟网络环境，包括其自己的 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 账户在每个 AWS 区域最多可以创建 5 个 VPC 实例。用户可以通过在此处提交 Amazon 的请求表单来请求更高的 VPC 限制：Amazon VPC 请求。

许可

AWS 上的 NetScaler VPX 实例需要许可证。以下是适用于在 AWS 上运行的 NetScaler VPX 实例的许可选项：

- 免费（无限制）
- 按小时计费
- 按年计费

自带许可证

© 1997–2026 Citrix Systems, Inc. All rights reserved.

免费试用（AWS Marketplace 中所有 NetScaler VPX-AWS 订阅产品均可免费试用 21 天）。

部署选项

用户可以在 AWS 上部署 NetScaler VPX 独立实例。 有关详细信息，请参阅 在 AWS 上部署 NetScaler VPX 独立实例

用于混合云和多云部署的 NetScaler 全局负载平衡

NetScaler 混合云和多云全局服务器负载平衡 (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发应用程序流量。NetScaler 混合云和多云 GSLB 解决方案可帮助用户在混合云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，他们可以在完全迁移到云之前，使用 NetScaler 混合云和多云 GSLB 解决方案在云中测试其部分服务。例如，用户可以仅将一小部分流量路由到云，并在本地处理大部分流量。NetScaler 混合云和多云 GSLB 解决方案还使用户能够从单一的统一控制台管理和监控跨地理位置的 NetScaler 实例。

混合云和多云架构还可以通过避免“供应商锁定”并使用不同的基础设施来满足用户合作伙伴和客户的需求，从而提高整体企业绩效。借助多云架构，用户可以更好地管理其基础设施成本，因为他们现在只需按使用量付费。用户还可以更好地扩展其应用程序，因为他们现在按需使用基础设施。它还提供了快速从一个云切换到另一个云的能力，以利用每个提供商的最佳产品。

NetScaler 混合云和多云 GSLB 解决方案

NetScaler GSLB 节点处理 DNS 名称解析。任何这些 GSLB 节点都可以接收来自任何客户端位置的 DNS 请求。接收 DNS 请求的 GSLB 节点将返回由配置的负载平衡方法选择的负载平衡虚拟服务器 IP 地址。指标（站点、网络和持久性指标）通过指标交换协议 (MEP) 在 GSLB 节点之间交换，MEP 是一种专有的 NetScaler 协议。有关 MEP 协议的详细信息，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，GSLB 和 NetScaler 节点之间的指标通过 MEP 交换。但是，在父子拓扑中，在 GSLB 和 NetScaler LB 节点之间配置监视器探测是可选的。

NetScaler 代理可实现 NetScaler ADM 与用户数据中心中托管实例之间的通信。有关 NetScaler 代理及其安装方法的详细信息，请参阅 入门。

注意：

本文档作出以下假设：

- 如果用户有现有的负载平衡设置，则该设置已启动并正在运行。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在每个 NetScaler GSLB 节点上都配置了 SNIP 地址或 GSLB 站点 IP 地址。此 IP 地址在与其他数据中心交换指标时用作数据中心源 IP 地址。
- 在每个 NetScaler GSLB 实例上都配置了 ADNS 或 ADNS-TCP 服务以接收 DNS 流量。
- 所需的防火墙和安全组已在云服务提供商中配置。

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，并为 MEP 流量交换的 GSLB 站点 IP 地址打开端口 3009。在负载平衡节点上，用户必须打开适当的端口以接收应用程序流量。例如，用户必须打开端口 80 以接收 HTTP 流量，并打开端口 443 以接收 HTTPS 流量。打开端口 443 以用于 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 探测是使用其中一个 SNIP 启动的，因此必须为绑定到服务器端子网的安全组完成此设置。

NetScaler 混合云和多云 GSLB 解决方案的功能

本节介绍 NetScaler 混合云和多云 GSLB 解决方案的一些功能。

与其他负载平衡解决方案的兼容性

NetScaler 混合云和多云 GSLB 解决方案支持各种负载平衡解决方案，例如 NetScaler 负载平衡器、NGINX、HAProxy 和其他第三方负载平衡器。

注意：

除 NetScaler 之外的负载平衡解决方案仅在使用了基于邻近性和非基于度量的 GSLB 方法且未配置父子拓扑时才受支持。

GSLB 方法

NetScaler 混合云和多云 GSLB 解决方案支持以下 GSLB 方法。

- 基于度量的 GSLB 方法。基于度量的 GSLB 方法通过度量交换协议从其他 NetScaler 节点收集度量。
  - 最少连接：客户端请求被路由到活动连接最少的负载平衡器。
  - 最少带宽：客户端请求被路由到当前处理流量最少的负载平衡器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - 最少数据包：客户端请求被路由到在过去 14 秒内接收数据包最少的负载均衡器。

- 非基于度量的 GSLB 方法
  - 轮询：客户端请求被路由到负载均衡器列表中排在最前面的负载均衡器的 IP 地址。该负载均衡器随后会移动到列表的末尾。
  - 源 IP 哈希：此方法使用客户端 IP 地址的哈希值来选择负载均衡器。

- 基于邻近度的 GSLB 方法
  - 静态邻近度：客户端请求被路由到距离客户端 IP 地址最近的负载均衡器。
  - 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均衡器的 IP 地址。

有关负载均衡方法的更多信息，请参阅 负载均衡算法。

GSLB 拓扑

NetScaler 混合云和多云 GSLB 解决方案支持主动-被动拓扑和父子拓扑。

- 主动-被动拓扑 - 通过防止故障点来提供灾难恢复并确保应用程序的持续可用性。如果主数据中心发生故障，被动数据中心将投入运行。有关 GSLB 主动-被动拓扑的更多信息，请参阅配置 GSLB 以实现灾难恢复。
- 父子拓扑 – 如果客户使用基于度量的 GSLB 方法来配置 GSLB 和 LB 节点，并且 LB 节点部署在不同的 NetScaler 实例上，则可以使用此拓扑。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度量交换是通过度量交换协议 (MEP) 进行的。

有关父子拓扑的更多信息，请参阅使用 MEP 协议部署父子拓扑。

IPv6 支持

NetScaler 混合云和多云 GSLB 解决方案还支持 IPv6。

监控

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 配置在同一个 NetScaler 实例上，或者使用父子拓扑，则配置监视器是可选的。

持久性

NetScaler 混合云和多云 GSLB 解决方案支持以下功能：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 基于源 IP 的持久性会话，以便来自同一客户端的多个请求在配置的超时窗口内到达时被定向到同一服务。如果超时值在客户端发送另一个请求之前过期，则会话将被丢弃，并使用配置的负载平衡算法为客户端的下一个请求选择一个新服务器。
- 溢出持久性，以便备份虚拟服务器即使在主服务器上的负载低于阈值后，仍继续处理其接收到的请求。有关更多信息，请参阅配置溢出。
- 站点持久性，以便 GSLB 节点选择一个数据中心来处理客户端请求，并为所有后续 DNS 请求转发所选数据中心的 IP 地址。如果配置的持久性应用于处于 DOWN 状态的站点，则 GSLB 节点将使用 GSLB 方法选择一个新站点，并且新站点将对来自客户端的后续请求保持持久性。

使用 NetScaler ADM StyleBook 进行配置

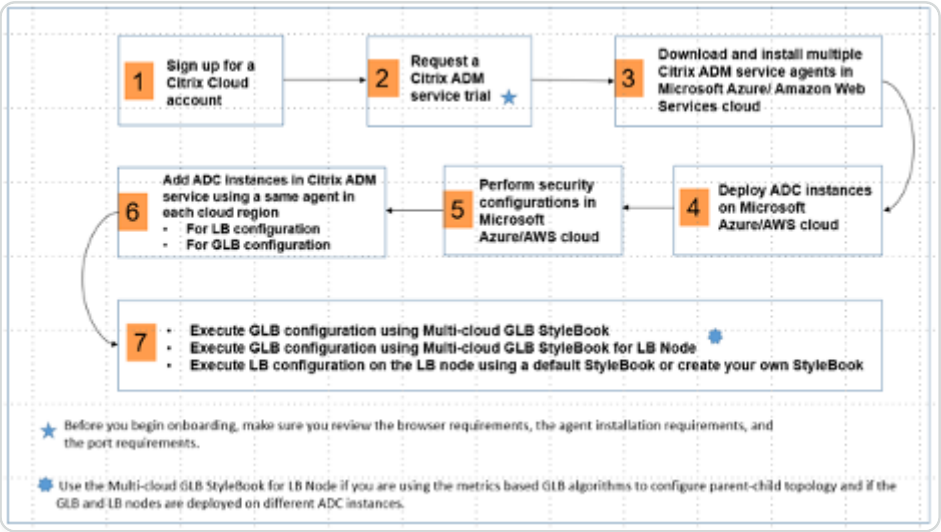
客户可以使用 NetScaler ADM 上的默认多云 GSLB StyleBook 来配置具有混合云和多云 GSLB 配置的 NetScaler 实例。

客户可以使用默认的多云 GSLB StyleBook 作为 LB 节点 StyleBook，来配置 NetScaler 负载平衡节点，这些节点是父子拓扑中的子站点，用于处理应用程序流量。仅当用户希望在父子拓扑中配置 LB 节点时才使用此 StyleBook。但是，每个 LB 节点都必须使用此 StyleBook 单独配置。

NetScaler 混合云和多云 GSLB 解决方案配置工作流

客户可以使用 NetScaler ADM 上随附的多云 GSLB StyleBook 来配置具有混合云和多云 GSLB 配置的 NetScaler 实例。

下图显示了配置 NetScaler 混合云和多云 GSLB 解决方案的工作流。工作流图中的步骤将在图后进行更详细的解释。



作为云管理员，执行以下任务：

1. 注册 NetScaler Cloud 帐户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要开始使用 NetScaler ADM，请创建 NetScaler Cloud 公司帐户或加入您公司中已有人创建的现有帐户。

2. 用户登录 NetScaler Cloud 后，单击 **NetScaler Application Delivery Management** 磁贴上的“**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。在每个区域安装一个代理，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。有关上述三项任务的更多信息，请参阅入门。
4. 在 Microsoft AWS 云/本地数据中心部署负载均衡器。

   根据用户在云和本地部署的负载均衡器类型，相应地进行预配。例如，用户可以在 Amazon Web Services (AWS) 虚拟私有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 实例的更多信息，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 实例是用户希望从 NetScaler ADM 发现、管理和监控的网络设备或虚拟设备。要管理和监控这些实例，用户必须将实例添加到服务并注册 LB（如果用户将 NetScaler 用于 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 StyleBook 实施 GSLB 和 LB 配置。

   - 使用 Multi-cloud GSLB StyleBook 在选定的 GSLB NetScaler 实例上执行 GSLB 配置。
   - 实施负载均衡配置。（如果用户已在托管实例上配置了负载均衡，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：
   - 手动配置实例以对应用程序进行负载均衡。有关如何手动配置实例的更多信息，请参阅 设置基本负载均衡。
   - 使用 StyleBooks。用户可以使用 NetScaler ADM StyleBooks 之一（HTTP/SSL 负载均衡 StyleBook 或 HTTP/SSL 负载均衡（带监视器）StyleBook）在选定的 NetScaler 实例上创建

© 1997–2026 Citrix Systems, Inc. All rights reserved.

负载均衡器配置。用户还可以创建自己的 StyleBooks。有关 StyleBooks 的更多信息，请参阅 StyleBooks。

8. 在以下任何情况下，使用 Multi-cloud GSLB StyleBook for LB Node 配置 GSLB 父子拓扑：
   - 如果用户正在使用基于指标的 GSLB 算法（最少数据包、最少连接、最少带宽）来配置 GSLB 和 LB 节点，并且 LB 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 LB 节点上配置 GSLB

如果客户正在使用基于指标的 GSLB 算法（最少数据包、最少连接、最少带宽）来配置 GSLB 和 LB 节点，并且 LB 节点部署在不同的 NetScaler 实例上，则可以使用 **Multi-cloud GSLB StyleBook for LB Node**。

用户还可以使用此 StyleBook 为现有父站点配置更多子站点。此 StyleBook 一次配置一个子站点。因此，请根据子站点的数量，从此 StyleBook 创建相应数量的配置（配置包）。此 StyleBook 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 Multi-cloud GSLB StyleBook 配置父站点。

此 StyleBook 做出以下假设：

- 已配置 SNIP 地址或 GSLB 站点 IP 地址。
- 已在云服务提供商中配置所需的防火墙和安全组。

使用用于 LB 节点的 Multi-cloud GSLB StyleBook 在父子拓扑中配置子站点

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**。

   StyleBook 显示为一个用户界面页面，用户可以在其中输入此 StyleBook 中定义的所有参数的值。

   > **注意：**
   >
   > 术语“数据中心”和“站点”在本文档中可互换使用。

3. 设置以下参数：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **应用程序名称**。输入部署在 GSLB 站点上且您要为其创建子站点的 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，选择用于检查表示站点上应用程序的负载均衡器 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，请输入当 VIP 运行状况良好时，HTTP 请求响应中预期的 HTTP 状态代码列表。

4. 配置父站点。

   - 提供您希望在其下创建子站点（LB 节点）的父站点（GSLB 节点）的详细信息。
     - **站点名称**。输入父站点的名称。
     - **站点 IP 地址**。输入父站点在与其他站点交换指标时用作其源 IP 地址的 IP 地址。此 IP 地址假定已在每个站点的 GSLB 节点上配置。
     - **站点公共 IP 地址**。（可选）如果父站点的 IP 地址经过 NAT 转换，请输入用于交换指标的父站点的公共 IP 地址。

5. 配置子站点。

   - 提供子站点的详细信息。
     - **站点名称**。输入站点的名称。
     - **站点 IP 地址**。输入子站点的 IP 地址。此处，使用配置为子站点的 NetScaler 节点的私有 IP 地址或 SNIP。
     - **站点公共 IP 地址**。（可选）如果子站点的 IP 地址经过 NAT 转换，请输入用于交换指标的子站点的公共 IP 地址。

6. 配置活动 GSLB 服务（可选）

   - 仅当 LB 虚拟服务器 IP 地址不是公共 IP 地址时，才配置活动 GSLB 服务。本节允许用户配置部署应用程序的站点上的本地 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。
     - **服务公共 IP 地址**。如果虚拟 IP 地址是私有的，并且已将其 NAT 转换为公共 IP 地址，请指定该公共 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **服务端口**。输入此站点上 GSLB 服务的端口。
- **站点名称**。输入 GSLB 服务所在的站点的名称。

7. 单击 **目标实例**，然后选择在每个站点上配置为 GSLB 实例的 NetScaler 实例，以部署 GSLB 配置。
8. 点击 **创建** 以在选定的 NetScaler 实例（LB 节点）上创建 LB 配置。用户还可以点击 **试运行** 以检查将在目标实例中创建的对象。用户创建的 StyleBook 配置会显示在“配置”页面上的配置列表中。用户可以使用 NetScaler ADM GUI 检查、更新或删除此配置。

CloudFormation 模板部署

NetScaler VPX 在 AWS Marketplace 中以 Amazon Machine Images (AMI) 的形式提供。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。Marketplace 中的每个 NetScaler VPX 版本都需要此步骤。

CloudFormation 存储库中的每个模板都附带了描述模板用法和架构的文档。这些模板旨在将 NetScaler VPX 的推荐部署架构编入代码，或向用户介绍 NetScaler，或演示特定功能、版本或选项。用户可以重用、修改或增强这些模板，以满足其特定的生产和测试需求。大多数模板除了创建 IAM 角色的权限外，还需要完整的 EC2 权限。

CloudFormation 模板包含特定于 NetScaler VPX 特定版本（例如，版本 12.0-56.20）和版本（例如，NetScaler VPX Platinum Edition - 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，用户需要编辑模板并替换 AMI ID。

最新的 NetScaler AWS-AMI-ID 位于此处：NetScaler AWS CloudFormation Master。

CFT 三网卡部署

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）。它部署一个 Internet 网关，并在公共子网上设置默认路由。此模板还在可用区之间创建了一个高可用性对，其中包含两个 NetScaler 实例：主实例上有 3 个 ENI 与 3 个 VPC 子网（管理、客户端、服务器）关联，辅助实例上有 3 个 ENI 与 3 个 VPC 子网（管理、客户端、服务器）关联。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 管理 GUI 的 HTTPS URL（使用自签名证书）
- PrimaryCitrixADCManagementURL2 - 主 VPX 管理 GUI 的 HTTP URL
- PrimaryCitrixADCInstanceID - 新创建的主 VPX 实例的实例 ID
- PrimaryCitrixADCPublicVIP - 与 VIP 关联的主 VPX 实例的弹性 IP 地址

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- PrimaryCitrixADCPrivateNSIP - 用于管理主 VPX 的私有 IP（NS IP）
- PrimaryCitrixADCPublicNSIP - 用于管理主 VPX 的公共 IP（NS IP）
- PrimaryCitrixADCPrivateVIP - 与 VIP 关联的主 VPX 实例的私有 IP 地址
- PrimaryCitrixADCSNIP - 与 SNIP 关联的主 VPX 实例的私有 IP 地址
- SecondaryCitrixADCManagementURL - 指向辅助 VPX 管理 GUI 的 HTTPS URL（使用自签名证书）
- SecondaryCitrixADCManagementURL2 - 指向辅助 VPX 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 的私有 IP (NS IP)
- SecondaryCitrixADCPublicNSIP - 用于管理辅助 VPX 的公共 IP (NS IP)
- SecondaryCitrixADCPrivateVIP - 与 VIP 关联的辅助 VPX 实例的私有 IP 地址
- SecondaryCitrixADCSNIP - 与 SNIP 关联的辅助 VPX 实例的私有 IP 地址
- SecurityGroup - VPX 所属的安全组 ID

向 CFT 提供输入时，CFT 中任何参数旁的 `*` 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，这超出了正常的 EC2 完全权限。此模板的用户还需要在使用此 CloudFormation 模板之前接受条款并订阅 AWS Marketplace 产品。

还应存在以下内容：

- 密钥对
- 3 个未分配的 EIP
- 主管理
- 客户端 VIP
- 辅助管理

有关在 AWS 上预置 NetScaler VPX 实例的更多信息，用户可以访问：在 AWS 上预置 NetScaler VPX 实例。

有关如何使用 StyleBook 配置 GSLB 的信息，请访问 使用 StyleBook 配置 GSLB

先决条件

在尝试在 AWS 中创建 VPX 实例之前，用户应确保具备以下条件：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 一个 AWS 账户，用于在 Amazon Web Services (AWS) 虚拟私有云 (VPC) 中启动 NetScaler VPX AMI。用户可以在 Amazon 免费创建 AWS 账户。
- 一个 AWS Identity and Access Management (IAM) 用户账户，用于安全地控制用户对 AWS 服务和资源的访问。有关如何创建 IAM 用户账户的更多信息，请参阅主题：创建 IAM 用户（控制台）。

对于独立部署和高可用性部署，IAM 角色都是强制性的。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
- ec2:DescribeAddresses
- ec2:AssociateAddress
- ec2:DisassociateAddress
- 自动扩缩:*
- 简单通知服务:*
- 简单队列服务:*
- iam:SimulatePrincipalPolicy
- iam:GetRole

如果使用 NetScaler CloudFormation 模板，IAM 角色会自动创建。该模板不允许选择已创建的 IAM 角色。

注意：

当用户通过 GUI 登录 VPX 实例时，会出现一个配置 IAM 角色所需权限的提示。如果权限已配置，请忽略该提示。

- 需要 AWS CLI 才能通过终端程序使用 AWS 管理控制台提供的所有功能。有关更多信息，请参阅 什么是 AWS 命令行界面？。用户还需要 AWS CLI 来将网络接口类型更改为 SR-IOV。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GSLB 先决条件

NetScaler GSLB 服务组的先决条件包括一个正常运行的 AWS 环境，并具备配置安全组、Linux Web 服务器、AWS 中的 NetScaler ADC、弹性 IP 和弹性负载均衡器的知识和能力。

GSLB DBS 服务集成要求 NetScaler 版本 12.0.57 支持 AWS ELB 负载均衡器实例。

有关当前支持的 VPX 型号和 AWS 区域、实例类型和服务的最新更新，请参阅 VPX-AWS 支持矩阵。

其他资源

适用于混合云和多云部署的 NetScaler ADM GSLB。

配置 NetScaler VPX 实例以使用 SR-IOV 网络接口

注意：

从 NetScaler 12.0 57.19 版本开始，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，除了 3G 和 5G 的 NetScaler VPX AWS Marketplace 版本，SR-IOV 在网络接口的默认配置中未启用。

在开始配置之前，请阅读以下主题：

- 先决条件
- 限制和使用指南

本节包括以下主题：

- 将接口类型更改为 SR-IOV
- 在高可用性设置上配置 SR-IOV

将接口类型更改为 SR-IOV

您可以运行 show interface summary 命令来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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> 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 的更多信息，请参阅 `<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sriov-networking.html>`

更改接口类型为 SR-IOV

1. 关闭在 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 \<instance\_id\> --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 \<instance\_id\> --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 SriovNetSupport 的值将缺失。

   示例 4： 在以下示例中，未启用 SR-IOV 支持。

```
{
    "InstanceId": "i-0c3e84cfa65b04cc8",
    "SriovNetSupport": {}
}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 启动 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： 以下屏幕截图显示了已启用 SR-IOV 的网络接口。接口 10/1、10/2、10/3 已启用 SR-IOV。

```
> show interface summary
--------------------------------------------------------------------------------
      Interface  MTU       MAC                Suffix
--------------------------------------------------------------------------------
1     10/1       1500      0a:1e:2e:17:a2:37  Intel 82599 10G VF Interface
2     10/2       1500      0a:df:17:0a:fe:83  Intel 82599 10G VF Interface
3     10/3       1500      0a:de:5d:31:bf:c3  Intel 82599 10G VF Interface
4     LO/1       1500      0a:1e:2e:17:a2:37  Netscaler Loopback interface
 Done
```

这些步骤完成了配置 VPX 实例以使用 SR-IOV 网络接口的过程。

在高可用性设置上配置 SR-IOV

从 NetScaler 12.0 版本 57.19 及更高版本开始，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 12.0 56.20 及更低版本的 Citrix CloudFormation 模板部署的，则附加到高可用性设置的 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
- 自动扩缩:*
- 简单通知服务:*
- sqs:所有
- IAM:SimulatePrincipalPolicy
- IAM:GetRole

默认情况下，适用于 NetScaler 12.0 57.19 版本的 Citrix CloudFormation 模板会自动将所需的权限添加到 IAM 角色。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

具有 SR-IOV 接口的高可用性设置大约需要 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。

配置 NetScaler VPX 实例以使用 AWS ENA 增强网络

在 AWS 上创建 NetScaler VPX 实例后，您可以使用 AWS CLI 配置虚拟设备以使用 增强网络 和 AWS 弹性网络适配器 (ENA)。

结合 AWS ENA，增强网络可提供更高的带宽、更高的每秒数据包 (PPS) 性能以及持续更低的实例间延迟。

在开始配置之前，请阅读以下主题：

- 先决条件
- 限制和使用指南

ENA 启用实例支持以下 HA 配置：

- 私有 IP 地址可以在同一可用区内移动。
- 弹性 IP 地址可以在可用区之间移动。

在 AWS 上升级 NetScaler VPX 实例

您可以升级在 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最大程度地减少停机时间。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

- NetScaler VPX AMI（包括实用程序许可证和客户许可证）的 NetScaler 软件版本 10.1.e-124.1308.e 或更高版本不支持 M1 和 M2 实例系列。
- 由于 VPX 实例支持的更改，不支持从 10.1.e-124 或更高版本降级到 10.1.123.x 或更早版本。
- 大多数升级不需要启动新的 AMI，并且可以在当前的 NetScaler AMI 实例上完成升级。如果您确实想升级到新的 NetScaler AMI 实例，请使用高可用性配置方法。

更改 AWS 上 NetScaler VPX 实例的 EC2 实例类型

如果您的 NetScaler VPX 实例运行的是 10.1.e-124.1308.e 或更高版本，您可以按如下方式从 AWS 控制台更改 EC2 实例类型：

1. 停止 VPX 实例。
2. 从 AWS 控制台更改 EC2 实例类型。
3. 启动实例。

您还可以使用上述过程更改早于 10.1.e-124.1308.e 版本的 EC2 实例类型，除非您想将实例类型更改为 M3。在这种情况下，您必须首先遵循标准的 NetScaler 升级过程，将 NetScaler 软件升级到 10.1.e-124 或更高版本，然后执行上述步骤。

升级 AWS 上 NetScaler VPX 实例的吞吐量或软件版本

要升级软件版本（例如，从 Standard 版升级到 Premium 版）或吞吐量（例如，从 200 Mbps 升级到 1000 Mbps），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，您可以从 Citrix® 网站购买并下载新许可证，然后将其安装到 VPX 实例上。有关从 Citrix 网站下载和安装许可证的更多信息，请参阅 VPX 许可指南。

使用实用程序许可证（按小时计费的实用程序许可证）

AWS 不支持对基于费用的实例进行直接升级。要升级基于费用的 NetScaler VPX 实例的软件版本或吞吐量，请启动具有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，如本页的 小节中所述。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

升级 AWS 上的 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。

如果您需要将运行早于 10.1.e-124.1308.e 版本的 VPX 实例升级到 10.1.e-124.1308.e 或更高版本，请首先升级系统软件，然后按如下方式将实例类型更改为 M3：

1. 停止 VPX 实例。
2. 从 AWS 控制台更改 EC2 实例类型。
3. 启动实例。

通过使用 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的 NetScaler AMI 实例，请执行以下任务：

- 从 AWS Marketplace 创建具有所需 EC2 实例类型、软件版本、吞吐量或软件版本的新实例。
- 在旧实例（待升级）和新实例之间配置高可用性。在旧实例和新实例之间配置高可用性后，旧实例的配置将同步到新实例。
- 强制将 HA 故障转移从旧实例转移到新实例。结果，新实例成为主实例并开始接收流量。
- 停止、重新配置或从 AWS 中移除旧实例。

先决条件和注意事项

- 确保您了解两个 NetScaler VPX 实例之间在高可用性方面的工作原理。有关两个 NetScaler VPX 实例之间高可用性配置的更多信息，请参阅在 AWS 上部署高可用性对。
- 您必须在新实例与旧实例相同的可用区中创建新实例，并具有完全相同的安全组和子网。
- 高可用性设置需要与用户 AWS Identity and Access Management (IAM) 账户关联的访问密钥和秘密密钥，这两个密钥都适用于这两个实例。如果在创建 VPX 实例时未使用正确的密钥信息，则 HA 设置将失败。有关为 VPX 实例创建 IAM 账户的更多信息，请参阅先决条件。
    - 您必须使用 EC2 控制台创建新实例。您不能使用 AWS 一键式启动，因为它不接受访问密钥和秘密密钥作为输入。
    - 新实例必须只有一个 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. 配置旧实例和新实例之间的高可用性。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下键入：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `add ha node <nodeID> <IPaddress of the node to be added>`
- `save config`

示例：

在旧实例的命令提示符下，键入：

```
add ha node 30 192.0.2.30

Done
```

在新实例的命令提示符下，键入：

```
add ha node 10 192.0.2.10

Done
```

请注意以下事项：

- 在 HA 设置中，旧实例是主节点，新实例是辅助节点。
- NSIP IP 地址不会从旧实例复制到新实例。因此，升级后，您的新实例将具有与之前实例不同的管理 IP 地址。
- HA 同步后，新实例的 `nsroot` 帐户密码将设置为旧实例的密码。

有关 AWS 上两个 NetScaler VPX 实例之间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 HA 故障转移。要在高可用性配置中强制执行故障转移，请在任一实例的命令提示符处键入：

```
force HA failover
```

强制执行故障转移后，旧实例的 ENI 将迁移到新实例，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。

如果出现以下警告消息，请键入 N 以中止操作：

```
[WARNING]:Force Failover may cause configuration loss, peer health not
optimum. Reason(s):
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
HA version mismatch

HA heartbeats not seen on some interfaces

Please confirm whether you want force-failover (Y/N)?
```

出现警告消息是因为两个 VPX 实例的系统软件不兼容 HA。因此，在强制故障转移期间，旧实例的配置无法自动同步到新实例。

以下是此问题的解决方法：

a. 在旧实例的 NetScaler shell 提示符处，键入以下命令以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 提示符处，键入以下命令以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. 在任一节点的命令提示符下，键入以下命令以强制进行故障转移，然后键入 Y 以确认警告消息以确认强制故障转移操作：

   - `force ha failover`

示例：

```
        > force ha failover



WARNING]:Force Failover may cause configuration loss, peer health not
optimum.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        Reason(s):

        HA version mismatch

        HA heartbeats not seen on some interfaces

        Please confirm whether you want force-failover (Y/N)? Y
```

3. 删除 HA 配置，以便这两个实例不再处于 HA 配置中。首先从辅助节点删除 HA 配置，然后从主节点删除 HA 配置。

   要在两个 NetScaler VPX 实例之间删除 HA 配置，请在每个实例的命令提示符下键入：

   ```
   > remove ha node \<nodeID\>

   >  save config
   ```

   有关 AWS 上两个 VPX 实例之间高可用性配置的更多信息，请参阅在 AWS 上部署高可用性对。

   示例：

在旧实例（新辅助节点）的命令提示符下，键入：

```
> remove ha node 30

  Done

> save config

  Done
```

在新实例（新主节点）的命令提示符下，键入：

```
> remove ha node 10

  Done

> save config
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

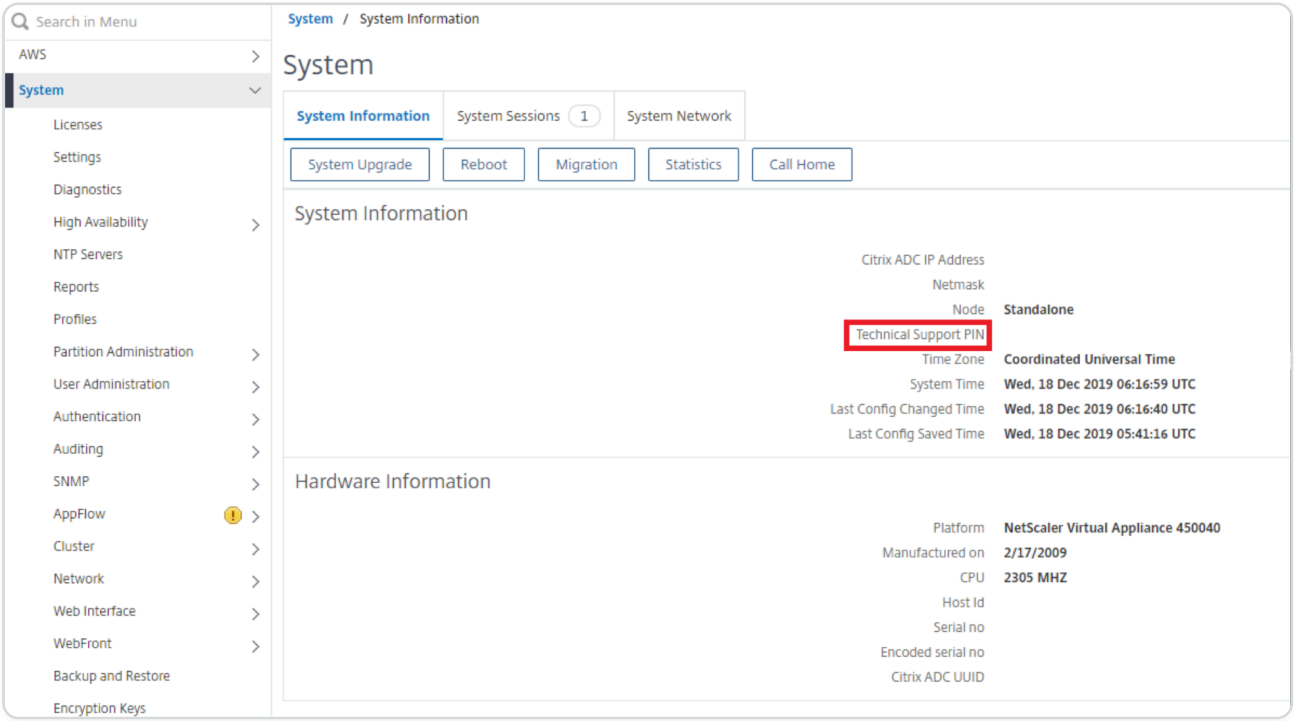
```
Done
```

在 AWS 上排查 VPX 实例故障

Amazon 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。只有在网络连接正常的情况下才能进行调试。要查看实例的系统日志，请右键单击该实例并选择“系统日志”。

NetScaler 为 AWS 上获得 AWS Marketplace 许可的 NetScaler VPX 实例（按小时收费的实用程序许可证）提供支持。要提交支持案例，请查找您的 AWS 账号和支持 PIN 码，然后致电 NetScaler 支持。您还需要提供您的姓名和电子邮件地址。要查找支持 PIN 码，请登录 VPX GUI 并导航到“系统”页面。

以下是显示支持 PIN 码的系统页面示例。



AWS 常见问题

- **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，因此它与任何实例都能无缝协作。有关加密卷的更多信息，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 实例的最佳方式是什么？**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以通过以下任一方式在 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 剧本
- AWS EC2 启动工作流

您可以根据所使用的自动化工具选择列出的任何选项。

有关这些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？**

  要在 AWS 中升级 NetScaler VPX 实例，您可以按照 (/zh-cn/vpx/13-1/deploy-aws/upgrade-vpx-aws.html) 中的步骤升级系统软件或升级到新的 NetScaler VPX Amazon Machine Image (AMI)。

  升级 NetScaler VPX 实例的推荐方法是按照 (/zh-cn/citrix-application-delivery-management-service/networks/configuration-jobs/how-to-upgrade-adc-instances.html) 中的步骤使用 ADM 服务。

- **NetScaler VPX 在 AWS 中的 HA 故障转移时间是多少？**

  - NetScaler VPX 在 AWS 可用区内的 HA 故障转移大约需要 3 秒。
  - NetScaler VPX 跨 AWS 可用区的 HA 故障转移大约需要 5 秒。

- **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，为提供技术支持 PIN 的客户提供“选择软件”服务。

- **在 (/zh-cn/vpx/13-1/deploy-aws/vpx-ha-eip-different-aws-zones.html) 部署中，我们需要为每个应用程序创建多个 IPSet 吗？**

  是的。如果存在多个应用程序，并且这些应用程序的多个 VIP 映射到多个 EIP，则需要多个 IPSet。因此，在 HA 故障转移期间，所有 EIP 的主 VIP 映射都会更改为辅助（新主）VIP。

- **为什么在跨不同区域的高可用性部署中启用 INC 模式？**

  跨可用区的 HA 对位于不同的网络中。对于 HA 同步，网络配置不得同步。这通过在 HA 对上启用 INC 模式来实现。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **如果 HA 节点与后端服务器位于同一 VPC 中的不同可用区，HA 节点可以与后端服务器通信吗？**

  是的，通过添加一个指向后端服务器子网的额外路由（通过 SNIP），同一 VPC 中不同可用区内的子网是可达的。例如，如果 AZ1 中 ADC 的 SNIP 子网是 192.168.3.0/24，并且 AZ2 中后端服务器子网是 192.168.6.0/24，则必须在 AZ1 中存在的 NetScaler 设备中添加路由 192.168.6.0 255.255.255.0 192.168.3.1。

- **(/zh-cn/vpx/13-1/deploy-aws/vpx-ha-eip-different-aws-zones.html) 和 (/zh-cn/vpx/13-1/deploy-aws/vpx-ha-pip-different-aws-zones.html) 部署可以协同工作吗？**

  是的，这两种配置都可以应用在同一个 HA 对上。

- **在 使用私有 IP 跨不同区域的高可用性 部署中，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在 HA 故障转移期间知道要检查的路由表？**

  辅助节点知道主 NIC 并搜索 VPC 中的所有路由表。

- **在使用 AWS 上的 VPX 默认映像时，`/var` 分区的大小是多少？如何增加磁盘空间？**

  根磁盘的大小限制为 20 GB，以保持磁盘映像较小。

  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，您必须附加一个额外的磁盘并在将关键内容复制到新磁盘后，创建指向 `/var` 的符号链接。

- **有多少个数据包引擎被激活并分配给 vCPU？**

  数据包引擎 (PE) 受限于许可的 vCPU 数量。NetScaler 守护程序不绑定到任何特定的 vCPU，并且可能在任何非 PE vCPU 上运行。根据 AWS，C5.9xlarge 是一个具有 36 个 vCPU 和 72 GB 内存的实例。通过池化许可，NetScaler VPX 实例部署时具有最大数量的 PE。在这种情况下，19 个 PE 在核心 1-19 上运行。但是，ADC 管理进程在 CPU 20-31 上运行。

- **如何为 ADC 选择合适的 AWS 实例？**

  a. 了解您的用例和要求，例如吞吐量、PPS、SSL 要求和平均数据包大小。

  b. 选择符合您要求的 ADC 产品和许可，例如 VPX 带宽产品或基于 vCPU 的许可。

  c. 根据所选产品，决定 AWS 实例。

  示例：

  5 Gbps 许可证可启用 5 个数据包引擎。因此，vCPU 要求为 6 (5 个用于数据包引擎，1 个用于管理)。但 6 vCPU 实例不可用。因此，只要您选择支持 5 Gbps 带宽的网络，8 vCPU 就足以达到该吞吐量。例如，对于 5 Gbps 带宽许可证，您必须选择 m5.2xlarge 才能为 5 Gbps 许可证启

© 1997–2026 Citrix Systems, Inc. All rights reserved.

用最大 PE 分配。但是，如果您使用不受吞吐量限制的 vCPU 许可证，则可以使用 m5.xlarge 实例本身获得 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

- **ADC 在 AWS 中是否必须采用三网卡三子网部署？**

  三网卡三子网是推荐的部署方式，其中每个网卡分别用于管理、客户端和服务器网络。这种部署方式提供了更好的流量隔离和 VPX 性能。两网卡两子网和一网卡一子网是其他可用选项。不建议在 AWS 中让多个网卡共享一个子网，例如两网卡一子网部署。这种情况可能导致网络问题，例如非对称路由。欲了解更多信息，请参阅 在 AWS 中配置网络接口的最佳实践。

- **为什么 AWS 上的 ENA 驱动程序总是显示 1Gbps (1/1) 的链路速度，而不管实例的网络功能如何？**

  AWS 弹性网络适配器 (ENA) 报告的速度通常显示为 1Gbps (1/1)，无论所选实例类型如何。这是因为所示速度并不直接反映实际网络性能。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，实际网络吞吐量会因具体的实例类型和当前网络负载而显著不同。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 Microsoft Azure 上部署 NetScaler VPX 实例

在 Microsoft Azure Resource Manager (ARM) 上部署 NetScaler VPX 实例时，您可以使用以下两种功能集来满足您的业务需求：

- Azure 云计算功能
- NetScaler 负载平衡和流量管理功能

您可以在 ARM 上部署 NetScaler VPX 实例，既可以作为独立实例，也可以作为主动-备用模式下的高可用性对。

您可以通过两种方式在 Microsoft Azure 上部署 NetScaler VPX 实例：

- 通过 Azure Marketplace。NetScaler VPX 虚拟设备在 Microsoft Azure Marketplace 中以映像形式提供。
- 使用 GitHub 上提供的 NetScaler Azure Resource Manager (ARM) JSON 模板。有关详细信息，请参阅NetScaler 解决方案模板的 GitHub 存储库。

Microsoft Azure Stack 是一个集成了硬件和软件的平台，可在本地数据中心提供 Microsoft Azure 公有云服务，从而使组织能够构建混合云。您现在可以在 Microsoft Azure Stack 上部署 NetScaler VPX 实例。

注意：

Azure 限制并阻止来自 Azure 外部的流量访问。要提供访问权限，请通过在连接到具有公共 IP 地址的虚拟机 (VM) 的 NIC 的网络安全组中添加入站规则来启用服务或端口。有关详细信息，请参阅 Azure 文档中关于 入站 NAT 规则 的内容。

先决条件

在 Azure 上部署 NetScaler VPX 实例之前，您需要具备一些先决知识。

- 熟悉 Azure 术语和网络详细信息。有关信息，请参阅 (/zh-cn/vpx/13-1/deploy-vpx-on-azure/azure-terminology.html) 。
- 了解 NetScaler 设备。有关 NetScaler 设备的详细信息，请参阅 (/zh-cn/citrix-adc/13-1.html) 。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 了解 NetScaler 网络。请参阅 (/zh-cn/citrix-adc/13-1/networking.html) 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：

- 称为 NSIP 地址的管理 IP 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，用于接受客户端请求

有关详细信息，请参阅 (/zh-cn/vpx/13-1/deploy-vpx-on-azure/network-architecture-vpx-azure.html)。

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核心和超过 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 数据表。

在 Azure 部署中，您可以通过三种方式在 Azure 上预置 NetScaler VPX 实例：

- 多 NIC 多 IP 架构
- 单 NIC 多 IP 架构
- 单 NIC 单 IP

根据您的需求，您可以使用任何这些受支持的架构类型。

多 NIC 多 IP 架构

在此部署类型中，您可以将多个网络接口 (NIC) 附加到 VPX 实例。任何 NIC 都可以具有一个或多个 IP 配置 - 分配给它的静态或动态公共和私有 IP 地址。

有关详细信息，请参阅以下用例：

- 配置具有多个 IP 地址和 NIC 的高可用性设置
- 使用 PowerShell 命令配置具有多个 IP 地址和 NIC 的高可用性设置

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

为避免 Azure 环境中的 MAC 移动和接口静默，我们建议您为 NetScaler VPX 实例的每个数据接口（无标签）创建一个 VLAN，并绑定 Azure 中 NIC 的主 IP。有关详细信息，请参阅 CTX224626 文章。

单 NIC 多 IP 架构

在此部署类型中，一个网络接口 (NIC) 与多个 IP 配置相关联 - 分配给它的静态或动态公共和私有 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，该地址用于执行 NSIP、SNIP 和 VIP 的功能。

有关详细信息，请参阅 配置 NetScaler VPX 独立实例。

注意：

单 IP 模式仅在 Azure 部署中可用。此模式不适用于本地、AWS 或其他部署类型的 NetScaler VPX 实例。

NetScaler VPX 许可

在 Azure 上运行的 NetScaler VPX 实例需要有效的许可证。适用于在 Azure 上运行的 NetScaler VPX 实例的许可选项包括：

- **自带许可证 (BYOL)**：要使用 BYOL 选项，请按照以下步骤操作：
  - 使用 NetScaler® 网站上的许可门户生成有效许可证。
  - 将生成的许可证上传到实例。
- **NetScaler VPX 签入和签出许可证**：此许可模型允许您从可用许可证池中签出许可证，并在不再需要时将其签回。有关更多信息和详细说明，请参阅 NetScaler VPX 签入和签出许可证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

- Azure 上的 NetScaler VPX 实例不再支持市场订阅许可。
- 在 NetScaler VPX 实例上进行任何配置更改之前，请执行热重启以启用正确的 NetScaler VPX 许可证。

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 NIC/2 NIC	VPX 3 NIC	VPX 最多 8 NIC
高达 200 Mbps	Standard_D2s_v5	Standard_D8s_v5	Standard_D16_v5
高达 1 Gbps	Standard_D4s_v5	Standard_D8s_v5	Standard_D16_v5
高达 5 Gbps	Standard_D8ds_v5	Standard_D8ds_v5	Standard_D16_v5
高达 10 Gbps	Standard_D8s_v5	Standard_D8s_v5	Standard_D16_v5

注意：

Microsoft Azure 网络适配器 (MANA) 在 NetScaler 13.1-59.x 及更高版本中受支持。有关详细信息，请参阅Microsoft 文档。

注意事项

- Azure 支持高达 10 Gbps 的 VPX 吞吐量。有关详细信息，请参阅NetScaler VPX 数据表。
- 为了在吞吐量超过 1 Gbps 的 NetScaler VPX 实例上实现最佳性能，您必须启用 Azure 加速网络。建议为此目的使用支持加速网络的 Azure 实例类型。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。
- 如果您预计可能随时需要关闭并临时解除分配 NetScaler VPX 虚拟机，请在创建虚拟机时分配一个静态内部 IP 地址。如果您不分配静态内部 IP 地址，Azure 可能会在每次虚拟机重新启动时为其分配不同的 IP 地址，从而导致虚拟机无法访问。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 对于 Citrix Virtual Apps and Desktops 部署，VPX 实例上的 VPN 虚拟服务器可以配置为以下模式：
  - 基本模式，其中 `ICAOnly` VPN 虚拟服务器参数设置为 ON。基本模式在未授权的 NetScaler VPX 实例上完全可用。
  - SmartAccess 模式，其中 `ICAOnly` VPN 虚拟服务器参数设置为 OFF。SmartAccess 模式在未授权的 NetScaler VPX 实例上仅支持五个 NetScaler AAA 会话用户。

注意：

要配置 SmartControl 功能，您必须为 NetScaler VPX 实例应用高级许可证。

Azure 中 NetScaler VPX 实例的 IPv6 支持

从版本 13.1-21.x 开始，NetScaler VPX 独立实例支持 Azure 中的 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？
- 在 Azure 虚拟网络中为 IPv4 应用程序添加 IPv6 - 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 后端自动扩缩。
- 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 架构不支持以下 NetScaler 功能：
  - 免费 ARP (GARP)
  - L2 模式
  - 标记 VLAN

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - 动态路由
  - 虚拟 MAC
  - USIP
  - 集群

- 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 事务数）可能会有所改善。
- Azure 在虚拟机预配期间生成的部署 ID 在 ARM 中对用户不可见。您不能使用此部署 ID 在 ARM 上部署 NetScaler VPX 设备。

Azure 术语

以下列出了 NetScaler VPX Azure 文档中使用的一些 Azure 术语。

1. Azure 负载均衡器 – Azure 负载均衡器是一种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的或面向 Internet 的，也可以是内部的。
2. Azure 资源管理器 (ARM) – ARM 是 Azure 中服务的新管理框架。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 – 这些是与虚拟机 NIC (NIC) 关联的 IP 地址，负载将分配到这些 NIC。
4. BLOB - 二进制大对象 – 可在 Azure 存储中存储的任何二进制对象，例如文件或图像。
5. 前端 IP 配置 – Azure 负载均衡器可以包含一个或多个前端 IP 地址，也称为虚拟 IP (VIP)。这些 IP 地址用作流量的入口。
6. 实例级公共 IP (ILPIP) – ILPIP 是一种公共 IP 地址，您可以直接将其分配给您的虚拟机或角色实例，而不是分配给您的虚拟机或角色实例所在的云服务。这不会取代分配给您的云服务的 VIP（虚拟 IP）。相反，它是一个额外的 IP 地址，您可以使用它直接连接到您的虚拟机或角色实例。

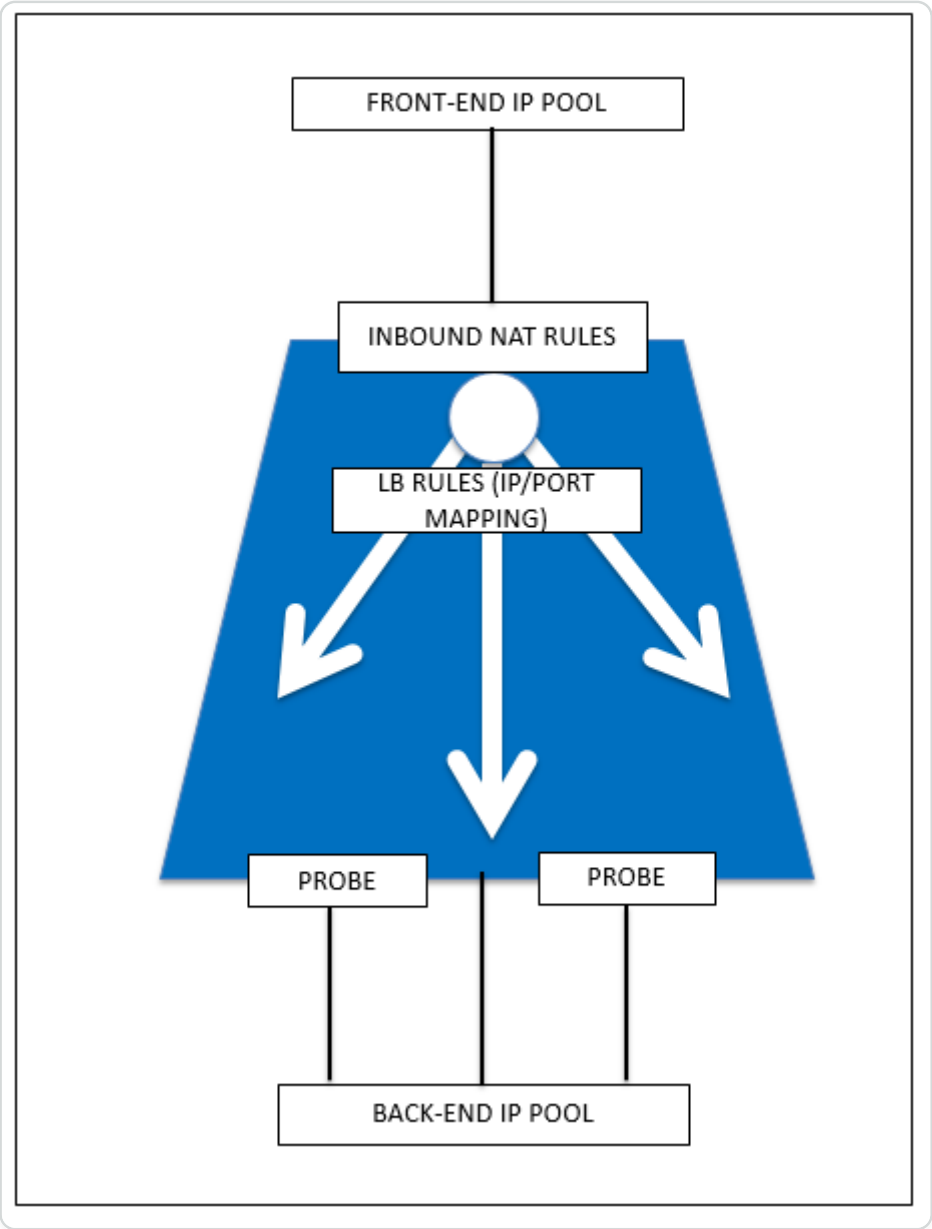
   注意：

   过去，ILPIP 被称为 PIP，即公共 IP。

7. 入站 NAT 规则 – 这包含将负载均衡器上的公共端口映射到后端地址池中特定虚拟机的端口的规则。
8. IP 配置 - 它可以定义为与单个 NIC 关联的 IP 地址对（公共 IP 和私有 IP）。在 IP 配置中，公共 IP 地址可以为 NULL。每个 NIC 可以关联多个 IP 配置，最多可达 255 个。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. 负载均衡规则 – 一种规则属性，将给定的前端 IP 和端口组合映射到一组后端 IP 地址和端口组合。通过负载均衡器资源的单个定义，您可以定义多个负载均衡规则，每个规则都反映了与虚拟机关联的前端 IP 和端口以及后端 IP 和端口的组合。



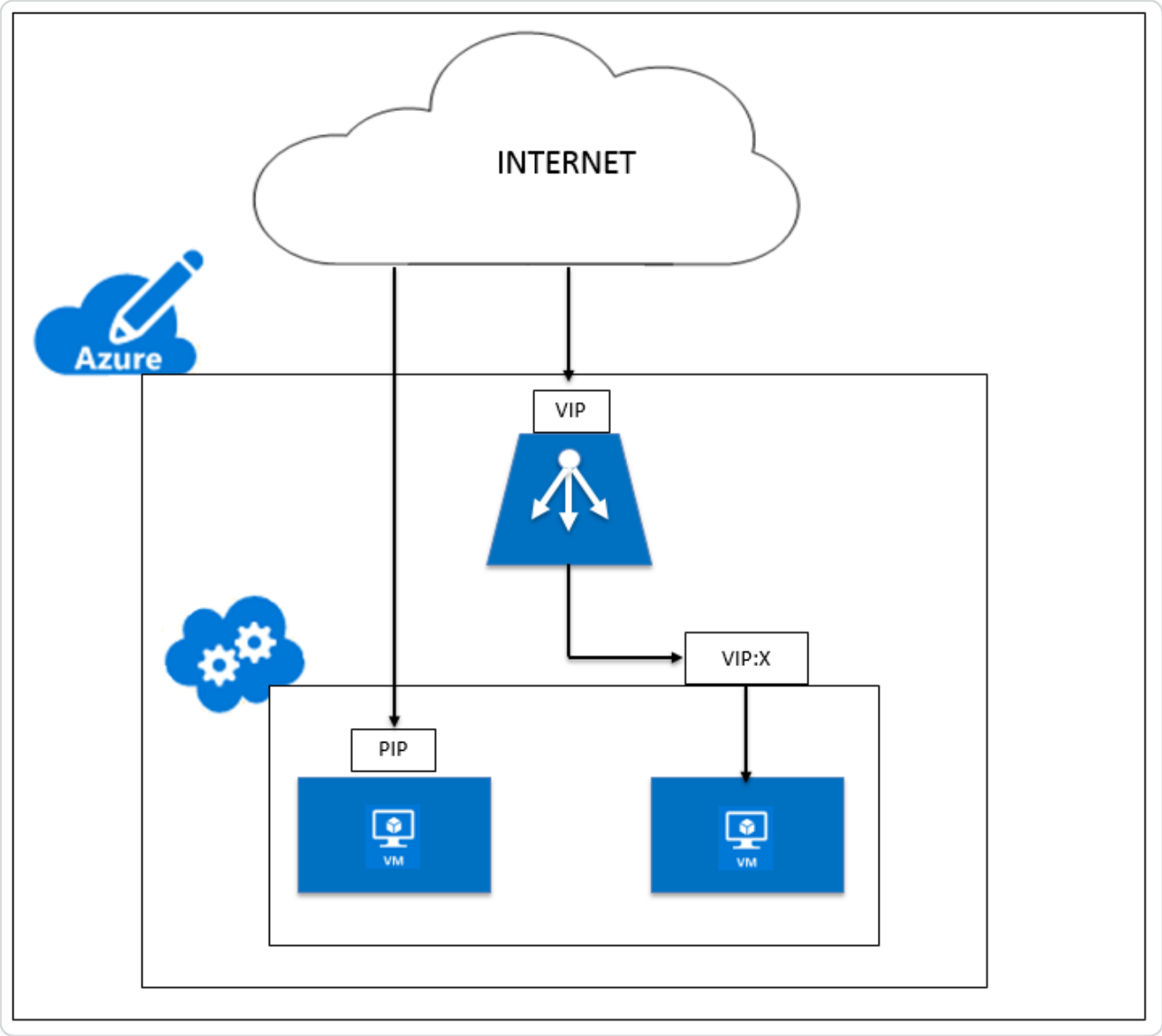
10. 网络安全组 – 包含一个访问控制列表 (ACL) 规则列表，这些规则允许或拒绝虚拟网络中虚拟机实例的网络流量。NSG 可以与子网或该子网内的单个虚拟机实例关联。当网络安全组与子网关联时，ACL 规则适用于该子网中的所有虚拟机实例。此外，通过将网络安全组直接关联到单个虚拟机，可以进一步限制流向该虚拟机的流量。

11. 私有 IP 地址 – 用于 Azure 虚拟网络内部通信，以及当您使用 VPN 网关将网络扩展到 Azure 时，用于您的本地网络通信。私有 IP 地址允许 Azure 资源通过 VPN 网关或 ExpressRoute 线路与虚拟网络或本地网络中的其他资源进行通信，而无需使用可通过 Internet 访问的 IP 地址。在 Azure Resource Manager 部署模型中，私有 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. 探测 – 这包含用于检查后端地址池中虚拟机实例可用性的运行状况探测。如果某个虚拟机在一段时间内未响应运行状况探测，则会将其从流量服务中移除。探测使您能够跟踪虚拟实例的运行状况。如果运行状况探测失败，虚拟实例将自动从轮换中移除。
13. 公共 IP 地址 (PIP) – PIP 用于与 Internet 通信，包括 Azure 面向公众的服务，并与虚拟机、面向 Internet 的负载均衡器、VPN 网关和应用程序网关相关联。
14. 区域 - 地理区域内不跨越国界且包含一个或多个数据中心的区域。定价、区域服务和产品类型在区域级别公开。一个区域通常与另一个区域配对，后者可能相距数百英里，以形成区域对。区域对可用作灾难恢复和高可用性场景的机制。通常也称为位置。
15. 资源组 - Resource Manager 中的容器，用于存放应用程序的相关资源。资源组可以包含应用程序的所有资源，或者只包含那些逻辑上分组在一起的资源。
16. 存储帐户 – Azure 存储帐户使您能够访问 Azure 存储中的 Azure Blob、队列、表和文件服务。您的存储帐户为您的 Azure 存储数据对象提供唯一的命名空间。
17. 虚拟机 – 运行操作系统的物理计算机的软件实现。多台虚拟机可以在同一硬件上同时运行。在 Azure 中，虚拟机有多种大小可供选择。
18. 虚拟网络 - Azure 虚拟网络是您在云中自有网络的表示。它是专用于您的订阅的 Azure 云的逻辑隔离。您可以在此网络中完全控制 IP 地址块、DNS 设置、安全策略和路由表。您还可以将 VNet 进一步细分为子网，并启动 Azure IaaS 虚拟机和云服务（PaaS 角色实例）。此外，您可以使用 Azure 中可用的连接选项之一将虚拟网络连接到您的本地网络。本质上，您可以将网络扩展到 Azure，完全控制 IP 地址块，并受益于 Azure 提供的企业级规模。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Microsoft Azure 上 NetScaler VPX 实例的网络架构

在 Azure Resource Manager (ARM) 中，NetScaler VPX 虚拟机 (VM) 驻留在虚拟网络中。可以在虚拟网络的给定子网中创建单个网络接口，并将其附加到 VPX 实例。您可以使用网络安全组筛选 Azure 虚拟网络中 VPX 实例的入站和出站网络流量。网络安全组包含安全规则，这些规则允许或拒绝 VPX 实例的入站或出站网络流量。有关详细信息，请参阅 安全组。

网络安全组筛选发往 NetScaler VPX 实例的请求，VPX 实例将这些请求发送到服务器。来自服务器的响应沿相同的路径反向返回。网络安全组可以配置为筛选单个 VPX VM，或者通过子网和虚拟网络，可以在部署多个 VPX 实例时筛选流量。

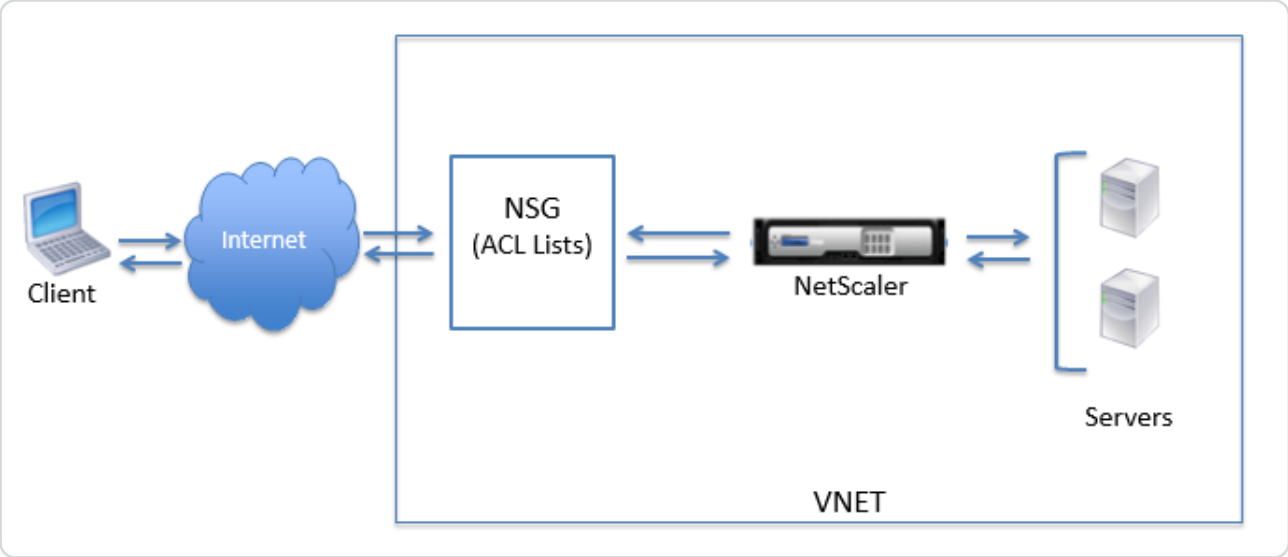
NIC 包含网络配置详细信息，例如虚拟网络、子网、内部 IP 地址和公共 IP 地址。

在 ARM 上，最好了解以下用于访问部署了单个 NIC 和单个 IP 地址的 VM 的 IP 地址：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 公共 IP (PIP) 地址是直接在 NetScaler® VM 的虚拟 NIC 上配置的面向 Internet 的 IP 地址。这允许您从外部网络直接访问 VM。
- NetScaler IP（也称为 NSIP）地址是 VM 上配置的内部 IP 地址。它不可路由。
- 虚拟 IP 地址 (VIP) 是通过使用 NSIP 和端口号配置的。客户端通过 PIP 地址访问 NetScaler 服务，当请求到达 NetScaler VPX™ VM 的 NIC 或 Azure 负载均衡器时，VIP 会转换为内部 IP (NSIP) 和内部端口号。
- 内部 IP 地址是 VM 从虚拟网络地址空间池获取的专用内部 IP 地址。此 IP 地址无法从外部网络访问。此 IP 地址默认为动态，除非您将其设置为静态。来自 Internet 的流量根据网络安全组上创建的规则路由到此地址。网络安全组与 NIC 集成，以选择性地将正确类型的流量发送到 NIC 上的正确端口，这取决于 VM 上配置的服务。

下图显示了流量如何通过在 ARM 中预置的 NetScaler VPX 实例从客户端流向服务器。

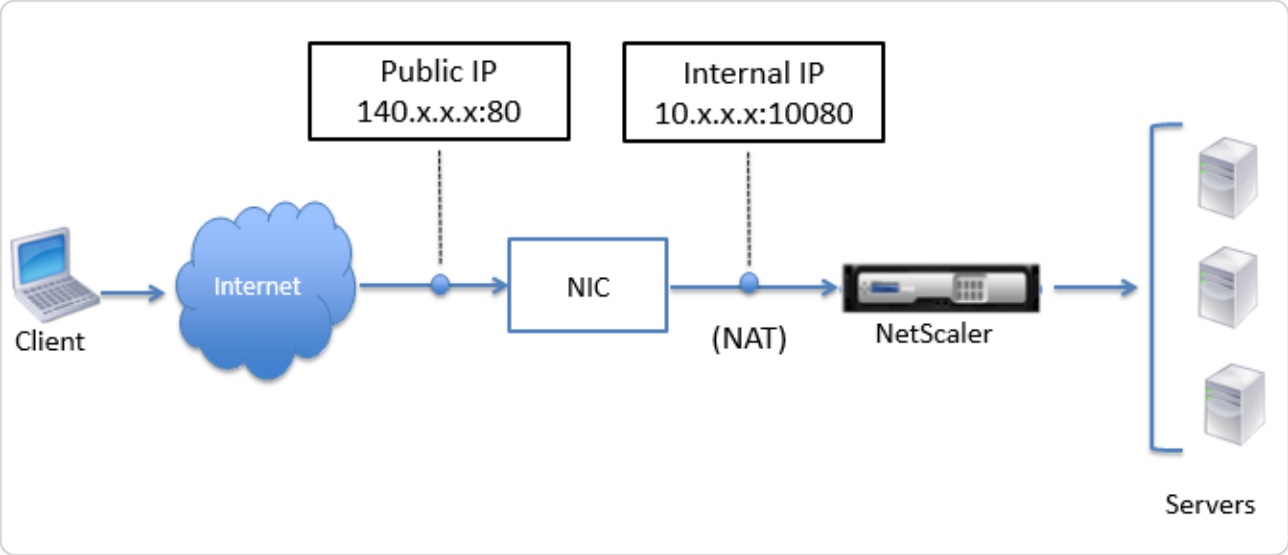


通过网络地址转换的流量流

您还可以为 NetScaler VPX 实例（实例级别）请求公共 IP (PIP) 地址。如果您在 VM 级别使用此直接 PIP，则无需定义入站和出站规则来拦截网络流量。来自 Internet 的入站请求直接在 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在此示例中，分配给网络安全组的公共 IP 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，公共 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 实例侦听的端口。客户端请求在公共 IP 地址 (140.x.x.x) 上接收。Azure 执行网络地址转换，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：

高可用性中的 NetScaler VPX VM 由外部或内部负载均衡器控制，这些负载均衡器上定义了入站规则以控制负载均衡流量。外部流量首先由这些负载均衡器拦截，然后根据配置的负载均衡规则进行分流，这些规则在负载均衡器上定义了后端池、NAT 规则和健康探测。

端口使用指南

您可以在创建 NetScaler VPX 实例时或在虚拟机预配后，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共端口和一个私有端口相关联。

在配置网络安全组规则之前，请注意以下有关可使用的端口号的指南：

1. NetScaler VPX 实例保留以下端口。当使用公共 IP 地址处理来自互联网的请求时，您不能将这些端口定义为私有端口。

   端口 21、22、80、443、8080、67、161、179、500、520、3003、3008、3009、3010、3011、4001、5061、9000、7000。

   但是，如果您希望面向互联网的服务（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，标准端口将映射到在 NetScaler 上为该 VIP 服务配置的另一个端口。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

例如，VIP 服务可能在 VPX 实例上的端口 8443 上运行，但被映射到公共端口 443。因此，当用户通过公共 IP 访问端口 443 时，请求将被定向到私有端口 8443。

2. 公共 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 实例关联的公共 IP 地址 (PIP) 的流量，而不是在 Azure 负载均衡器上配置的 PIP。

注意：

在 Azure 资源管理器中，NetScaler VPX 实例与两个 IP 地址相关联——一个公共 IP 地址 (PIP) 和一个内部 IP 地址。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。不要使用 PIP 配置 VIP。

配置 NetScaler VPX 独立实例

您可以通过创建虚拟机和配置其他资源，在 Azure Resource Manager (ARM) 门户中以独立模式预配单个 NetScaler VPX 实例。

开始之前

确保您具备以下条件：

- Microsoft Azure 用户帐户
- 访问微软 Azure 资源管理器
- 微软 Azure SDK
- 微软蔚蓝命令行管理程序

在 Microsoft Azure Portal 页面上，通过提供您的用户名和密码登录到 Azure Resource Manager 门户。

注意：

在 ARM 门户中，单击一个窗格中的选项会在右侧打开一个新窗格。从一个窗格导航到另一个窗格以配置您的设备。

配置步骤摘要

1. 配置资源组
2. 配置网络安全组

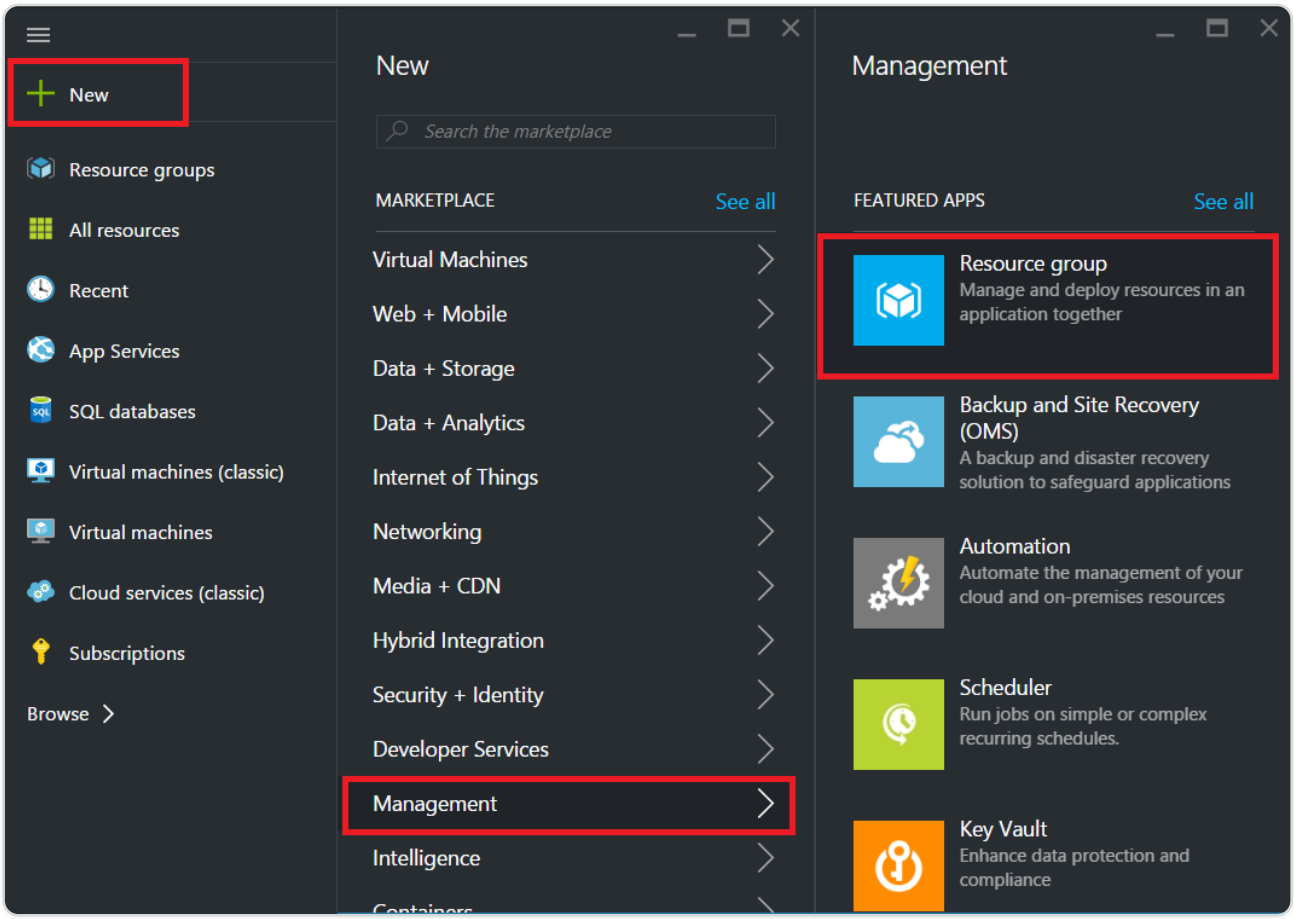
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 配置虚拟网络及其子网
4. 配置存储账户
5. 配置可用性集
6. 配置 NetScaler VPX 实例。

配置资源组

创建一个新的资源组，作为所有资源的容器。使用该资源组来部署、管理和监控您的资源。

1. 单击 **新建** > **管理** > **资源组**。
2. 在 **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

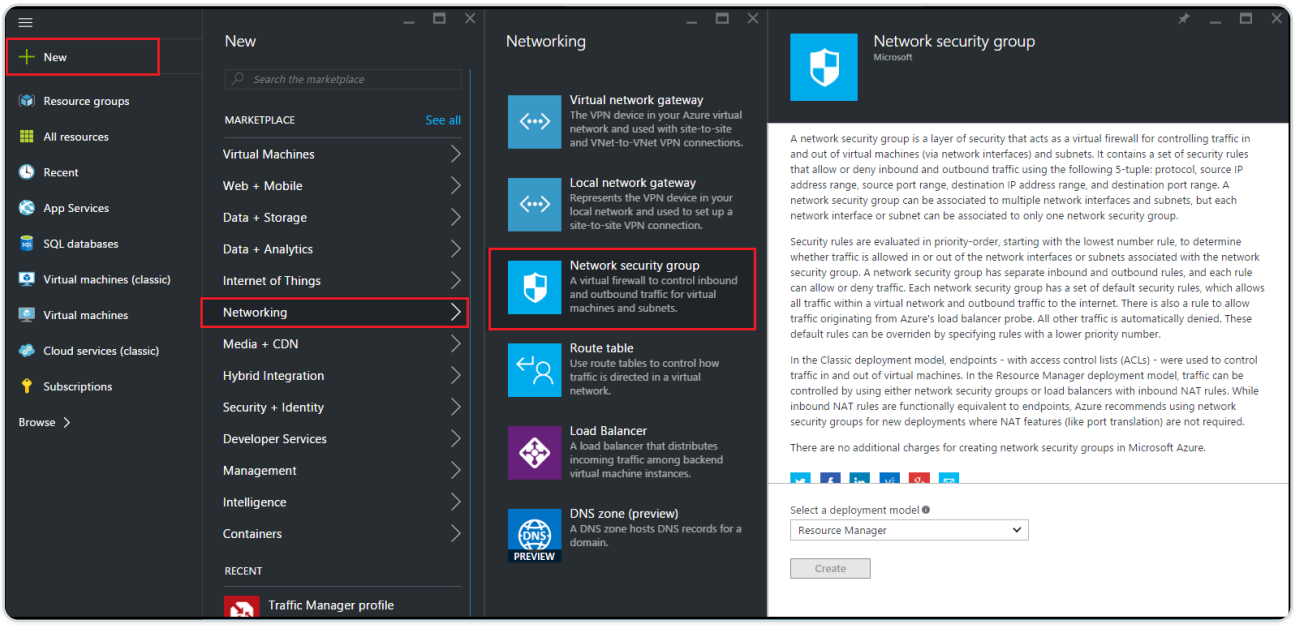
创建一个网络安全组，用于分配入站和出站规则，以控制虚拟网络中的传入和传出流量。网络安全组允许您为单个虚拟机定义安全规则，也可以为虚拟网络子网定义安全规则。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 单击 **新建** > **网络** > **网络安全组**。
2. 在 **创建网络安全组** 窗格中，输入以下详细信息，然后单击 **创建**。
   - 名称 - 输入安全组的名称
   - 资源组 - 从下拉列表中选择资源组

注意：

确保您已选择正确的位置。下拉列表中显示的资源列表因位置而异。



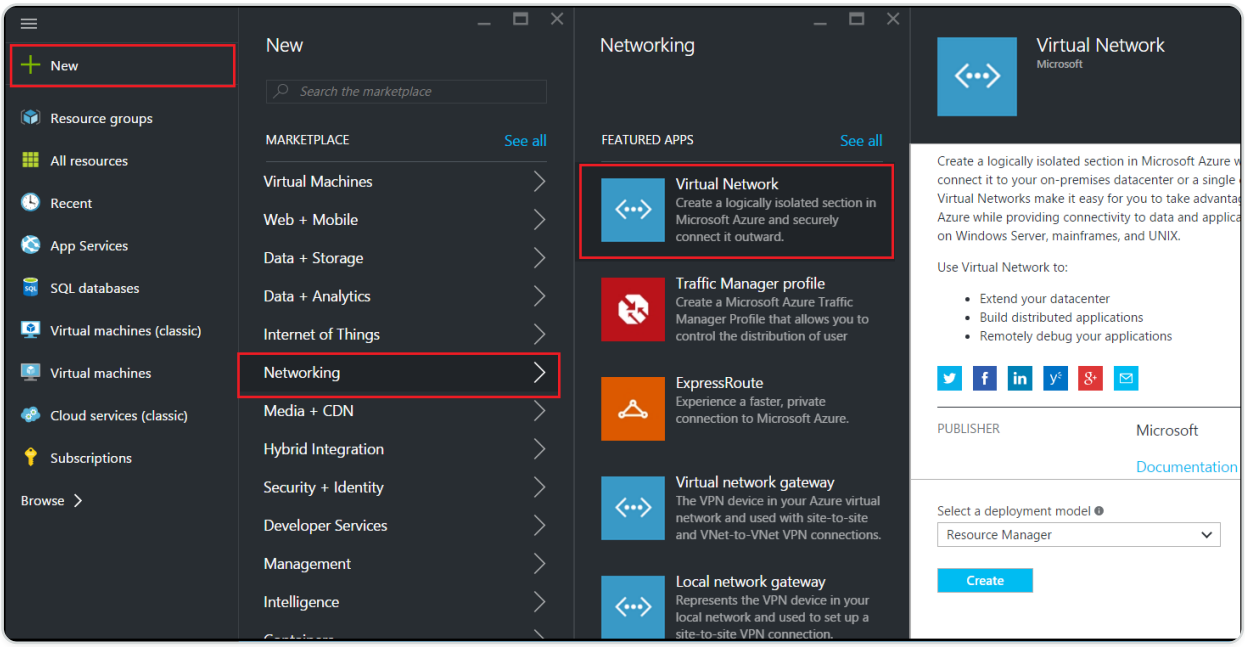
配置虚拟网络和子网

ARM 中的虚拟网络为您的服务提供了一层安全性和隔离。属于同一虚拟网络的 VM 和服务可以相互访问。

请按照以下步骤创建虚拟网络和子网。

1. 单击 **新建** > **网络** > **虚拟网络**。
2. 在“**虚拟网络**”窗格中，确保部署模式为“**资源管理器**”，然后单击“**创建**”。

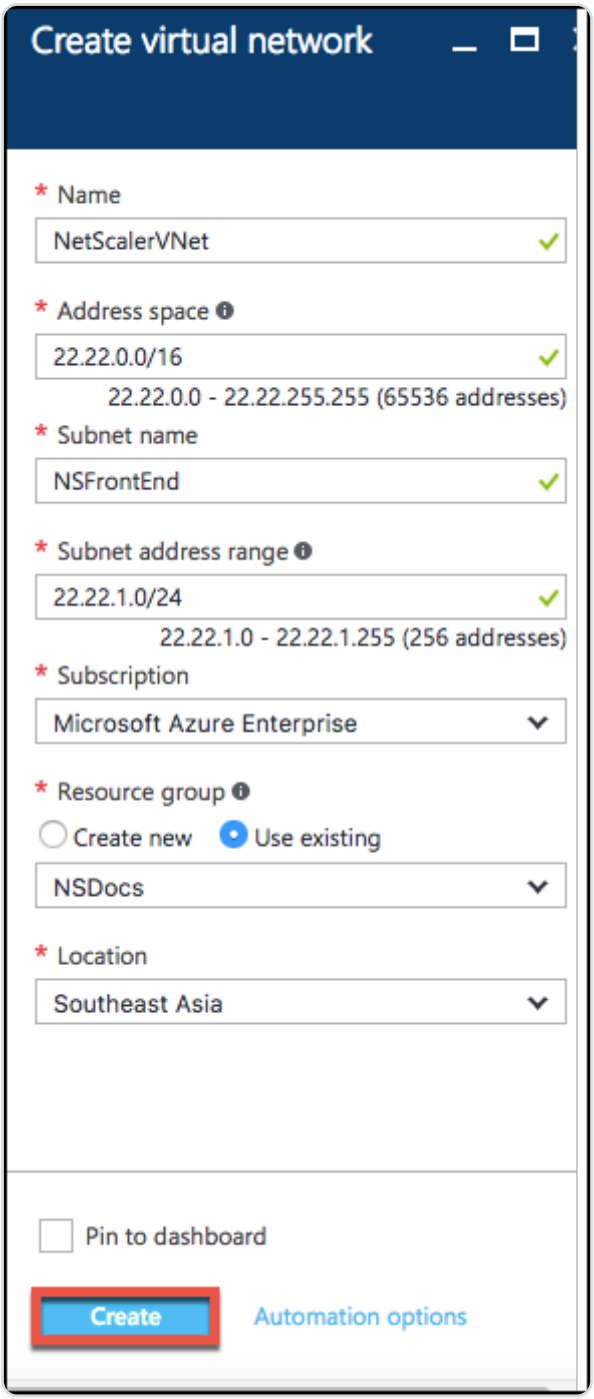
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 在“**创建虚拟网络**”窗格中，输入以下值，然后单击“**创建**”。

   - 虚拟网络的名称
   - 地址空间 - 输入虚拟网络的保留 IP 地址块
   - 子网 - 输入第一个子网的名称（您将在本步骤稍后创建第二个子网）
   - 子网地址范围 - 键入子网的保留 IP 地址块
   - 资源组 - 从下拉列表中选择之前创建的资源组

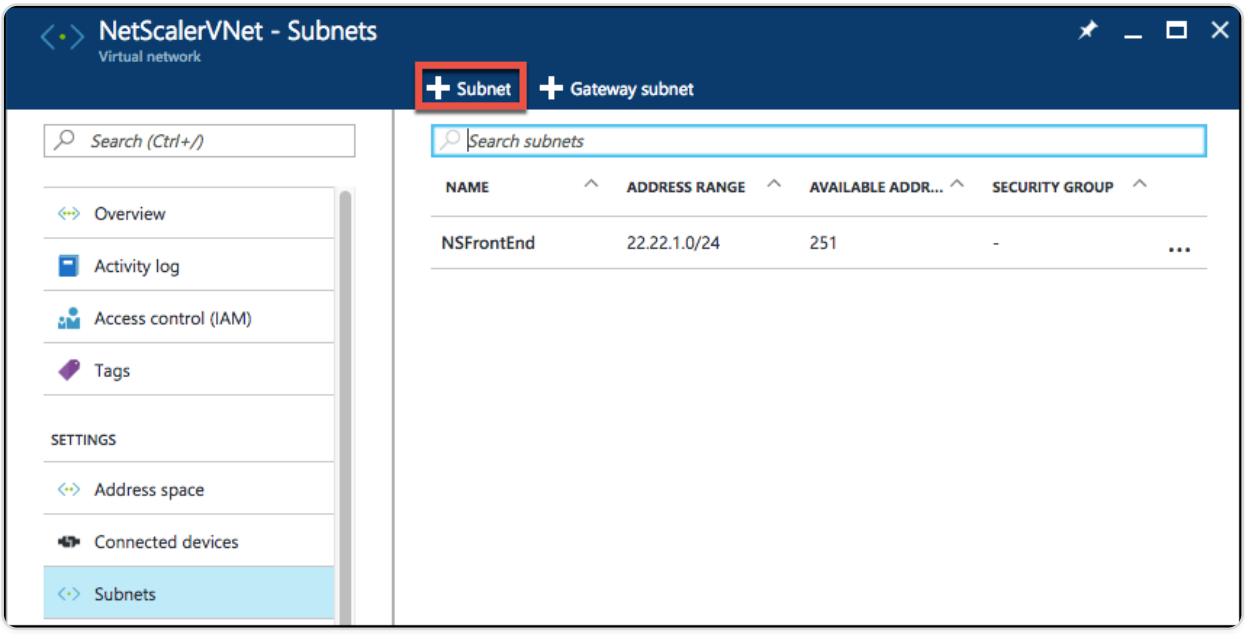
© 1997–2026 Citrix Systems, Inc. All rights reserved.



配置第二个子网

1. 从**所有资源**窗格中选择新创建的虚拟网络，并在**设置**窗格中，单击**子网**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

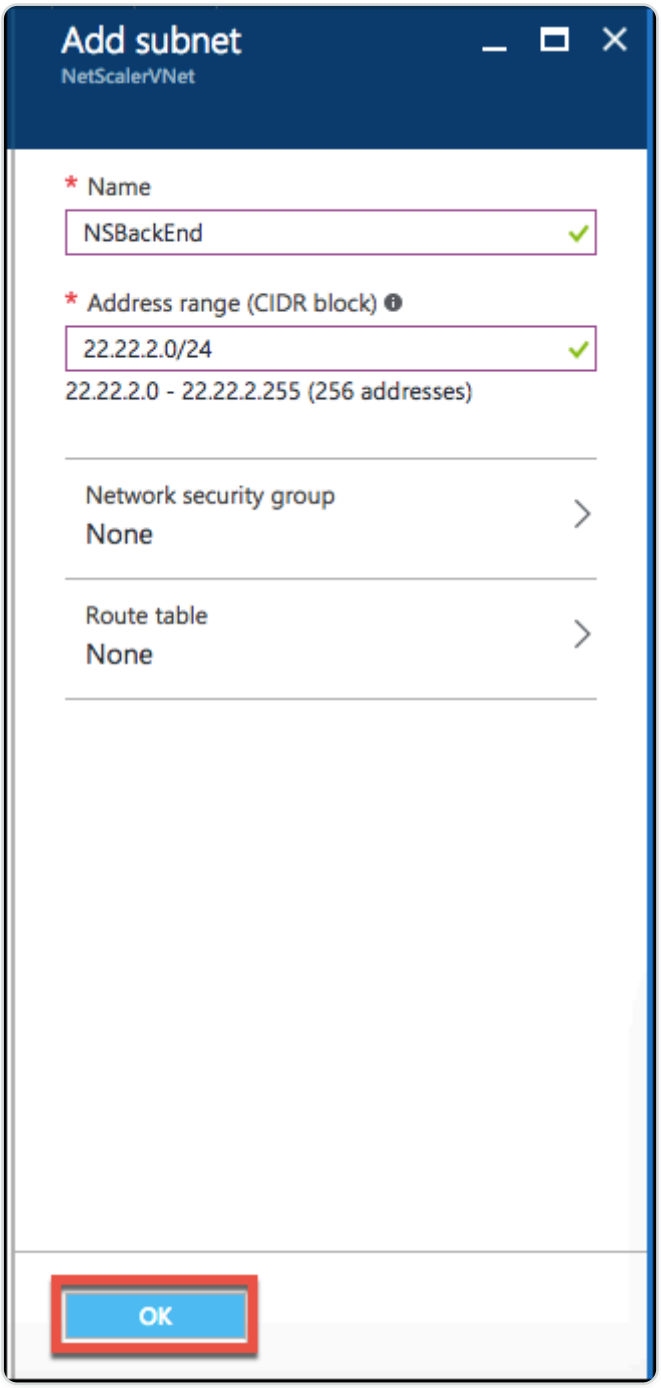


2. 单击**+子网**，并通过输入以下详细信息创建第二个子网。

   - 第二个子网的名称
   - 地址范围 - 键入第二个子网的保留 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**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



配置存储帐户

ARM IaaS 基础架构存储包括所有可以以 blob、表、队列和文件形式存储数据的服务。您还可以使用 ARM 中的这些存储数据形式创建应用程序。

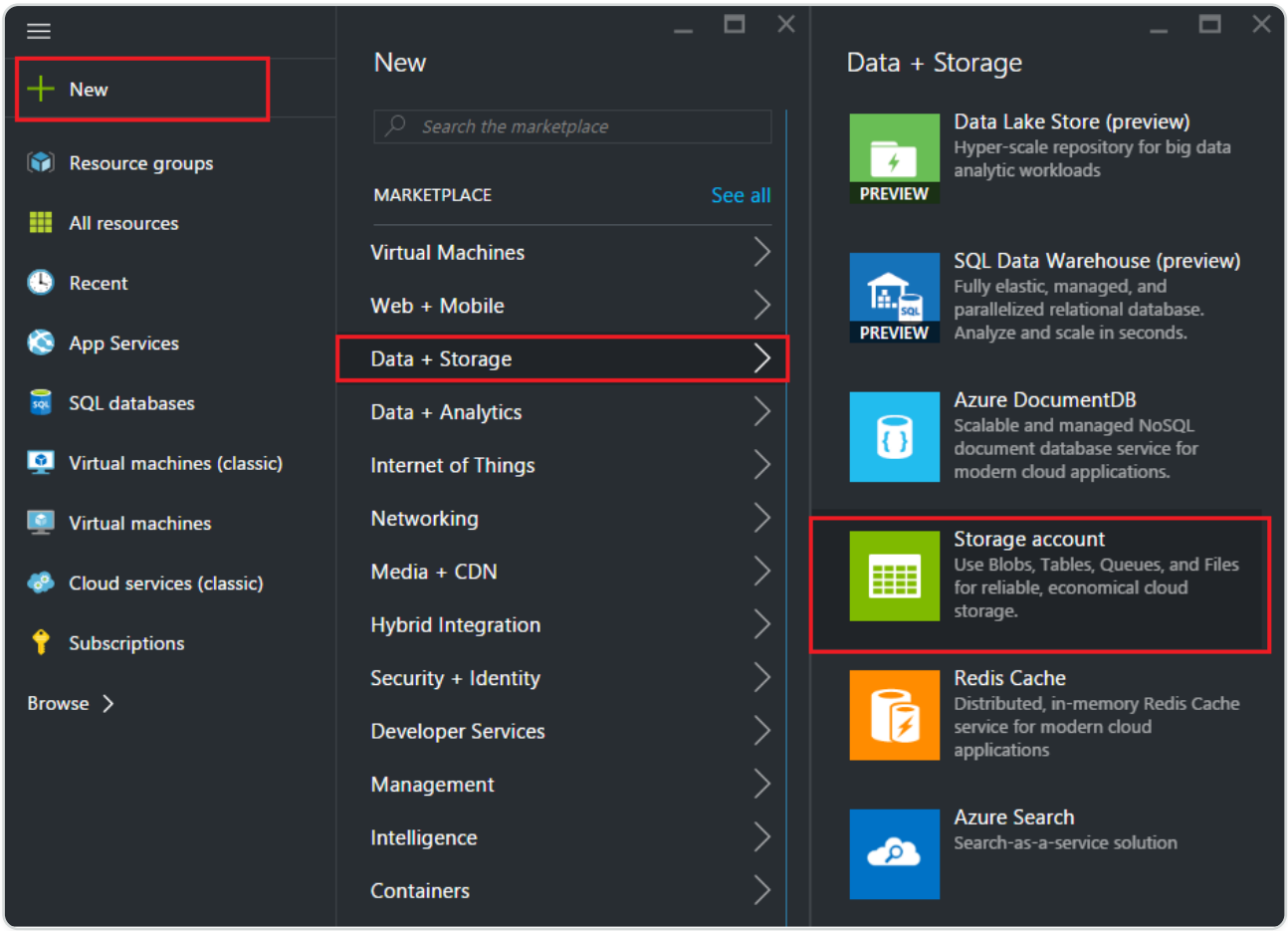
创建存储帐户以存储所有数据。

1. 单击 **+新建** > **数据 + 存储** > **存储帐户**。
2. 在“**创建存储帐户**”窗格中，输入以下详细信息：
   - 帐户名称

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 部署模式 - 请务必选择 **资源管理器**
- 帐户类型 - 从下拉列表中选择 **通用**
- 复制 - 从下拉列表中选择 **本地冗余存储**
- 资源组 - 从下拉列表中选择新创建的资源组

3. 单击 **创建**。

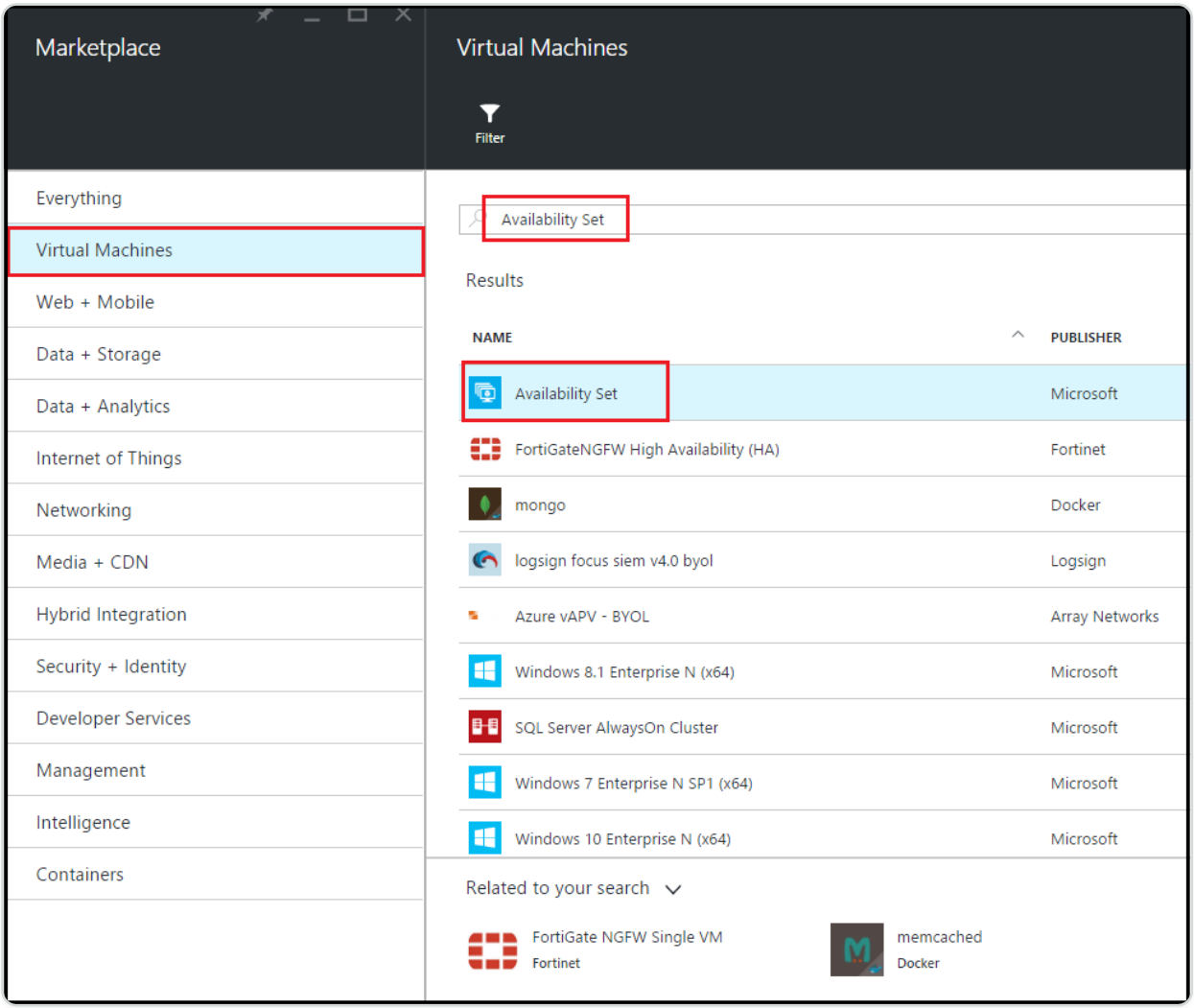


配置可用性集

可用性集可确保在计划内或计划外维护期间至少有一台 VM 保持运行。同一“可用性集”下的两台或更多 VM 放置在不同的故障域中，以实现冗余服务。

1. 单击 **+新建**。
2. 在 MARKETPLACE 窗格中单击 **查看全部**，然后单击 **虚拟机**。
3. 搜索可用性集，然后从显示的列表中选择 **可用性集** 实体。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 点击“**创建**”，并在“**创建可用性集**”窗格中，输入以下详细信息：

   - 集的名称
   - 资源组 - 从下拉列表中选择新创建的资源组

5. 点击“**创建**”。

   可用配置集(/en-us/vpx/media/config-avail-set-2.png)

配置 NetScaler VPX 实例

在虚拟网络中创建 NetScaler VPX 实例。从 Azure Marketplace 获取 NetScaler VPX 映像，然后使用 Azure 资源管理器门户创建 NetScaler VPX 实例。

在开始创建 NetScaler VPX 实例之前，请确保已创建包含实例所需子网的虚拟网络。您可以在 VM 预配期间创建虚拟网络，但无法灵活创建不同的子网。

（可选）配置 DNS 服务器和 VPN 连接，以允许虚拟机访问 Internet 资源。

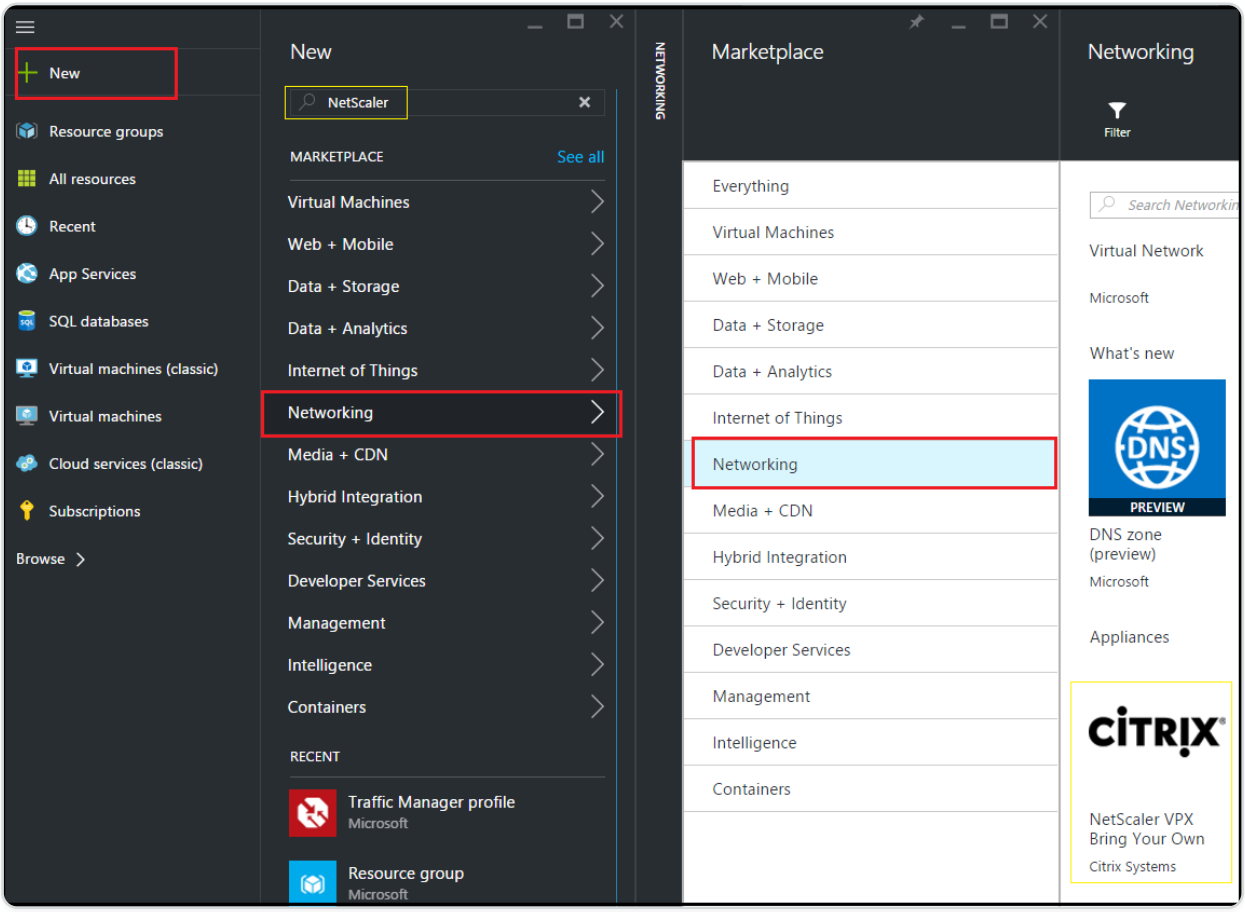
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

Citrix 建议您在预配 NetScaler VPX VM 之前创建资源组、网络安全组、虚拟网络和其他实体，以便在预配期间提供网络信息。

1. 点击“**+新建**” \> “**网络**”。
2. 点击“**查看全部**”，并在“网络”窗格中，点击“**NetScaler 13.0**”。
3. 从软件计划列表中选择“**NetScaler 13.0 VPX 自带许可证**”。

   作为在 ARM 门户上查找任何实体的快捷方式，您还可以在 Azure Marketplace 搜索框中键入实体名称，然后按 \<Enter\>。在搜索框中键入 NetScaler 以查找 NetScaler 映像。

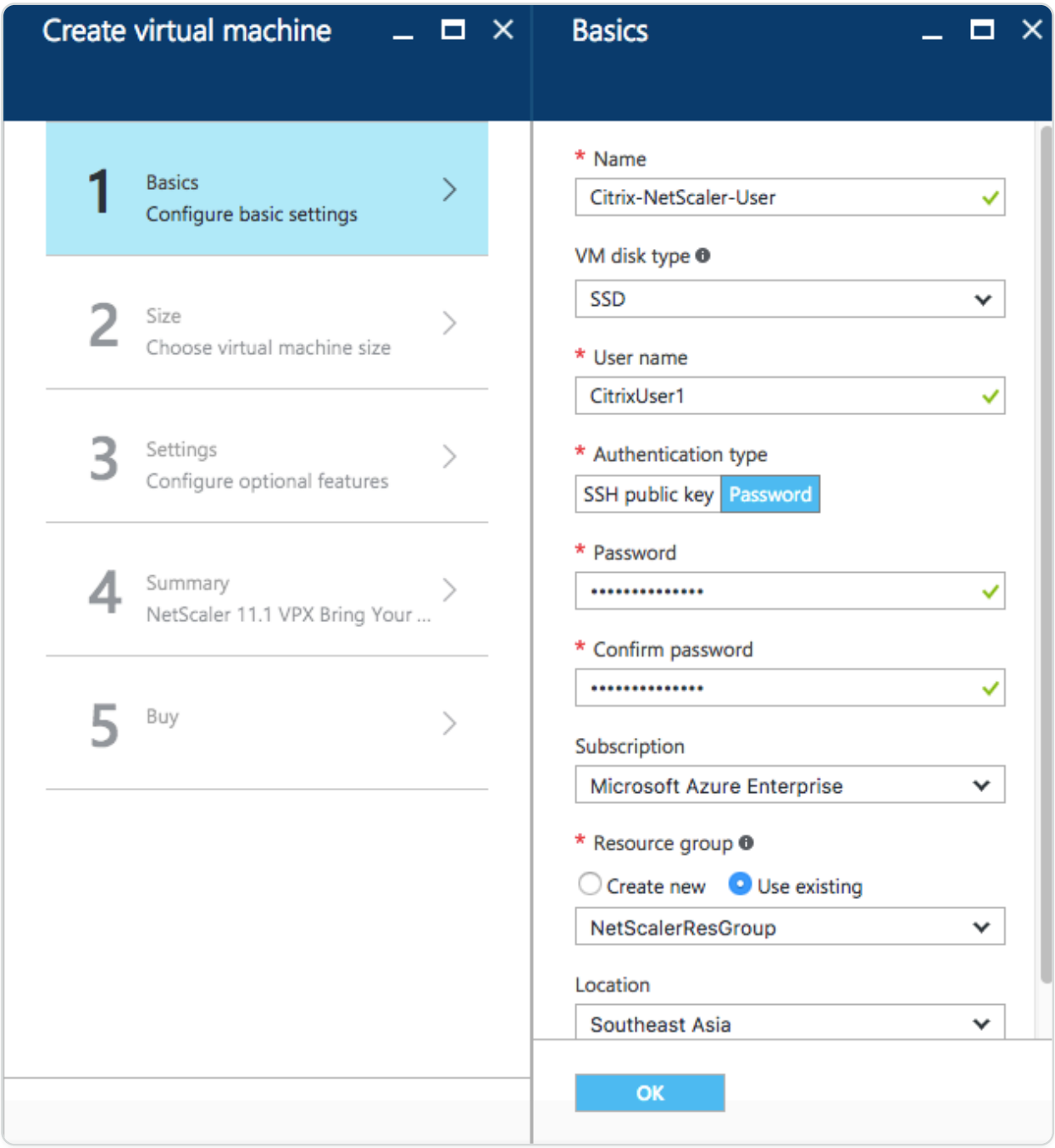


注意：

确保选择最新的映像。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 **Resource Manager**，然后单击 **创建**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 在 **创建虚拟机** 窗格中，在每个部分中指定所需值以创建虚拟机。在每个部分中单击 **确定** 以保存配置。

基本：

- 名称 - 为 NetScaler VPX 实例指定名称
- VM 磁盘类型 - 从下拉菜单中选择 SSD（默认值）或 HDD
- 用户名和密码 - 指定用户名和密码以访问您创建的资源组中的资源
- 身份验证类型 - 选择 SSH 公钥或密码
- 资源组 - 从下拉列表中选择您已创建的资源组

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以在此处创建资源组，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 Stack 环境中，除了基本参数之外，请指定以下参数：

- 蔚蓝堆栈域
- Azure Stack 租户（可选）
- Azure 客户端（可选）
- Azure 客户端密钥（可选）

大小：

根据您在基本设置中选择的 VM 磁盘类型（SDD 或 HDD），将显示磁盘大小。

- 根据您的要求选择磁盘大小，然后单击“**选择**”。

设置：

- 选择默认（标准）磁盘类型
- 存储帐户 - 选择存储帐户
- 虚拟网络 - 选择虚拟网络
- 子网 - 设置子网地址
- 公共 IP 地址 - 选择 IP 地址分配类型
- 网络安全组 - 选择您已创建的安全组。确保在安全组中配置了入站和出站规则。
- 可用性集 - 从下拉菜单框中选择可用性集

摘要：

配置设置已验证，“摘要”页面显示验证结果。如果验证失败，“摘要”页面会显示失败原因。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“**确定**”。

购买：

在“购买”页面上查看优惠详情和法律条款，然后单击“**购买**”。

对于高可用性部署，请在同一可用性集和同一资源组中创建两个独立的 NetScaler VPX 实例，以主动-备用配置部署它们。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

为 NetScaler VPX 独立实例配置多个 IP 地址

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 实例可以连接一个或多个 NIC，并且每个 NIC 可以分配一个或多个静态或动态的公共和私有 IP 地址。您可以将多个 IP 地址分配为 NSIP、VIP、SNIP 等。

有关详细信息，请参阅 Azure 文档 使用 Azure 门户将多个 IP 地址分配给虚拟机。

如果要使用 PowerShell 命令，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。

用例

在此用例中，独立 NetScaler VPX 设备配置了一个连接到虚拟网络 (VNET) 的单个 NIC。该 NIC 与三个 IP 配置 (ipconfig) 相关联，每个配置服务于不同的目的 - 如表中所示。

IP 配置	关联到	用途
IP 配置 1	静态公共 IP 地址；静态私有 IP 地址	用于管理流量
IP 配置 2	静态公共 IP 地址；静态私有地址	用于客户端流量
IP配置3	静态私有 IP 地址	与后端服务器通信

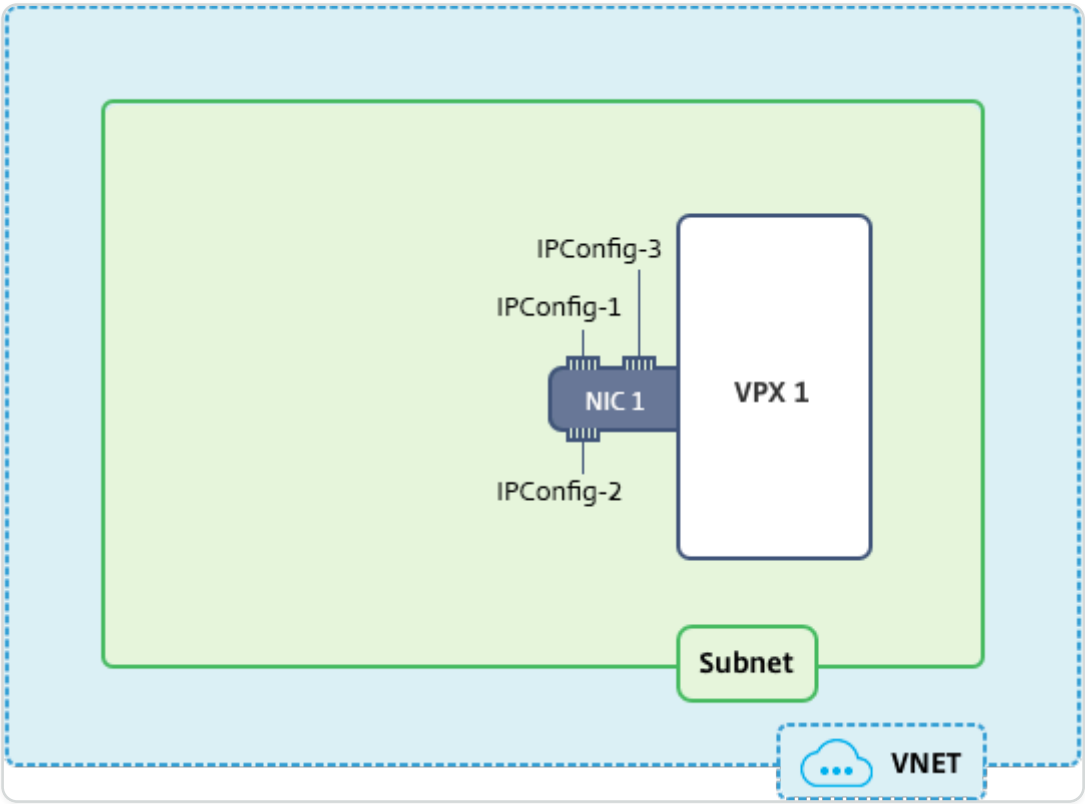
注意：

`IPConfig-3` 未与任何公共 IP 地址关联。

图：拓扑

以下是用例的可视化表示。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

在多网卡、多 IP 的 Azure NetScaler VPX 部署中，与主（第一个）网卡的主（第一个）`IPConfig` 关联的私有 IP 会自动添加为设备的管理 NSIP。与 `IPConfigs` 关联的其余私有 IP 地址需要根据您的要求，通过使用 `add ns ip` 命令，在 VPX 实例中作为 VIP 或 SNIP 添加。

开始之前

开始之前，请按照此链接中给出的步骤创建 VPX 实例：

配置 NetScaler VPX 独立实例

对于此用例，已创建 NSDoc0330VM VPX 实例。

在独立模式下为 NetScaler VPX 实例配置多个 IP 地址的步骤。

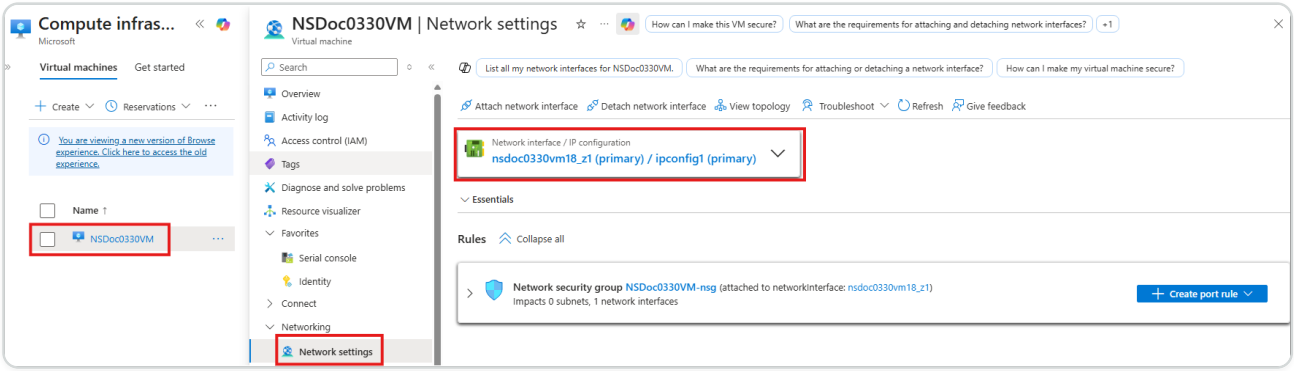
在独立模式下为 NetScaler VPX 设备配置多个 IP 地址：

1. 将 IP 地址添加到 VM
2. 配置 NetScaler 拥有的 IP 地址

步骤 1：将 IP 地址添加到 VM

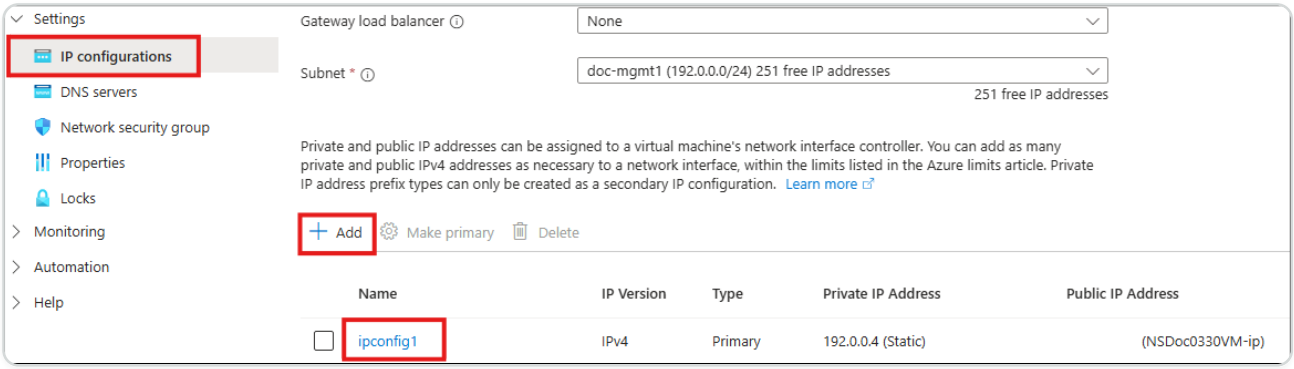
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 在门户中，在筛选框中单击**更多服务 > 键入虚拟机**，然后单击**虚拟机**。
2. 在“**虚拟机**”边栏选项卡中，单击要添加 IP 地址的 VM。在出现的虚拟机边栏选项卡中，单击“**网络接口**”，然后选择网络接口。



在为所选 NIC 出现的边栏选项卡中，单击“**IP 配置**”。将显示创建 VM 时分配的现有 IP 配置 **ipconfig1**。对于此用例，请确保与 ipconfig1 关联的 IP 地址是静态的。接下来，创建另外两个 IP 配置：ipconfig2 (VIP) 和 ipconfig3 (SNIP)。

要创建更多 `ipconfigs`，请点击“**添加**”。

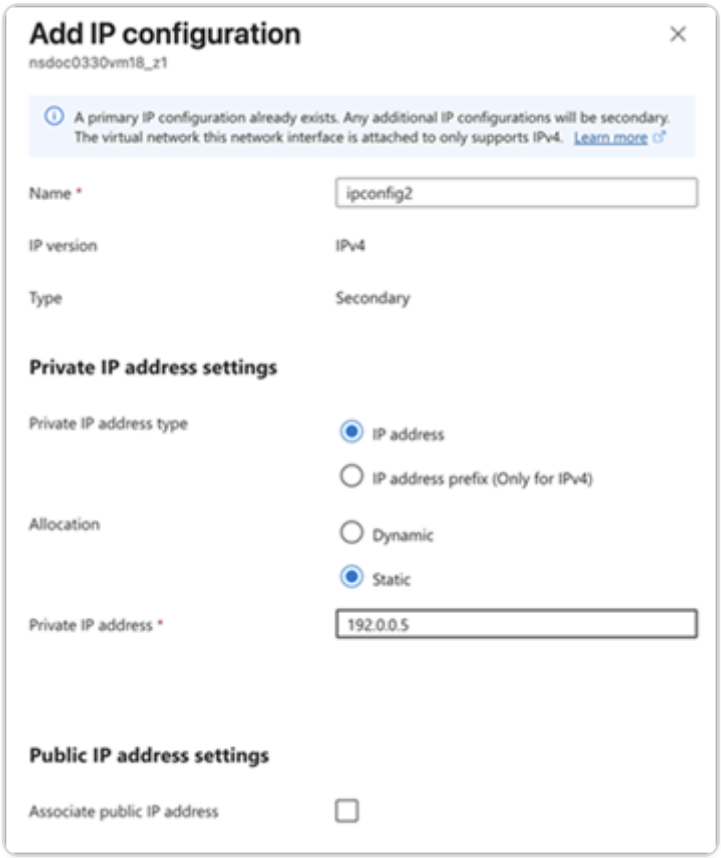


在“**添加 IP 配置**”窗口中，输入“**名称**”，将分配方法指定为“**静态**”，输入 IP 地址（此用例为 192.0.0.5），然后启用“**公共 IP 地址**”。

注意：

在添加静态私有 IP 地址之前，请检查 IP 地址的可用性，并确保该 IP 地址属于 NIC 所连接的同一子网。

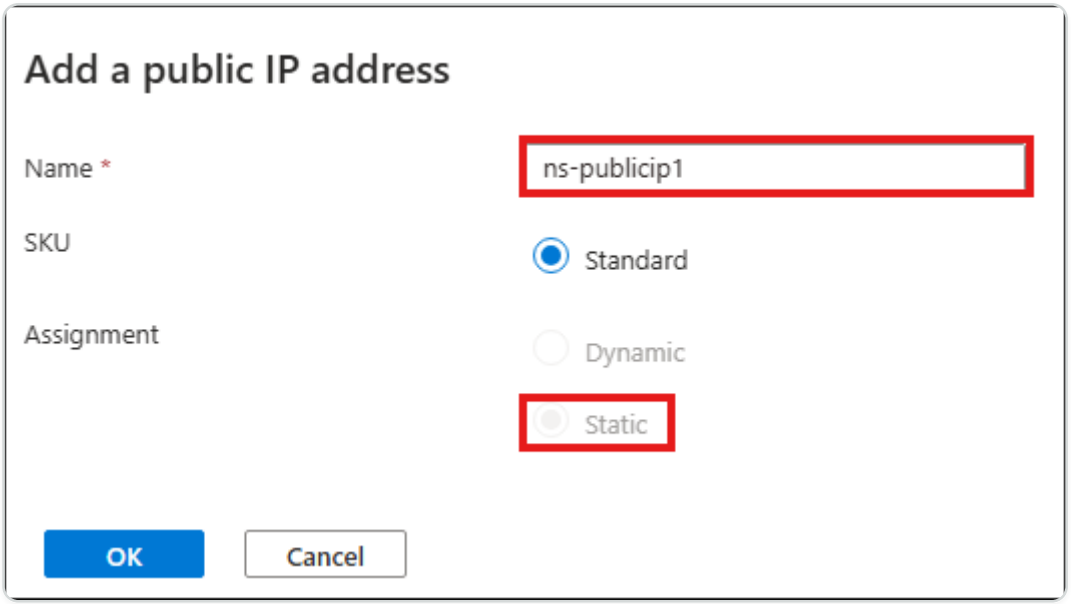
© 1997–2026 Citrix Systems, Inc. All rights reserved.



接下来，点击“**配置所需设置**”为 ipconfig2 创建静态公共 IP 地址。

默认情况下，公共 IP 是动态的。为确保 VM 始终使用相同的公共 IP 地址，请创建静态公共 IP。

在“创建公共 IP 地址”边栏选项卡中，添加名称，在“分配”下单击“**静态**”。然后单击“**确定**”。

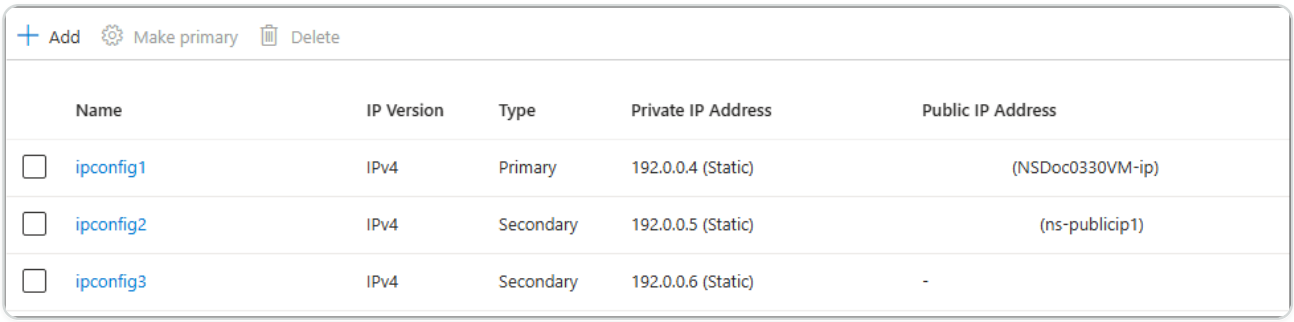


© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

即使将分配方法设置为静态，您也无法指定分配给公共 IP 资源的实际 IP 地址。相反，它会从资源创建所在的 Azure 位置的可用 IP 地址池中分配。

按照步骤为 ipconfig3 添加一个 IP 配置。公共 IP 不是强制性的。



Name	IP Version	Type	Private IP Address	Public IP Address
ipconfig1	IPv4	Primary	192.0.0.4 (Static)	(NSDoc0330VM-ip)
ipconfig2	IPv4	Secondary	192.0.0.5 (Static)	(ns-publicip1)
ipconfig3	IPv4	Secondary	192.0.0.6 (Static)	-

步骤 2：配置 NetScaler 拥有的 IP 地址

使用 GUI 或命令 `add ns ip` 配置 NetScaler 拥有的 IP 地址。有关详细信息，请参阅 配置 NetScaler 拥有的 IP 地址。

配置具有多个 IP 地址和网卡的高可用性设置

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，辅助节点不响应。一旦主节点向运行状况探测发送响应，ALB 就会开始向该实例发送数据流量。如果主实例错过两次连续的运行状况探测，ALB 不会将流量重定向到该实例。发生故障转移时，新的主节点开始响应运行状况探测，ALB 会将流量重定向到它。标准 VPX 高可用性故障转移时间为三秒。流量切换可能需要的总故障转移时间最长为 13 秒。

您可以在 Azure 上部署一对具有多个网卡的主动-被动高可用性 (HA) 设置的 NetScaler VPX 实例。每个网卡可以包含多个 IP 地址。

多网卡高可用性部署有以下选项：

- 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 可用性集和可用性区域的更多信息，请参阅 Azure 文档 管理 Linux 虚拟机的可用性。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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：

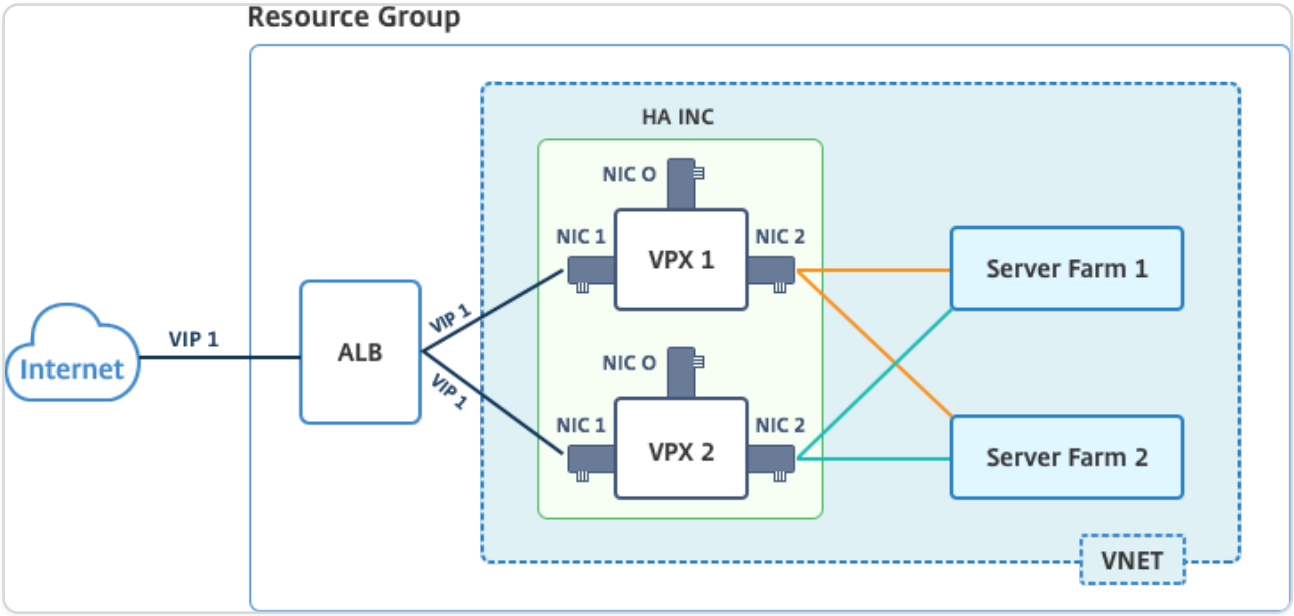
- HA 独立网络配置 (INC)
- 直接服务器返回 (DSR) 模式下的 Azure 负载均衡器 (ALB)

所有流量都通过主节点。辅助节点保持待机模式，直到主节点发生故障。

注意：

为了使 Azure 云上的 NetScaler VPX 高可用性部署正常工作，您需要一个可在两个 VPX 节点之间移动的浮动公共 IP (PIP)。Azure 负载均衡器 (ALB) 提供该浮动 PIP，该 PIP 在发生故障转移时会自动移动到第二个节点。

图示：使用 Azure 可用性集的 HA 部署架构示例



在主动-被动部署中，ALB 前端公共 IP (PIP) 地址被添加为每个 VPX 节点中的 VIP 地址。在 HA-INC 配置中，VIP 地址是浮动的，SNIP 地址是实例特定的。

您可以通过以下两种方式部署主动-被动高可用性模式的 VPX 对：

- **NetScaler VPX 标准高可用性模板**：使用此选项配置具有三个子网和六个 NIC 默认选项的 HA 对。
- **Windows PowerShell 命令**：使用此选项根据您的子网和 NIC 要求配置 HA 对。

本主题介绍如何使用 Citrix 模板在主动-被动 HA 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

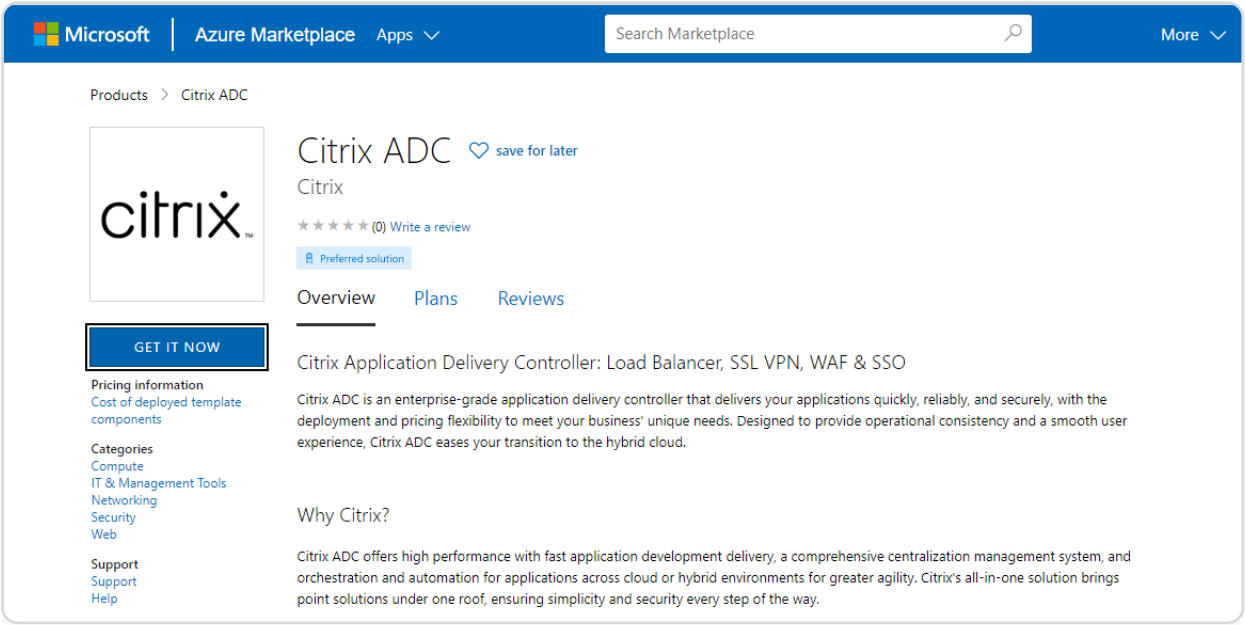
使用 NetScaler® 高可用性模板配置 HA-INC 节点

您可以使用标准模板快速高效地以 HA-INC 模式部署一对 VPX 实例。该模板创建两个节点，具有三个子网和六个 NIC。这些子网用于管理、客户端和服务器端流量，并且每个子网为两个 VPX 实例各有两个 NIC。

您可以在 Azure Marketplace 获取 NetScaler HA 对模板。

完成以下步骤以启动模板并使用 Azure 可用性集部署高可用性 VPX 对。

1. 在 Azure Marketplace 中，搜索 **NetScaler**。



2. 单击 **立即获取**。
3. 选择所需的 HA 部署以及许可证，然后单击 **继续**。

   带许可证的 Azure HA(/en-us/vpx/media/adc-ha-license-citrix.png)

4. **基本信息**页面出现。创建资源组并选择**确定**。

   模板基本信息(/en-us/vpx/media/template-basics.png)

5. **常规设置**页面出现。输入详细信息并选择**确定**。

   常规设置(/en-us/vpx/media/monitoring-metrics.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

默认情况下，**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。将参与者角色分配给新创建的 AAD 应用程序。有关详细信息，请参阅使用门户创建可访问资源的 Azure Active Directory 应用程序和服务主体。

6. **网络设置**页面出现。检查 VNet 和子网配置，编辑所需设置，然后选择**确定**。

   网络设置(/en-us/vpx/media/template-networksettings.png)

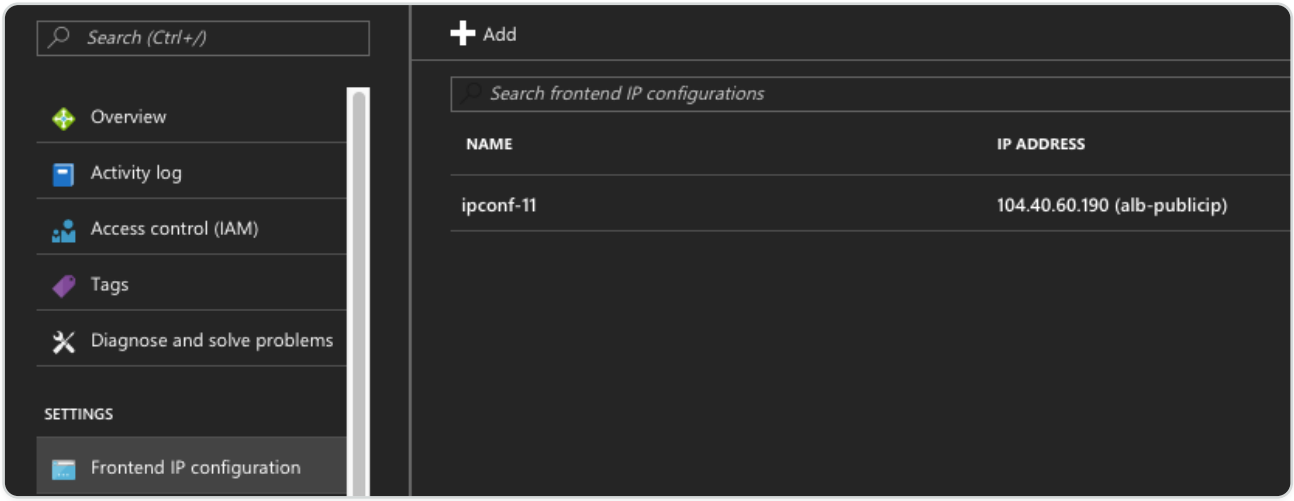
7. **摘要**页面出现。查看配置并进行相应编辑。选择**确定**以确认。
8. **购买**页面出现。选择**购买**以完成部署。

Azure 资源组可能需要一些时间才能使用所需的配置创建。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 ns-vpx0 和 ns-vpx1。

如果您的 HA 设置需要进一步修改，例如创建更多安全规则和端口，您可以从 Azure 门户进行操作。

Azure 门户(/en-us/vpx/media/node1and2-12-1.png)

接下来，您需要在主节点上使用 **ALB 的前端公共 IP (PIP) 地址**配置负载均衡虚拟服务器。要查找 ALB PIP，请选择 ALB \> **前端 IP 配置**。



有关如何配置负载均衡虚拟服务器的更多信息，请参阅“**资源**”部分。

资源：

以下链接提供了有关 HA 部署和虚拟服务器配置的更多信息：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在不同子网中配置高可用性节点
- 设置基本负载均衡

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 HA 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 区域内故障隔离的位置，提供冗余电源、散热和网络，并提高弹性。只有特定的 Azure 区域支持可用性区域。有关更多信息，请参阅 Azure 文档 [Azure 中的可用性区域是什么。

图：使用 Azure 可用性区域的高可用性部署架构示例

您可以使用 Azure Marketplace 中提供的名为“NetScaler 13.0 HA using Availability Zones”的模板，以高可用性模式部署 VPX 对。

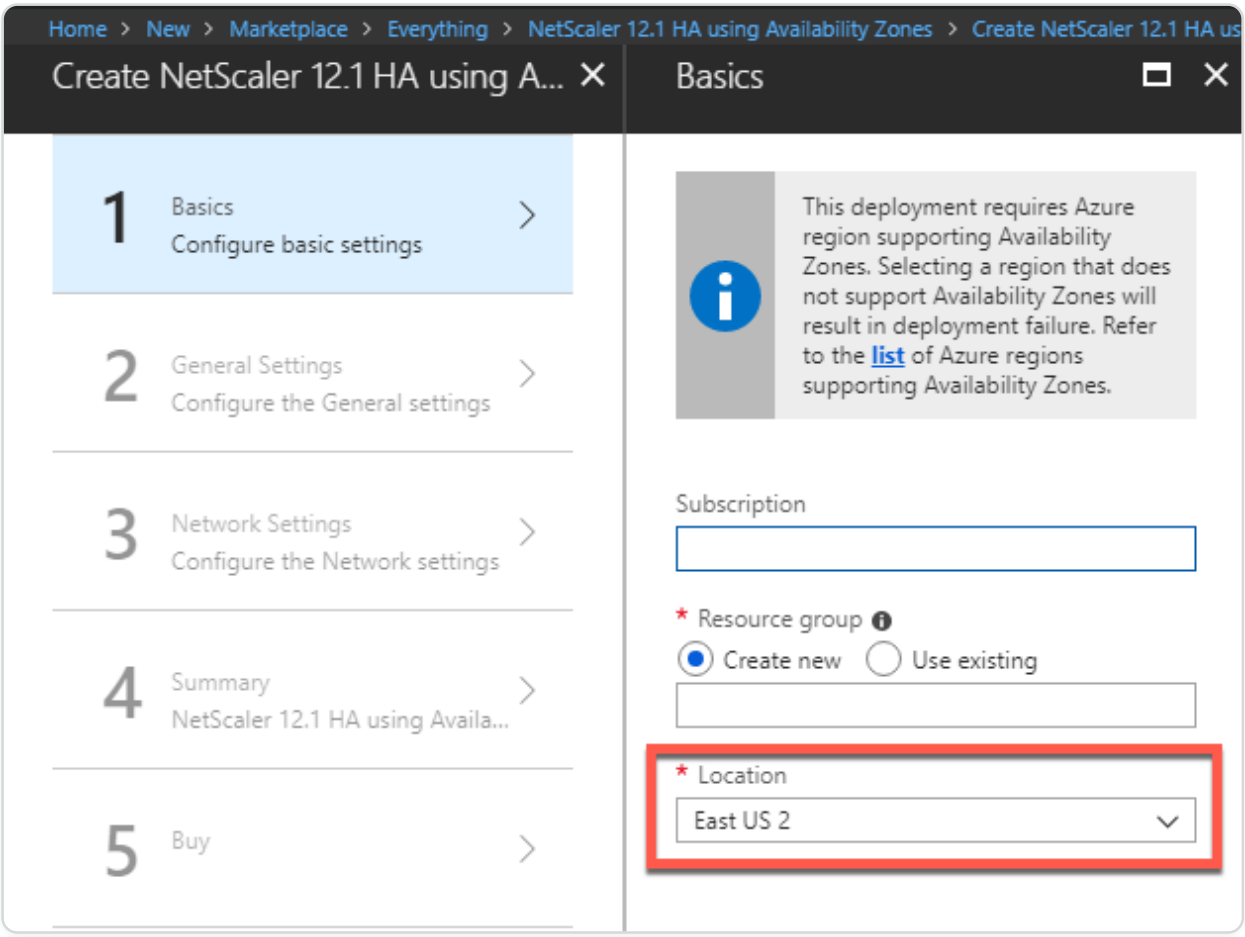
完成以下步骤以启动模板并使用 Azure 可用性区域部署高可用性 VPX 对。

1. 从 Azure Marketplace 中，选择并启动 Citrix® 解决方案模板。

2. 确保部署类型为 Resource Manager，然后选择“**创建**”。
3. 出现“**基本信息**”页面。输入详细信息，然后单击“**确定**”。

> **注意：**
>
> 确保选择支持可用区的 Azure 区域。有关支持可用区的区域的更多信息，请参阅 Azure 文档 Azure 中的可用区是什么？

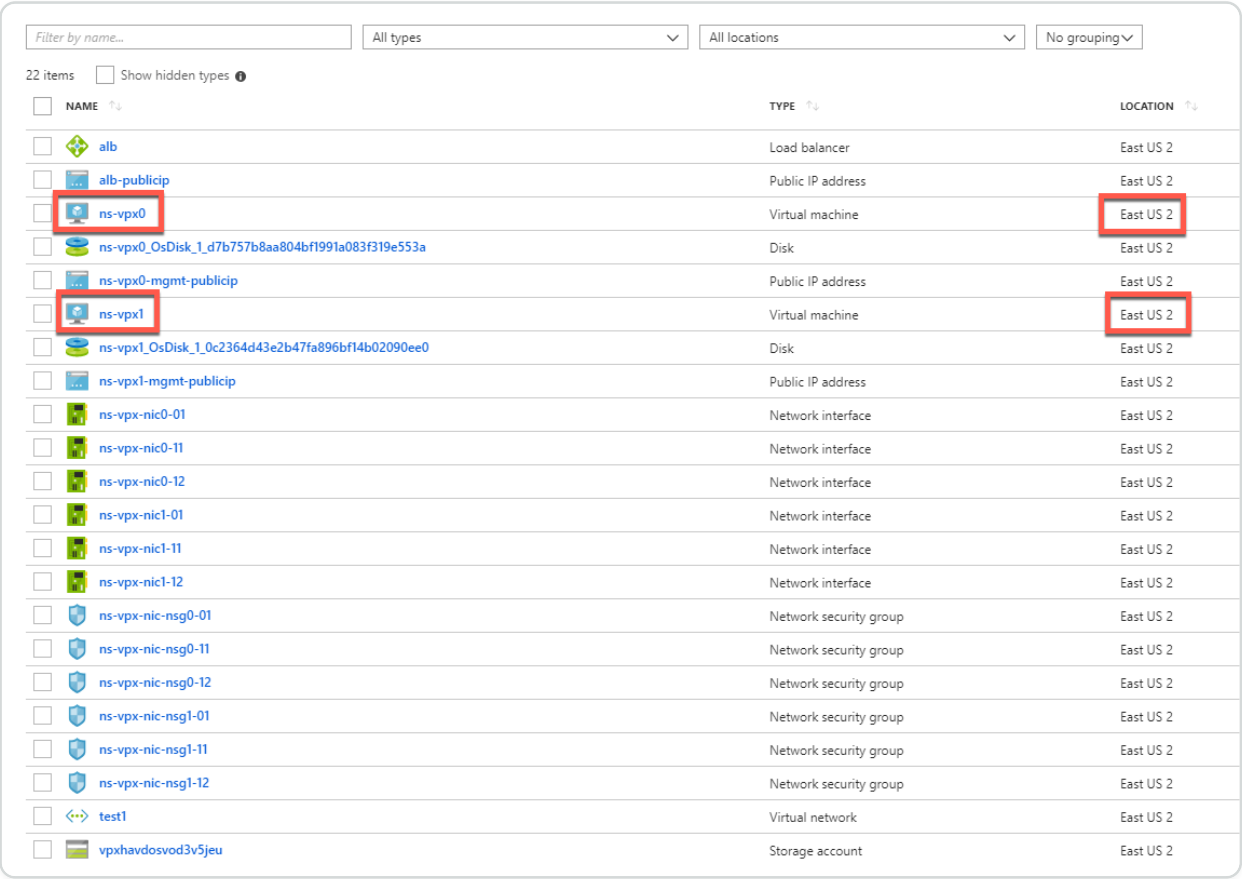
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 出现“**常规设置**”页面。输入详细信息，然后选择“**确定**”。
5. 出现“**网络设置**”页面。检查 VNet 和子网配置，编辑所需设置，然后选择“**确定**”。
6. 出现“**摘要**”页面。查看配置并进行相应编辑。选择“**确定**”以确认。
7. 出现“**购买**”页面。选择“**购买**”以完成部署。

   Azure 资源组可能需要一些时间才能使用所需的配置创建。完成后，选择“**资源组**”以在 Azure 门户中查看配置详细信息，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，您可以在“**位置**”列下看到位置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



如果您的 HA 设置需要进一步修改，例如创建更多安全规则和端口，您可以从 Azure 门户进行操作。

使用 Azure Monitor 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。您可以使用 **Metrics Explorer** 访问收集到的数据。有关详细信息，请参阅 Azure Monitor 指标概述。

注意事项

- 如果您通过 Azure Marketplace 产品在 Azure 上部署 NetScaler VPX 实例，则指标服务默认处于禁用状态。
- Azure CLI 不支持指标服务。
- 指标适用于 CPU（管理和数据包 CPU 使用率）、内存和吞吐量（入站和出站）。

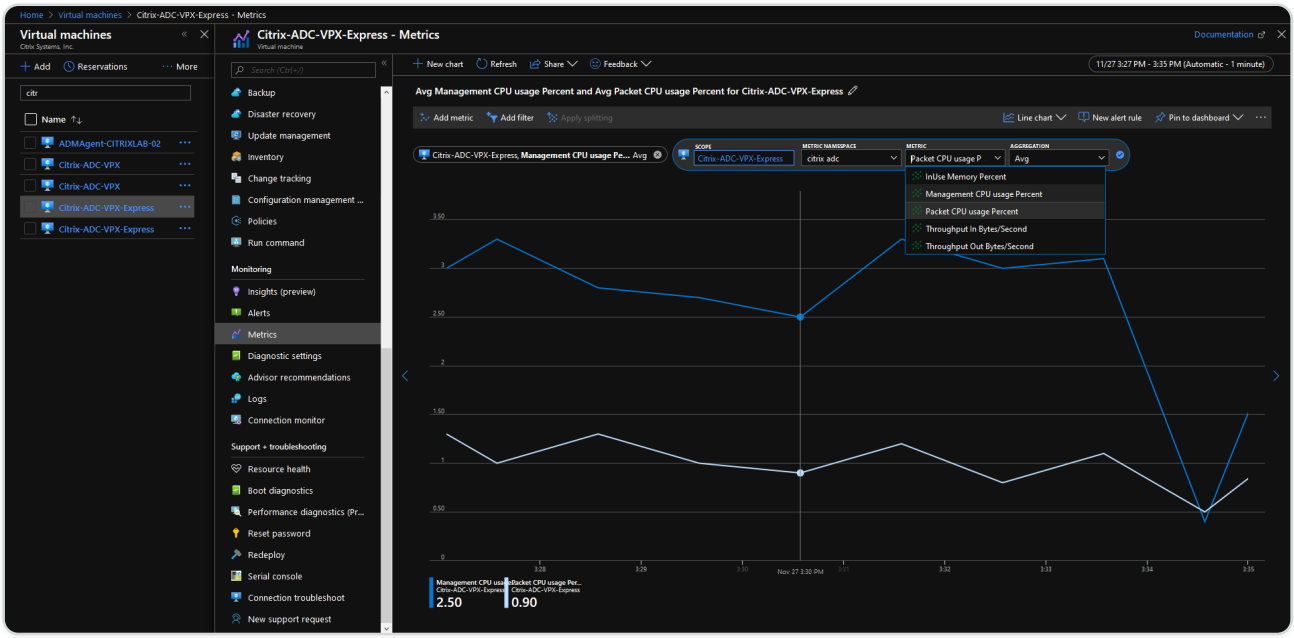
如何在 Azure 监视器中查看指标

若要在 Azure 监视器中查看实例的指标，请执行以下步骤：

1. 登录到 **Azure 门户 > 虚拟机**。
2. 选择作为主节点的虚拟机。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在“**监视**”部分，单击“**指标**”。
4. 从“**指标命名空间**”下拉菜单中，单击“**NetScaler**”。
5. 在“**指标**”下拉菜单中的“**所有指标**”下，单击要查看的指标。
6. 单击“**添加指标**”可在同一图表上查看另一个指标。使用“图表选项”自定义图表。



使用 PowerShell 命令配置具有多个 IP 地址和 NIC 的高可用性设置

您可以在 Azure 上部署一对具有多个 NIC 的 NetScaler VPX 实例，以实现主动-被动高可用性 (HA) 设置。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)
- 处于直接服务器返回 (DSR) 模式的 Azure 负载均衡器 (ALB)

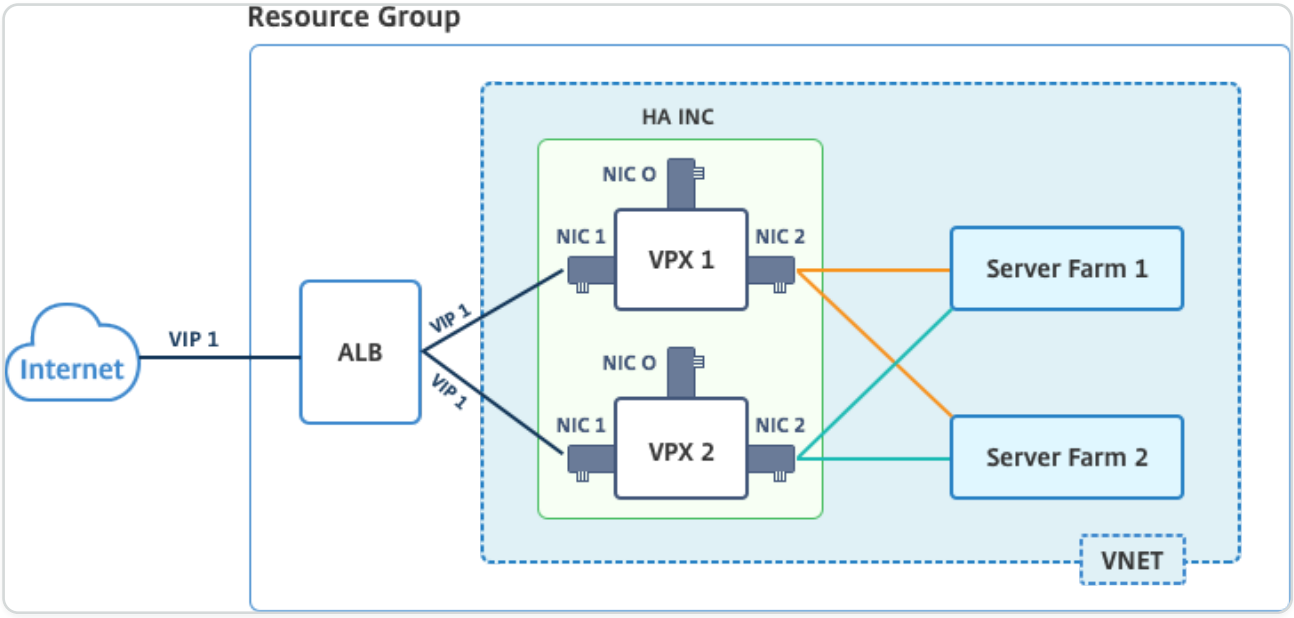
所有流量都通过主节点。辅助节点保持待机模式，直到主节点发生故障。

注意：

要在 Azure 云上实现 NetScaler VPX 高可用性部署，您需要一个可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) 提供该浮动 PIP，在故障转移事件中，该 PIP 会自动移动到第二个节点。

图：主动-被动部署架构示例

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在主动-被动部署中，ALB 浮动公共 IP (PIP) 地址作为 VIP 地址添加到每个 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 秒发送一次健康探测来监视每个 VPX 实例，并且仅将流量重定向到定期发送健康探测响应的实例。因此，在 HA 设置中，主节点响应健康探测，而辅助节点不响应。如果主实例连续两次未响应健康探测，ALB 将不会将流量重定向到该实例。在故障转移时，新的主节点开始响应健康探测，ALB 会将流量重定向到它。标准 VPX 高可用性故障转移时间为三秒。流量切换可能需要的总故障转移时间最长为 13 秒。

您可以通过以下两种方式部署主动-被动 HA 设置中的 VPX 对：

- **NetScaler VPX 标准高可用性模板**：使用此选项配置一个 HA 对，其中包含三个子网和六个 NIC 的默认选项。
- **Windows PowerShell 命令**：使用此选项根据您的子网和 NIC 要求配置 HA 对。

本主题介绍如何使用 PowerShell 命令在主动-被动 HA 设置中部署 VPX 对。如果要使用 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

在此场景中，您将使用表中给出的拓扑部署 NetScaler VPX 对。每个 VPX 实例包含三个 NIC，每个 NIC 部署在不同的子网中。每个 NIC 都分配有一个 IP 配置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ALB	VPX1	VPX2
ALB 与公共 IP 3 (pip3) 关联	管理 IP 配置为 IPConfig1，其中包括一个公共 IP (pip1) 和一个私有 IP (12.5.2.24)；nic1；Mgmtsubnet=12.5.2.0/24	管理 IP 配置为 IPConfig5，其中包括一个公共 IP (pip3) 和一个私有 IP (12.5.2.26)；nic4；Mgmtsubnet=12.5.2.0/24
配置的 LB 规则和端口为 HTTP (80)、SSL (443)、健康探测 (9000)	客户端 IP 配置为 IPConfig3，其中包括一个私有 IP (12.5.1.27)；nic2；FrontEndsubet=12.5.1.0/24	客户端 IP 配置为 IPConfig7，其中包括一个私有 IP (12.5.1.28)；nic5；FrontEndsubet=12.5.1.0/24
-	服务器端 IP 配置为 IPConfig4，其中包括一个私有 IP (12.5.3.24)；nic3；BackendSubnet=12.5.3.0/24	服务器端 IP 配置为 IPConfig8，其中包括一个私有 IP(12.5.3.28)；nic6；BackendSubnet=12.5.3.0/24
-	NSG 的规则和端口是 SSH (22)、HTTP (80)、HTTPS (443)	-

参数设置

在此场景中使用以下参数设置：

```
$locName= "South east Asia"

$rgName = "MulitIP-MultiNIC-RG"

$nicName1= "VM1-NIC1"

$nicName2 = "VM1-NIC2"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$domName1="vpx1dns"

$domName2="vpx2dns"

$domName3="vpxalbdns"

$vmNamePrefix="VPXMultiIPALB"

$osDiskSuffix1="osmultiipalbdiskdb1"

$osDiskSuffix2="osmultiipalbdiskdb2"

$lbName= "MultiIPALB"

$frontEndConfigName1= "FrontEndIP"

$backendPoolName1= "BackendPoolHttp"

$lbRuleName1= "LBRuleHttp"

$healthProbeName= "HealthProbe"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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. 创建公共 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$subnetName ="frontEndSubnet"

$subnet1=$vnet.Subnets|?{$_.Name -eq $subnetName}

$subnetName="backEndSubnet"

$subnet2=$vnet.Subnets|?{$_.Name -eq $subnetName}

$subnetName="mgmtSubnet"

$subnet3=$vnet.Subnets|?{$_.Name -eq $subnetName}
```

创建公共 IP 地址。

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
$rgName -DomainNameLabel $domName1 -Location $locName -AllocationMethod
Dynamic
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
$rgName -DomainNameLabel $domName2 -Location $locName -AllocationMethod
Dynamic



$pip3=New-AzureRmPublicIpAddress -Name $pubIPName3 -ResourceGroupName
$rgName -DomainNameLabel $domName3 -Location $locName -AllocationMethod
Dynamic
```

为 VPX1 创建 IP 配置。

```
$IpConfigName1 = "IPConfig1"





$IPAddress = "12.5.2.24"




$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1
-Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip1
-Primary




$IPConfigName3="IPConfig-3"




$IPAddress="12.5.1.27"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3
-Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary




$IPConfigName4 = "IPConfig-4"




$IPAddress = "12.5.3.24"




$IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4
-Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

为 VPX2 创建 IP 配置。

```
$IpConfigName5 = "IPConfig5"




$IPAddress="12.5.2.26"




$IPConfig5=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName5
-Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip2
-Primary
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$IPConfigName7="IPConfig-7"



$IPAddress="12.5.1.28"



$IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7
-Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary



$IPConfigName8="IPConfig-8"



$IPAddress="12.5.3.28"



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

为 VPX1 创建 NIC。

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig1
-NetworkSecurityGroupId $nsg.Id
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$nic2=New-AzureRmNetworkInterface -Name $nicName2 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig3
-NetworkSecurityGroupId $nsg.Id




$nic3=New-AzureRmNetworkInterface -Name $nicName3 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig4
-NetworkSecurityGroupId $nsg.Id
```

为 VPX2 创建 NIC。

```
$nic4=New-AzureRmNetworkInterface -Name $nicName4 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig5
-NetworkSecurityGroupId $nsg.Id




$nic5=New-AzureRmNetworkInterface -Name $nicName5 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig7
-NetworkSecurityGroupId $nsg.Id




$nic6=New-AzureRmNetworkInterface -Name $nicName6 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig8
-NetworkSecurityGroupId $nsg.Id
```

创建 VPX1。

此步骤包括以下子步骤：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 创建 VM 配置对象
- 设置凭据、操作系统和映像
- 添加网卡
- 指定操作系统磁盘并创建虚拟机

```
$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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 $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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.
```

```
$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 $nic4.Id
-Primary




$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic5.Id




$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic6.Id
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$osDiskName=$vmName + "-" + $osDiskSuffix2




$osVhdUri=$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

```
```
```

要查看分配给网卡的私有和公共 IP 地址，请键入以下命令：

```
```

$nic1.IPConfig
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.
```

```
$nic2.IPConfig




$nic3.IPConfig




$nic4.IPConfig




$nic5.IPConfig




$nic6.IPConfig
```

创建 Azure 负载均衡器 (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
- 创建负载均衡规则（HTTP 和 SSL）
- 使用前端 IP 配置、后端地址池和负载均衡规则创建 ALB
- 将 IP 配置与后端池关联

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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 NetScaler VPX 对后，登录到每个 VPX 实例以配置 HA-INC 以及 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. 将客户端 NIC 的私有 IP 地址添加为 VPX1 (NIC2) 和 VPX2 (NIC5) 的 SNIP。

   ```
   add nsip privateIPofNIC2 255.255.255.0 -type SNIP
   ```
   ```
   add nsip privateIPofNIC5 255.255.255.0 -type SNIP
   ```

3. 在主节点上添加负载平衡虚拟服务器，其前端 IP 地址为 ALB 的公共 IP。

   ```
   add lb virtual server v1 HTTP FrontEndIPofALB 80
   ```

相关资源：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 Azure 上配置主动-备用高可用性部署的 GSLB(/zh-cn/vpx/13-1/deploy-vpx-on-azure/configuring-gslb-active-standby-ha-deployment-azure.html)

在 Azure 上部署处于浮动 IP 禁用模式的 ALB 的 NetScaler 高可用性对

您可以在 Azure 上以主动-被动高可用性 (HA) 设置部署一对具有多个 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 负载均衡器 (ALB)，具有：
  - 浮动 IP 启用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。

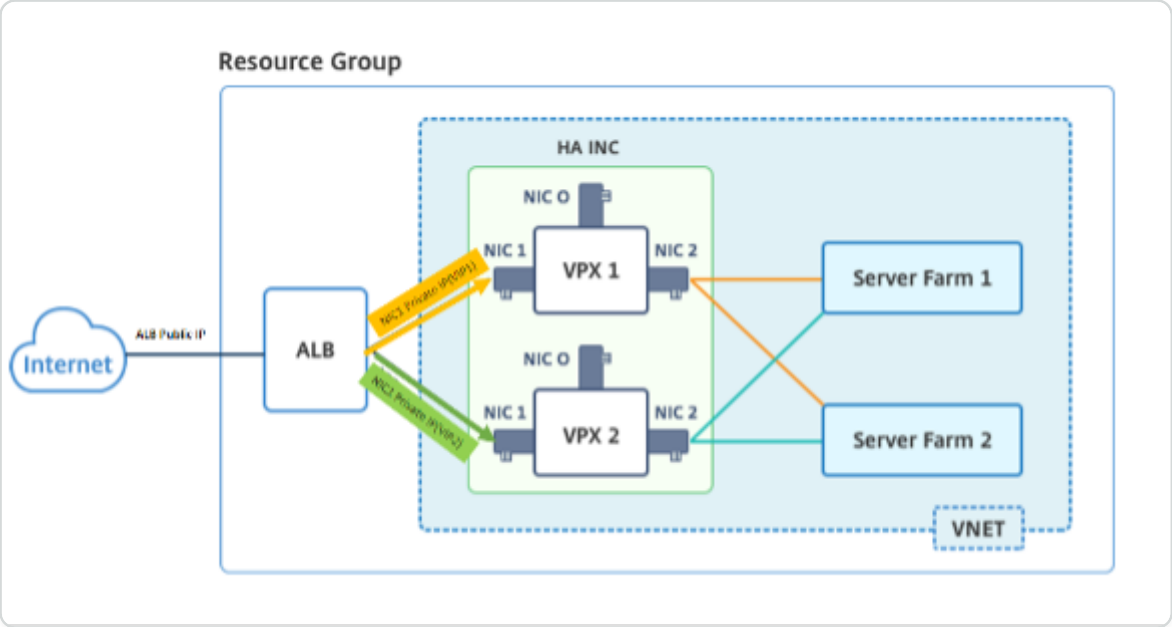
如果要在 Azure 上部署启用 ALB 浮动 IP 的主动-被动 HA 设置中的 VPX 对，请参阅 (/zh-cn/vpx/13-1/deploy-vpx-on-azure/configure-ha-pair-using-powershell.html)。

处于浮动 IP 禁用模式的 ALB 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私有 IP 地址作为 VIP 地址添加到每个 VPX 实例中。在 HA-INC 模式下进行配置，其中 VIP 地址使用 IPSet 共享，SNIP 地址是实例特定的。所有流量都通过主实例。辅助实例处于待机模式，直到主实例发生故障。

图：主动-被动部署架构示例

© 1997–2026 Citrix Systems, Inc. All rights reserved.



先决条件

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 网络。有关更多信息，请参阅 ADC 网络。
- Azure 负载均衡器和负载均衡规则配置。有关更多信息，请参阅 Azure ALB 文档。

如何在 Azure 上部署禁用 ALB 浮动 IP 的 VPX HA 对

以下是 HA 和 ALB 部署步骤的摘要：

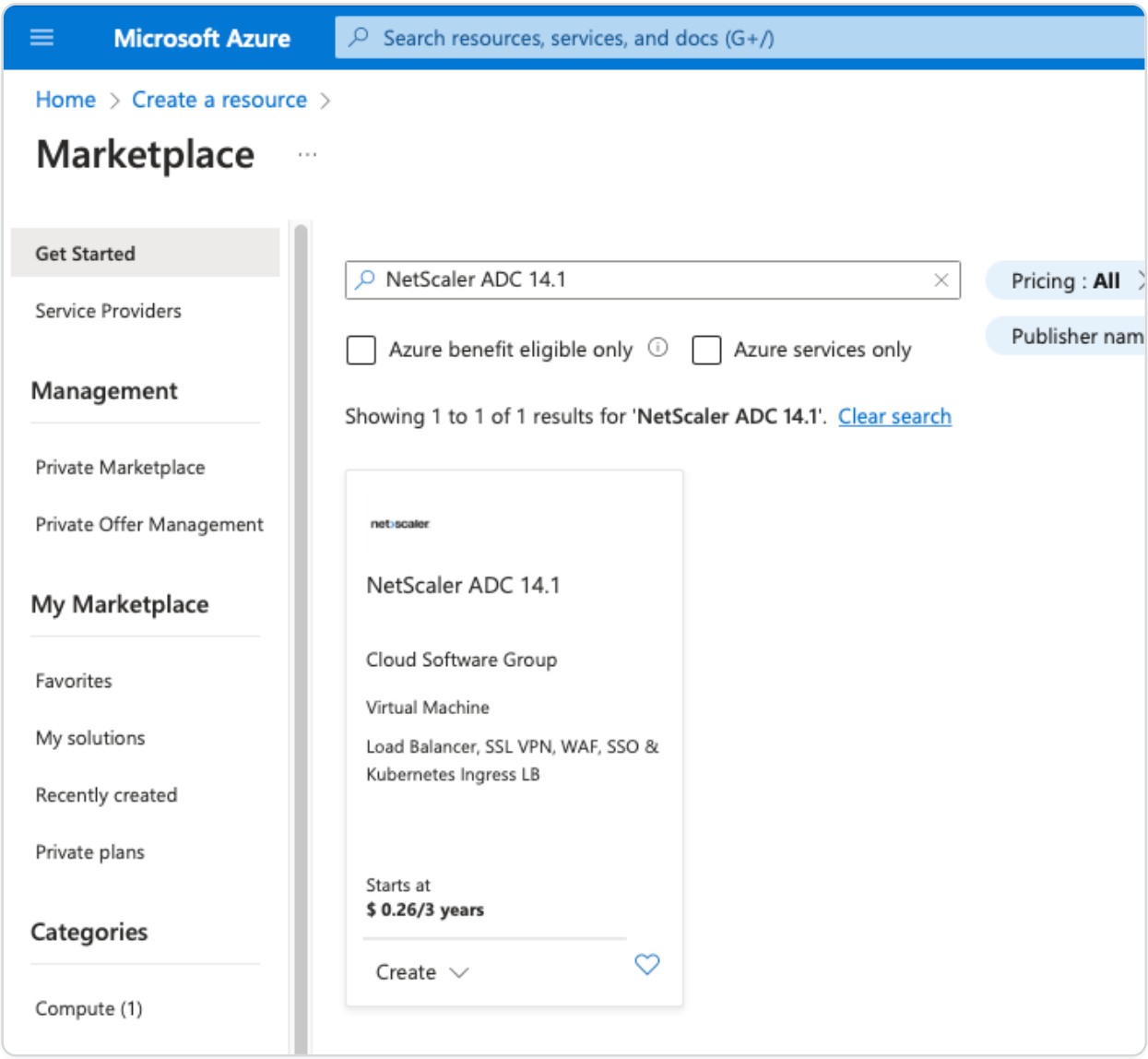
1. 在 Azure 上部署两个 VPX 实例（主实例和辅助实例）。
2. 在两个实例上添加客户端和服务器 NIC。
3. 部署一个 ALB，其负载均衡规则的浮动 IP 模式已禁用。
4. 使用 NetScaler GUI 在两个实例上配置 HA 设置。

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：

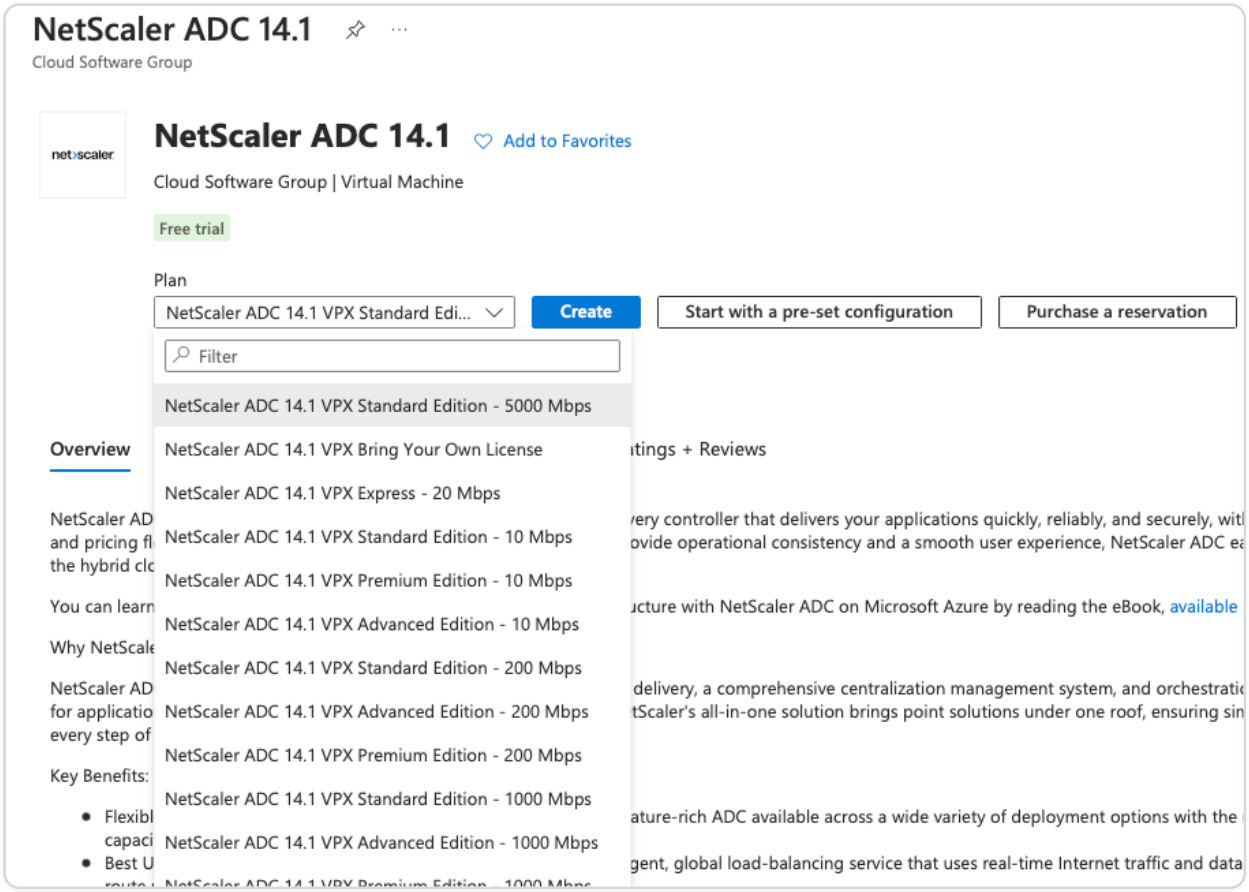
1. 从 Azure Marketplace 中选择 NetScaler 版本（在此示例中，使用 NetScaler 13.1 版本）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 选择所需的 ADC 许可模式，然后单击 **Create**。

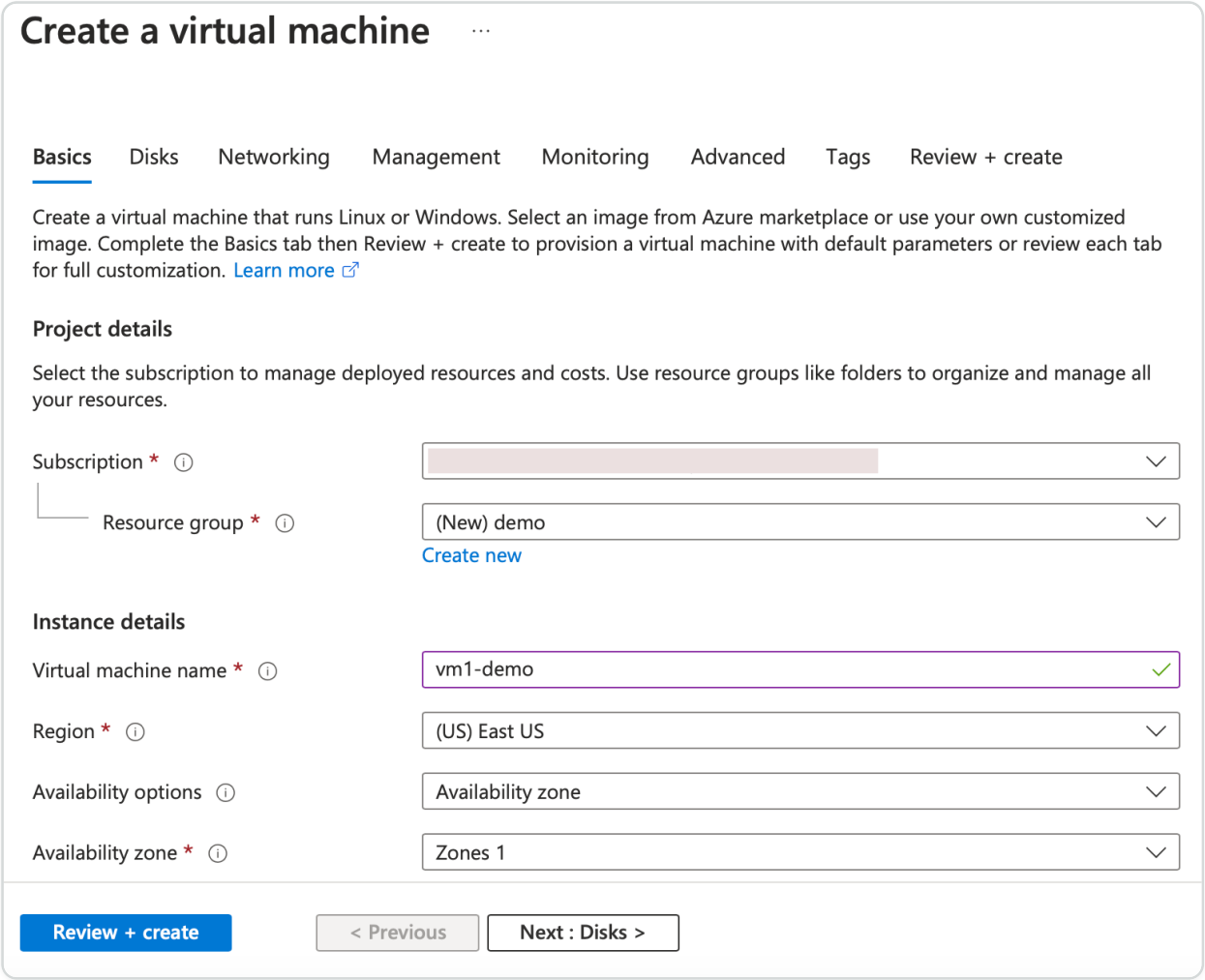
© 1997–2026 Citrix Systems, Inc. All rights reserved.



“**创建虚拟机**”页面打开。

3. 在每个选项卡中填写所需详细信息：基本信息、磁盘、网络、管理、监视、高级和标签，以成功部署。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



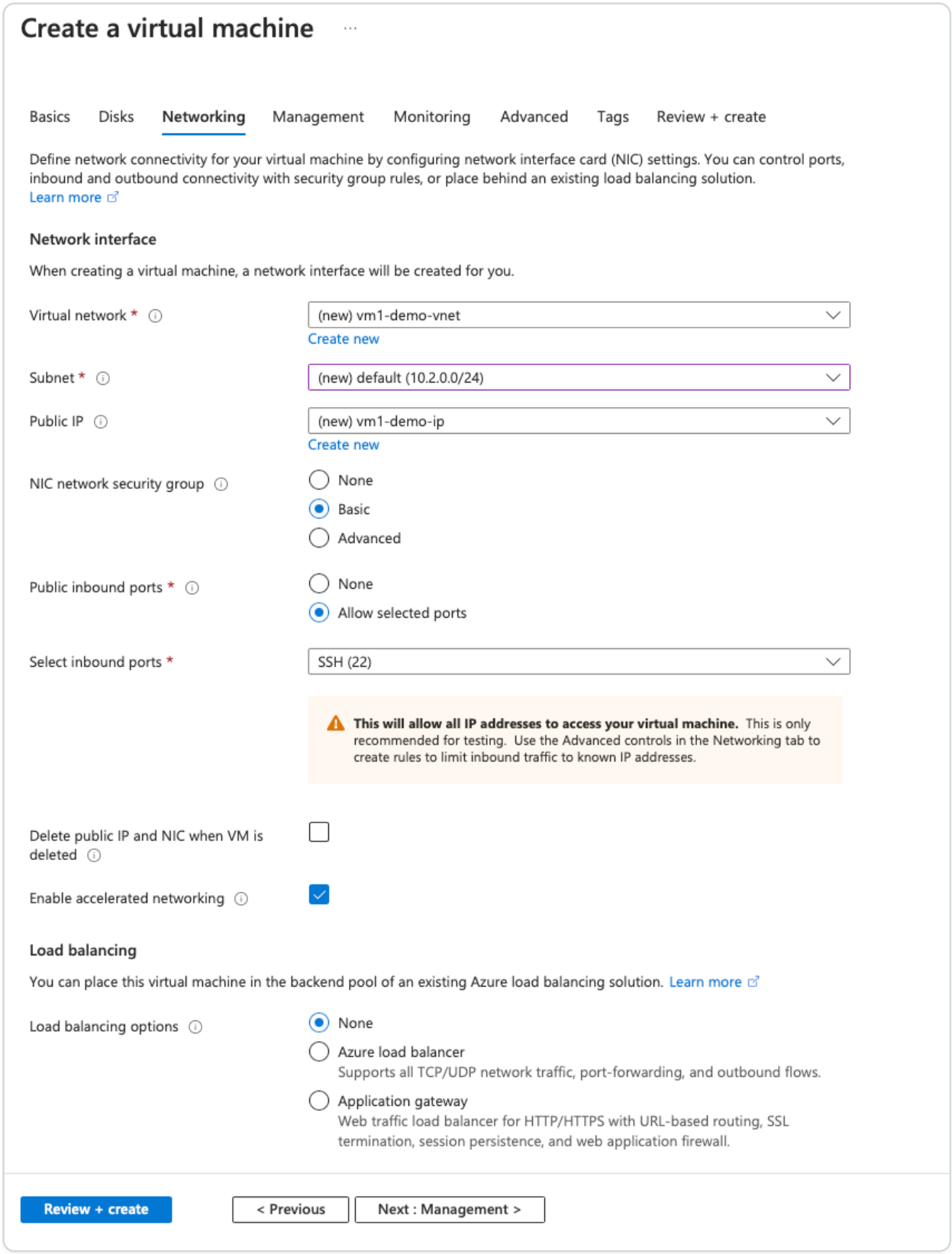
4. 在“**网络**”选项卡中，创建一个包含 3 个子网的新虚拟网络，分别用于：管理、客户端和服务器 NIC。否则，您也可以使用现有的虚拟网络。管理 NIC 在 VM 部署期间创建。客户端和服务器 NIC 在 VM 创建后创建并附加。对于 NIC 网络安全组，您可以执行以下操作之一：

   - 选择“**高级**”并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：

您也可以在 VM 部署完成后更改网络安全组设置。

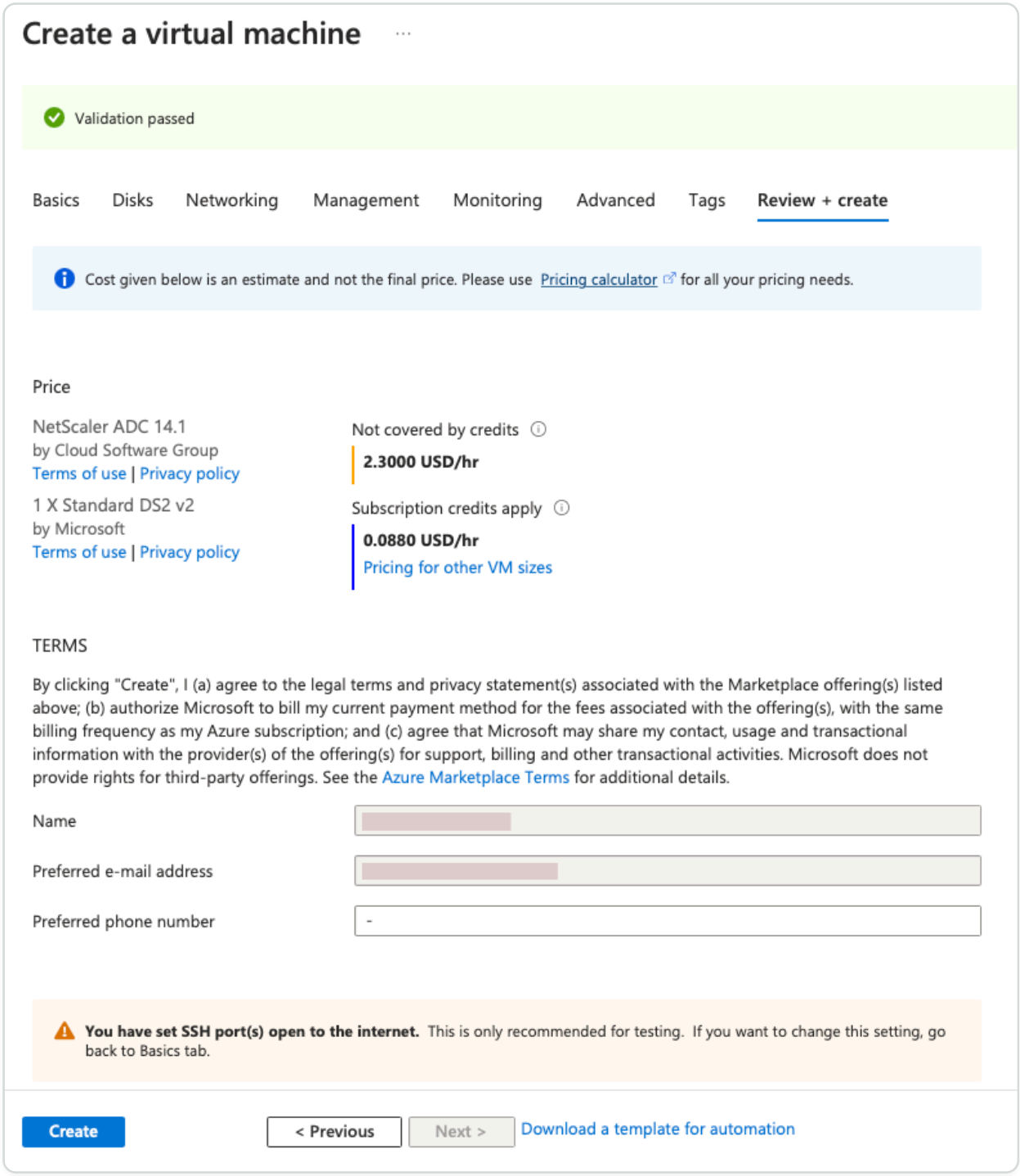
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 单击“下一步：**审核 + 创建 >**”。

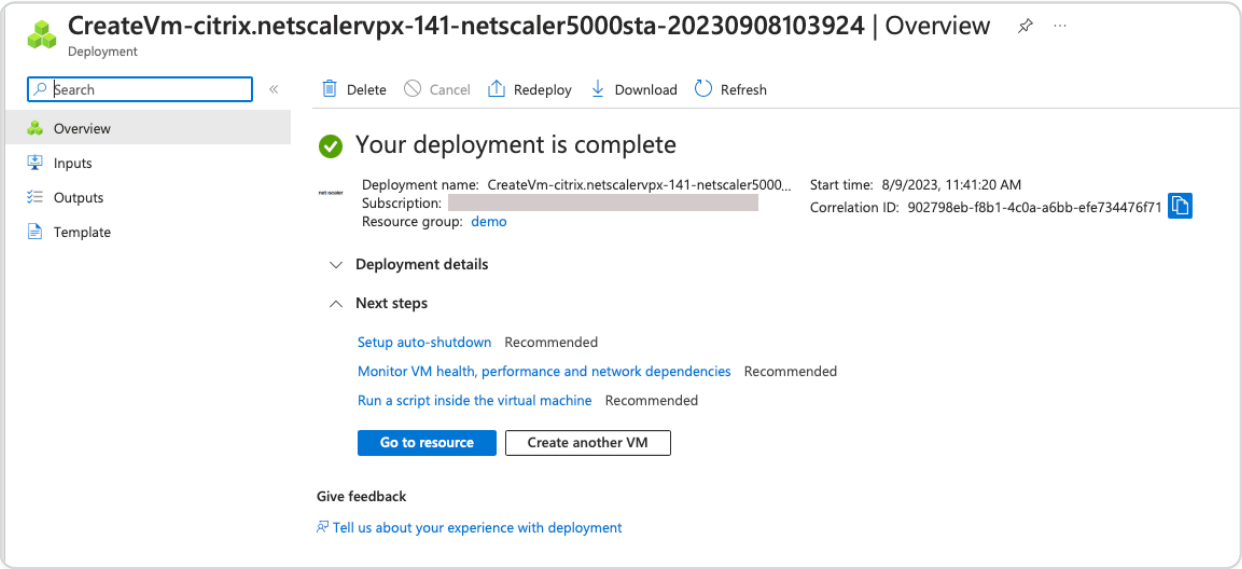
   验证成功后，查看基本设置、VM 配置、网络和附加设置，然后单击“**创建**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 部署完成后，单击“**转到资源**”以查看配置详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



同样，部署第二个 NetScaler VPX 实例。

步骤 2. 在两个实例上添加客户端和服务器 NIC。

注意：

要附加更多 NIC，您必须首先停止 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，请按照以下步骤操作：

1. 导航到“**网络 > 附加网络接口**”。

   您可以选择现有 NIC，也可以创建并附加新接口。

2. 对于 NIC 网络安全组，您可以通过选择“**高级**”来使用现有网络安全组，或者通过选择“**基本**”来创建一个新的网络安全组。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Home > vm1-demo | Networking >

Create network interface ...

Project details

Subscription

NSDev Platform CA anoop.agarwal@citrix.com

Resource group *

demo

Create new

Location

(US) East US

Network interface

Name *

vm1-demo-nic

Virtual network

vm1-demo-vnet

Subnet *

client (10.2.1.0/24)

NIC network security group

- ○ None
- ◉ Basic
- ○ Advanced

Public inbound ports *

- ◉ None
- ○ Allow selected ports

Select inbound ports

Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Private IP address assignment

Dynamic Static

要添加服务器 NIC，请遵循与添加客户端 NIC 相同的步骤。

NetScaler VPX 实例已附加所有三个 NIC（管理 NIC、客户端 NIC 和服务器 NIC）。

对辅助实例重复上述添加 NIC 的步骤。

在两个实例上创建并附加 NIC 后，通过转到“**概述 > 启动**”来重新启动这两个实例。

注意：

您必须允许流量通过客户端 NIC 入站规则中的端口，该端口稍后在配置 NetScaler VPX 实例时用于创建负载平衡虚拟服务器。

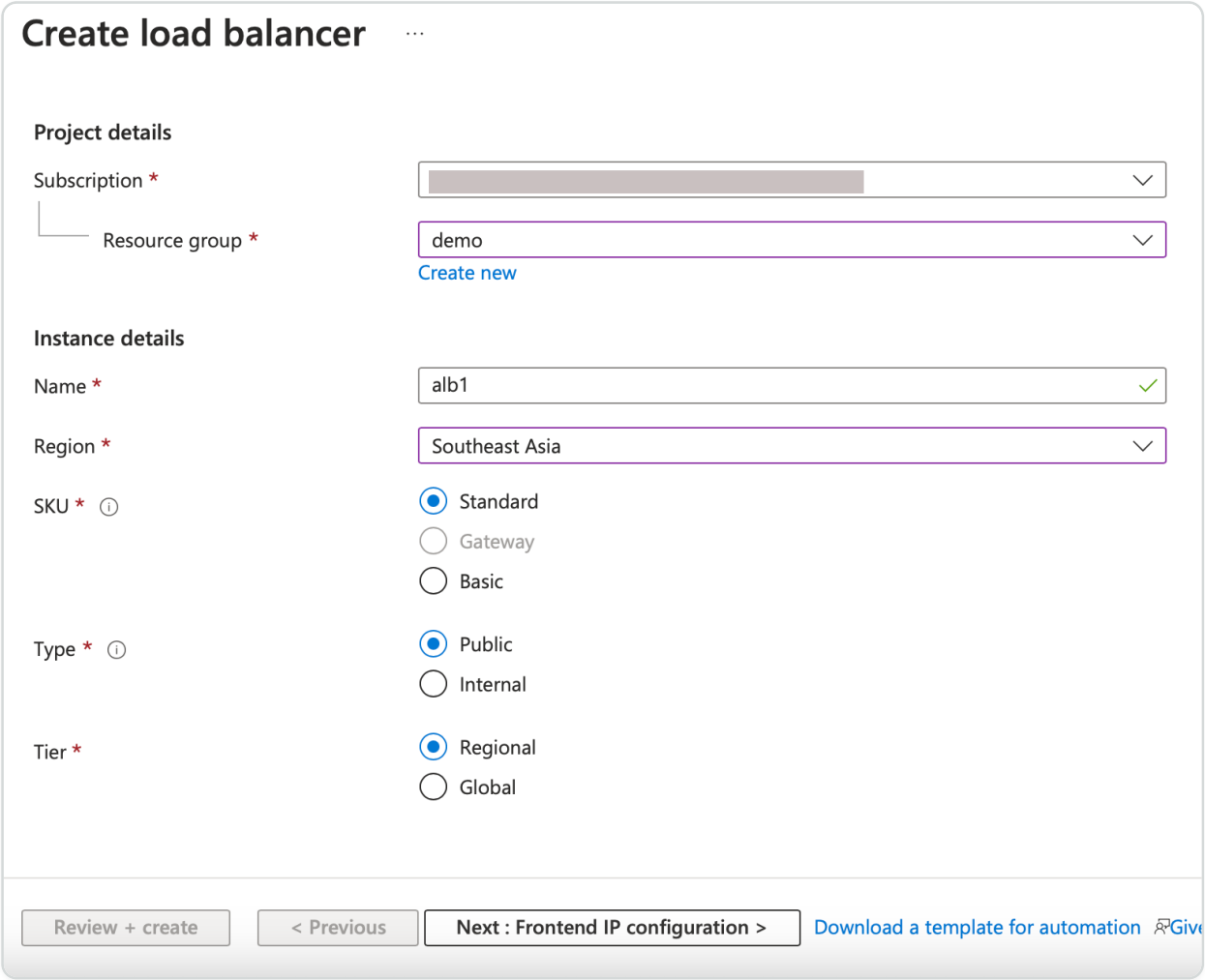
步骤 3. 部署一个 ALB，其负载均衡规则的浮动 IP 模式已禁用。

要开始配置 ALB，请按照以下步骤操作：

1. 转到“**负载均衡器**”页面，然后单击“**创建**”。
2. 在“**创建负载均衡器**”页面中，根据需要提供详细信息。

   在以下示例中，我们部署了一个标准 SKU 的区域公共负载均衡器。

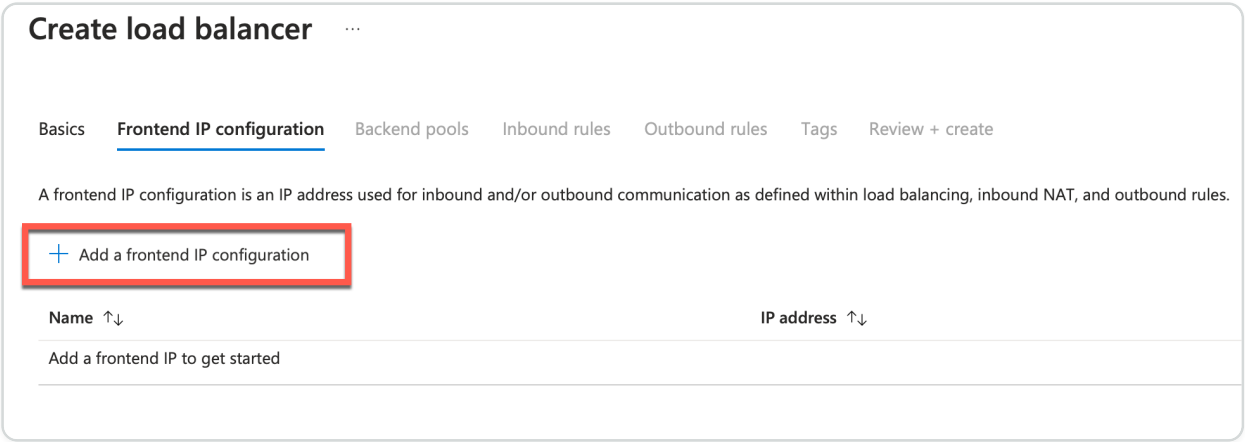
© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

附加到 NetScaler VM 的所有公共 IP 必须与 ALB 具有相同的 SKU。有关 ALB SKU 的更多信息，请参阅 Azure 负载均衡器 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。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add frontend IP configuration

Name *

alb-frontend

IP version

IPv4 IPv6

IP type

IP address IP prefix

Public IP address *

(New) alb-public-ip

Create new

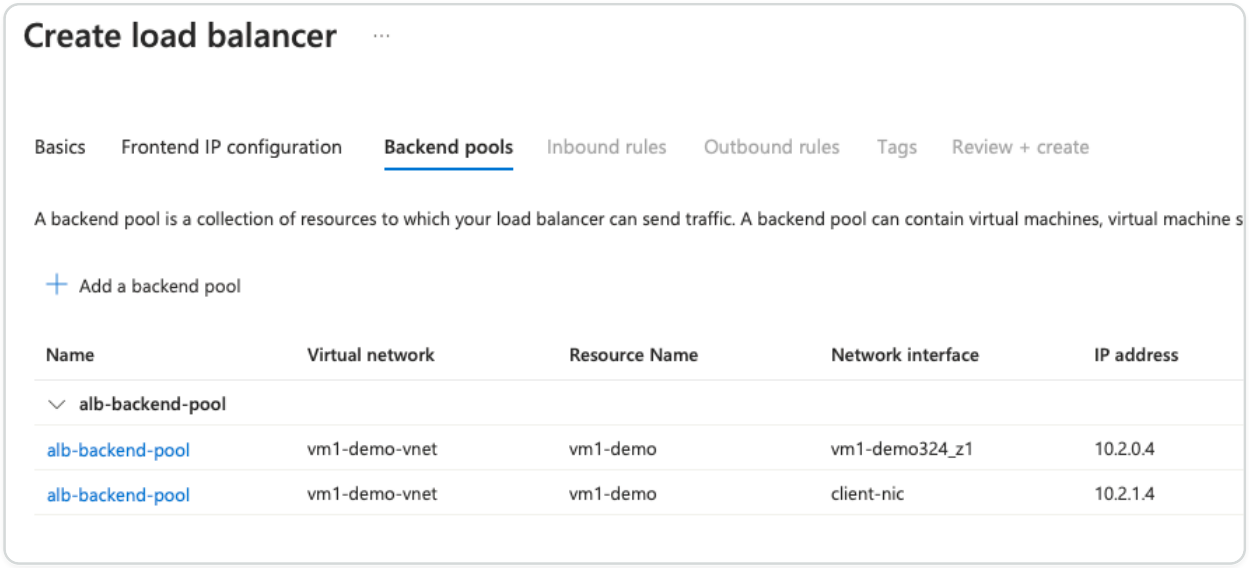
Gateway Load balancer

None

Add

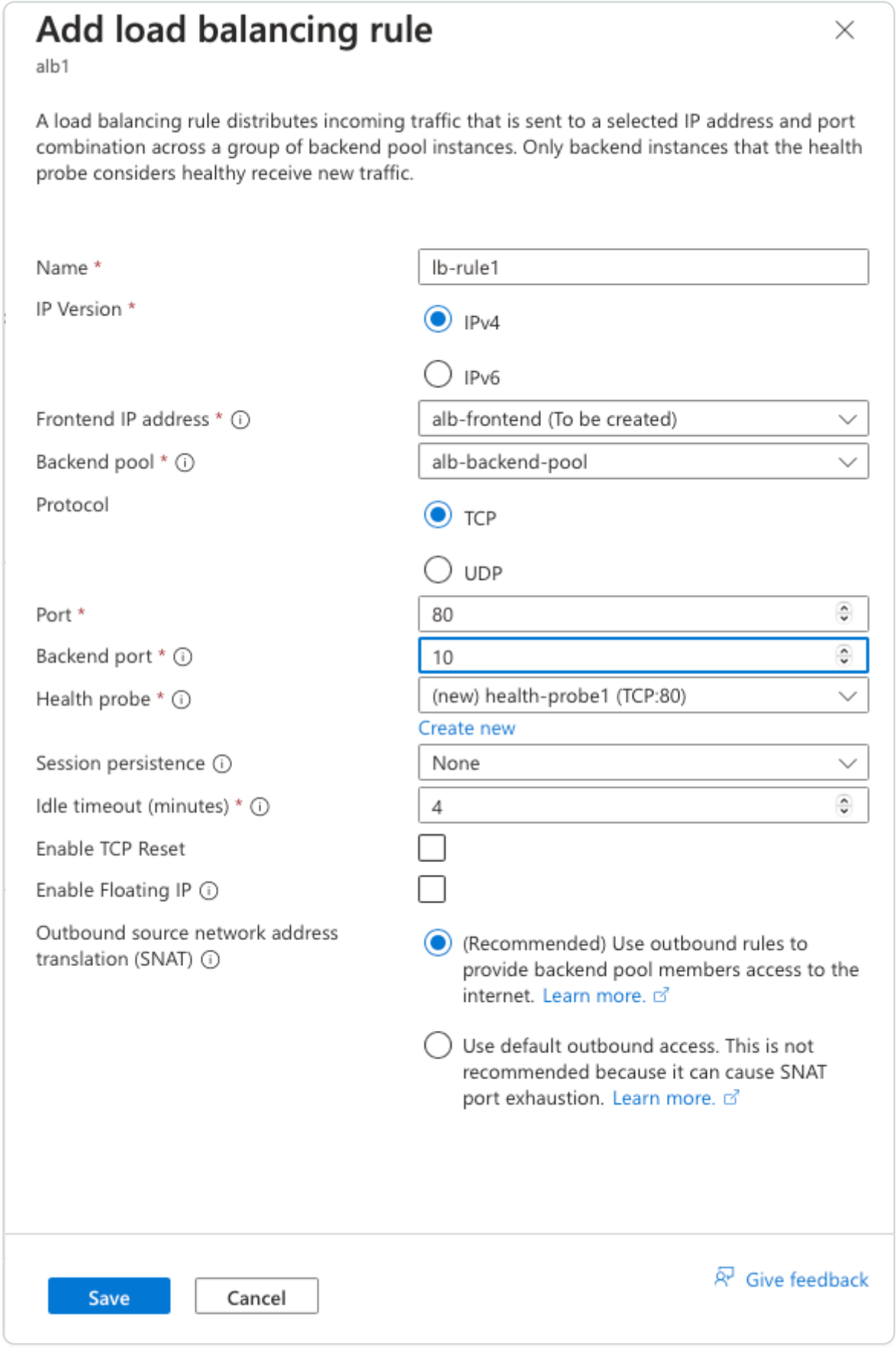
© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 在“**后端池**”选项卡中，选择基于 NIC 的后端池配置，并添加两个 NetScaler VM 的客户端 NIC。



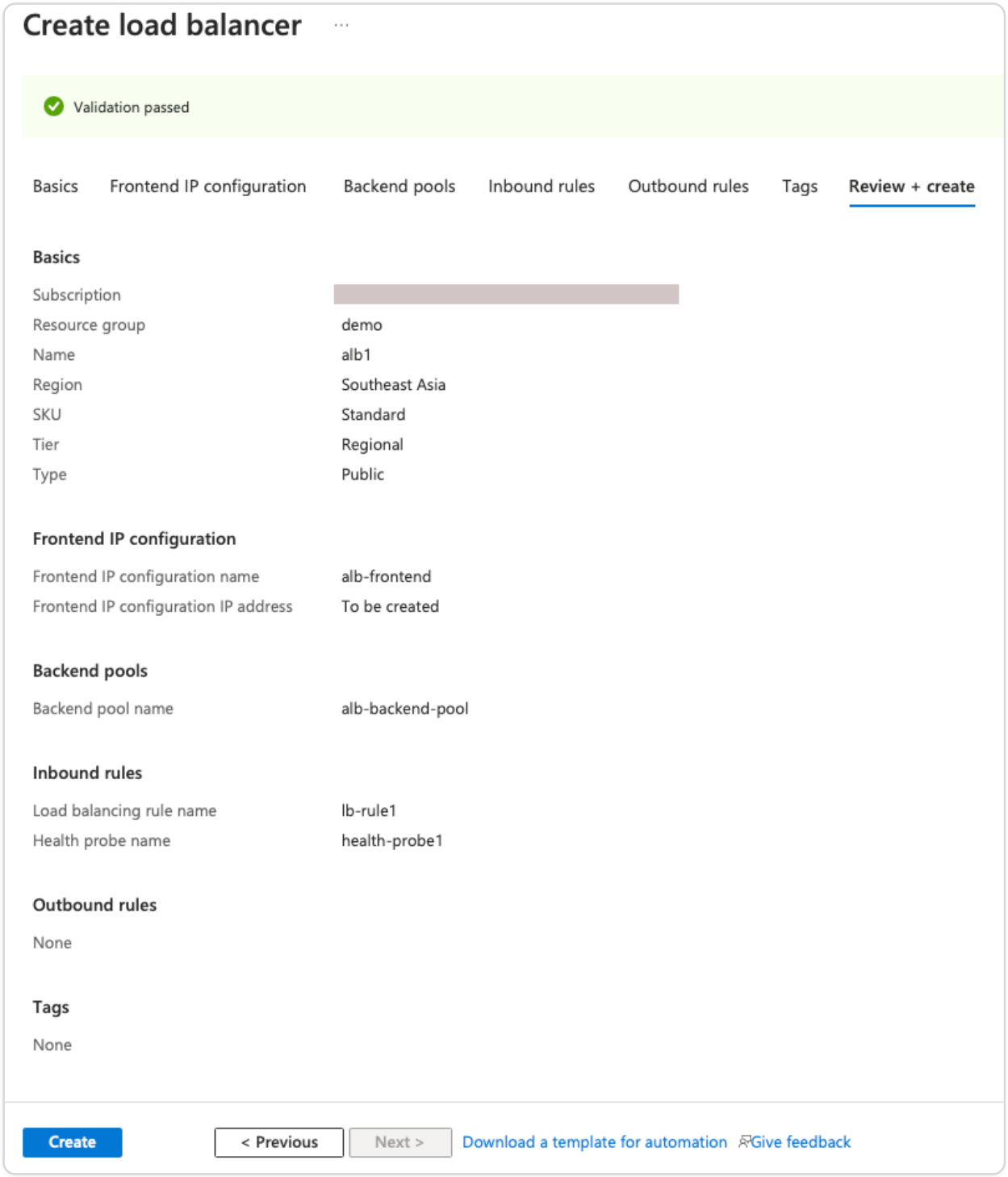
5. 在“**入站规则**”选项卡中，单击“**添加负载均衡规则**”，并提供前面步骤中创建的前端 IP 地址和后端池。根据您的要求选择协议和端口。创建或使用现有运行状况探测。浮动 IP 选项必须设置为“**禁用**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 单击“**审核 + 创建**”。验证通过后，单击“**创建**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



步骤 4. 使用 NetScaler GUI 在两个 NetScaler VPX 实例上配置 HA 设置。

在 Azure 上创建 NetScaler VPX 实例后，您可以使用 NetScaler GUI 配置 HA。

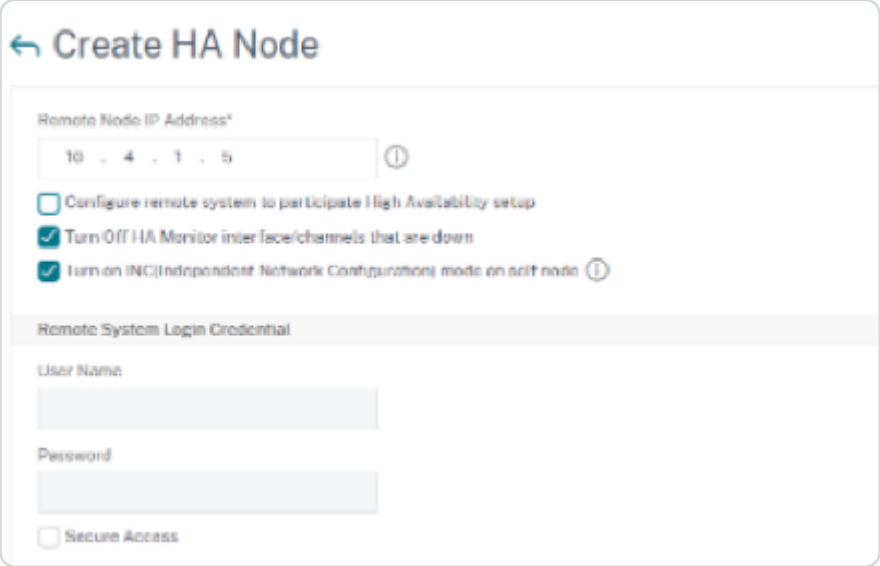
步骤 1. 在两个实例上以 INC 模式设置高可用性。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

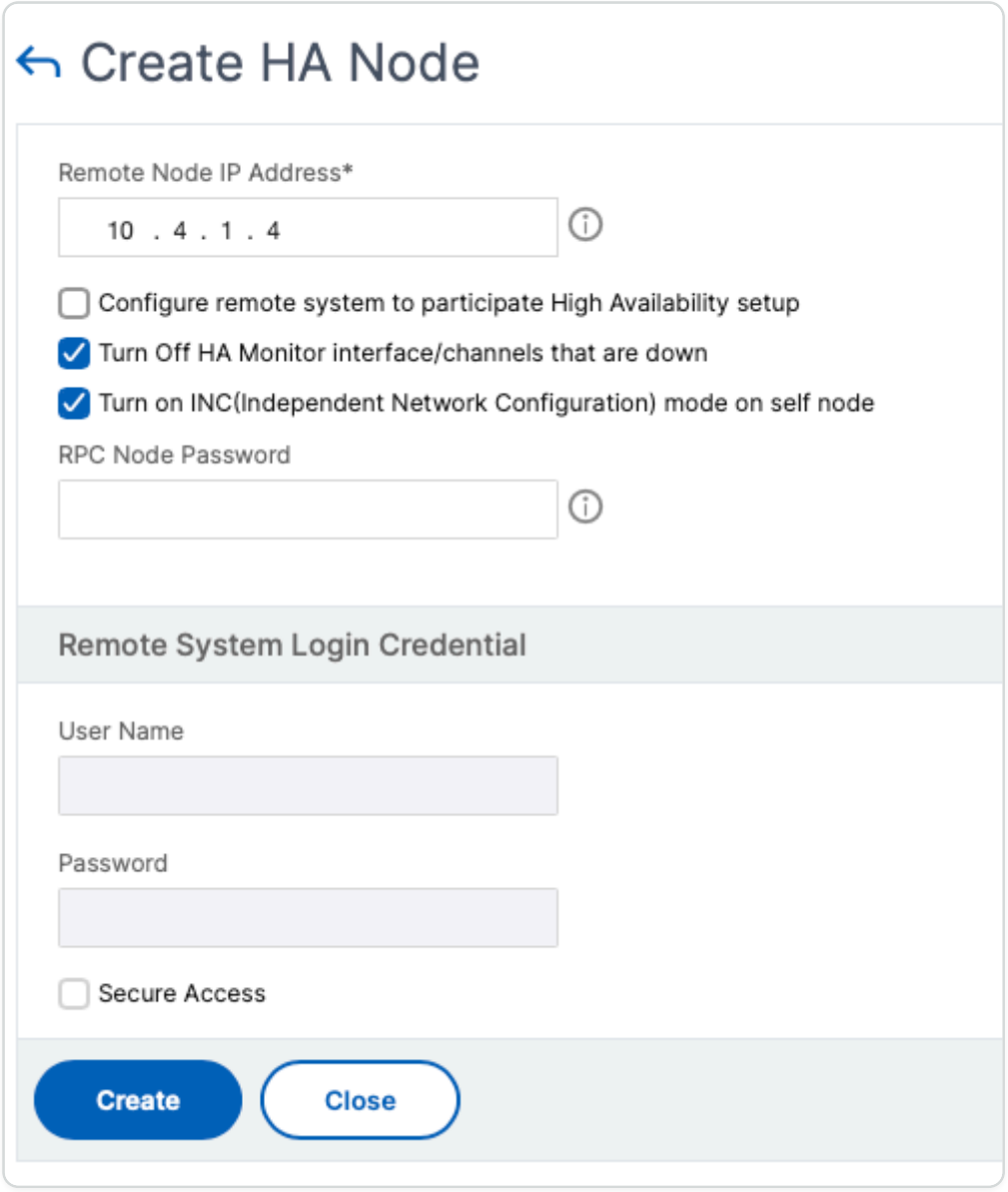
2. 导航到“**Configuration（配置）> System（系统）> High Availability（高可用性）> Nodes（节点）**”，然后单击“**Add（添加）**”。
3. 在“**Remote Node IP address（远程节点 IP 地址）**”字段中，输入辅助实例管理 NIC 的私有 IP 地址，例如：10.4.1.5。
4. 选中“**Turn on INC (Independent Network Configuration) mode on self node（在自节点上启用 INC（独立网络配置）模式）**”复选框。
5. 单击“**创建**”。



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，输入主实例管理 NIC 的私有 IP 地址，例如：10.4.1.4。
4. 选中**在自节点上启用 INC（独立网络配置）模式**复选框。
5. 单击**创建**。

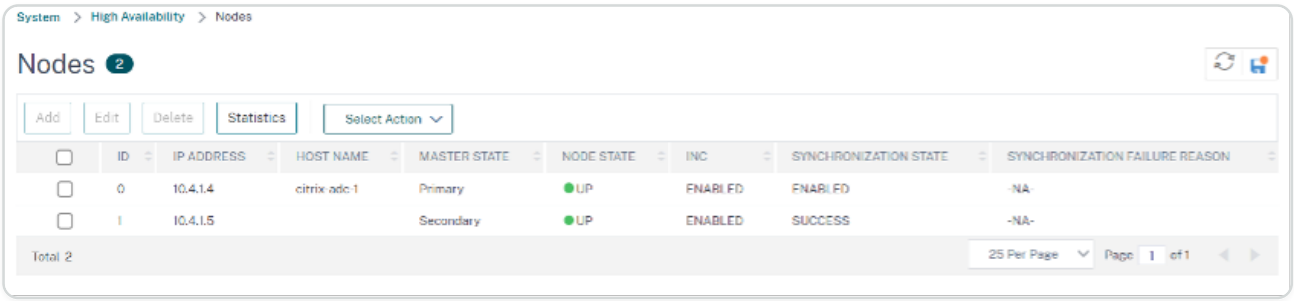
© 1997–2026 Citrix Systems, Inc. All rights reserved.



在继续之前，请确保辅助实例的**同步状态**在**节点**页面中显示为**成功**。

注意：

现在，辅助实例具有与主实例相同的登录凭据。

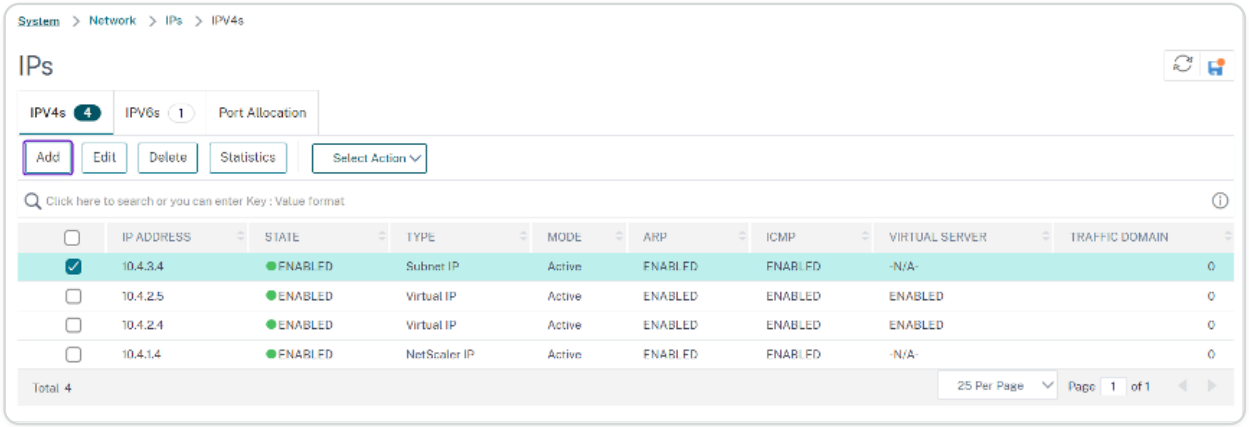


步骤 2. 在两个实例上添加虚拟 IP 地址和子网 IP 地址。

在主实例上，执行以下步骤：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 导航到**系统 > 网络 > IP > IPv4**，然后单击**添加**。
2. 按照以下步骤添加主 VIP 地址：
   a. 输入主实例客户端 NIC 的私有 IP 地址以及在 VM 实例中为客户端子网配置的子网掩码。
   b. 在**IP 类型**字段中，从下拉菜单中选择**虚拟 IP**。
   c. 单击**创建**。
3. 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子网掩码。
   b. 在 **IP 类型**字段中，从下拉菜单中选择 **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 VM 实例中的客户端子网配置的子网掩码。
   b. 在 **IP 类型**字段中，从下拉菜单中选择 **虚拟 IP**。
   c. 单击 **创建**。



在辅助实例上，执行以下步骤：

1. 导航到 **系统 > 网络 > IP > IPv4s**，然后单击 **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 VM 实例中的客户端子网配置的子网掩码。
   b. 在 **IP 类型**字段中，从下拉菜单中选择 **虚拟 IP**。
3. 按照以下步骤添加辅助 SNIP 地址：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 输入辅助实例的服务器网卡内部 IP 地址，以及为辅助实例中的服务器子网配置的子网掩码。

b. 在 **IP 类型** 字段中，从下拉菜单中选择 **子网 IP**。

c. 单击 **创建**。

添加辅助 VIP 和 SNIP(/en-us/vpx/media/alb-floating-ip-secondary-vip-snip.png)

步骤 3. 添加 IP 集并将 IP 集绑定到两个实例上的辅助 VIP。

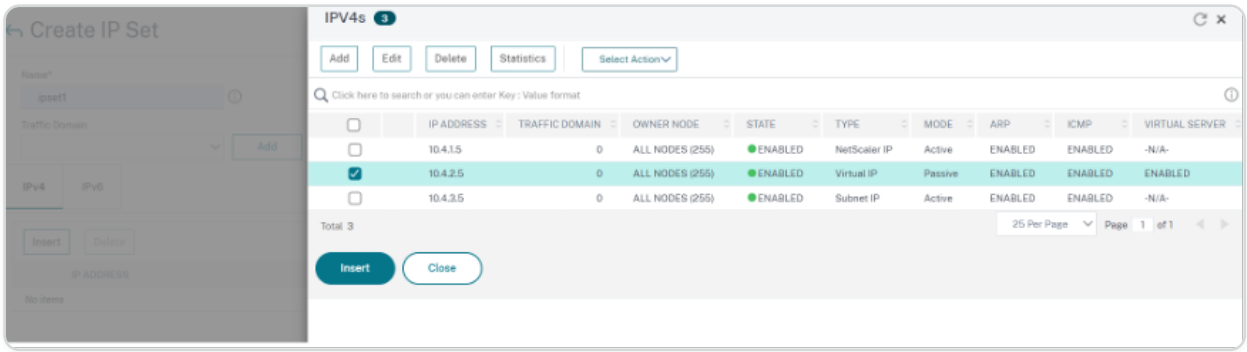
在主实例上，执行以下步骤：

1. 导航到 **系统 > 网络 > IP 集 > 添加**。
2. 添加 IP 集名称并单击 **插入**。
3. 在 **IPV4s** 页面中，选择虚拟 IP（辅助 VIP）并单击 **插入**。
4. 单击 **创建** 以创建 IP 集。

创建主 IP 集(/en-us/vpx/media/alb-floating-ip-create-ip-set.png)

在辅助实例上，执行以下步骤：

1. 导航到 **系统 > 网络 > IP 集 > 添加**。
2. 添加 IP 集名称并单击 **插入**。
3. 在 **IPv4s** 页面中，选择虚拟 IP（辅助 VIP）并单击 **插入**。
4. 单击 **创建** 以创建 IP 集。



注意：

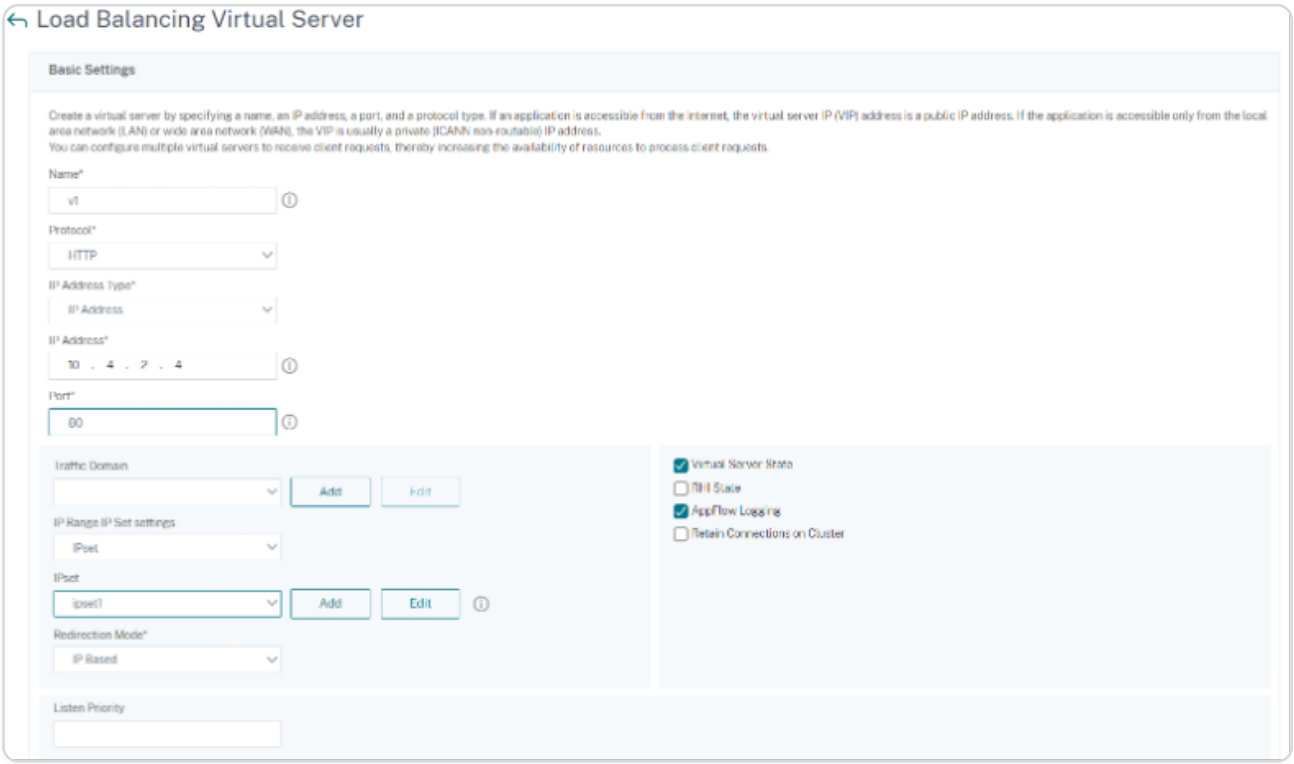
IP 集名称在主实例和辅助实例上必须相同。

步骤 4. 在主实例上添加负载平衡虚拟服务器。

1. 导航到 **配置 > 流量管理 > 负载平衡 > 虚拟服务器 > 添加**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 为名称、协议、IP 地址类型 (IP 地址)、IP 地址 (主 VIP) 和端口添加所需值。
3. 单击 **更多**。导航到 **IP 范围 IP 集设置**，从下拉菜单中选择 **IPset**，并提供在 **步骤 3** 中创建的 IPset。
4. 单击 **确定** 以创建负载平衡虚拟服务器。



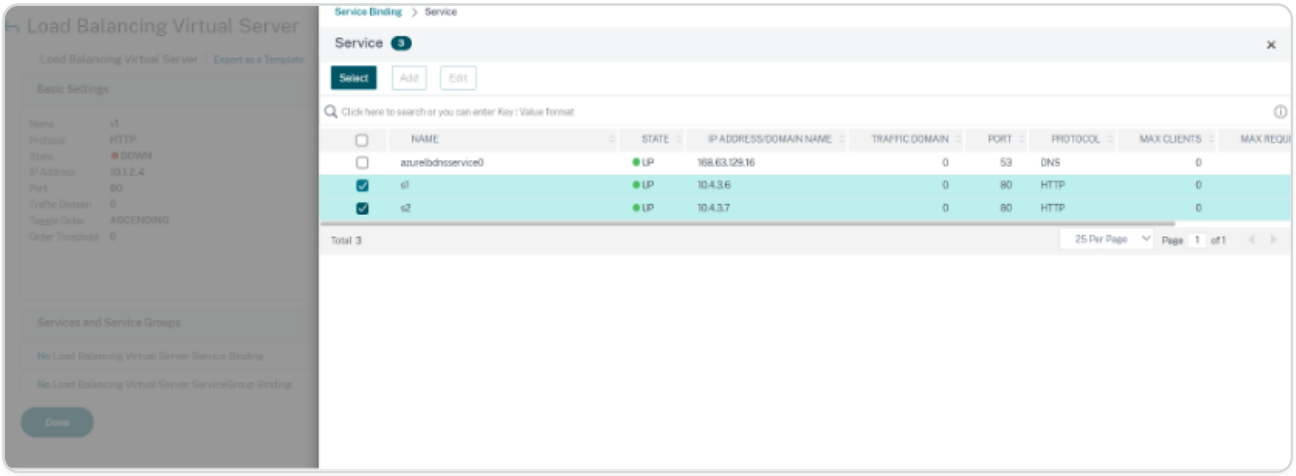
步骤 5. 在主实例上添加服务或服务组。

1. 导航到 **配置 > 流量管理 > 负载平衡 > 服务 > 添加**。
2. 为服务名称、IP 地址、协议和端口添加所需值，然后单击 **确定**。

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 **配置 > 流量管理 > 负载平衡 > 虚拟服务器**。
2. 选择在 **步骤 4** 中配置的负载均衡虚拟服务器，然后单击 **编辑**。
3. 在 **服务和服务器组** 选项卡中，单击 **无负载均衡虚拟服务器服务绑定**。
4. 选择在 **步骤 5** 中配置的服务，然后单击 **绑定**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



步骤 7. 保存配置。

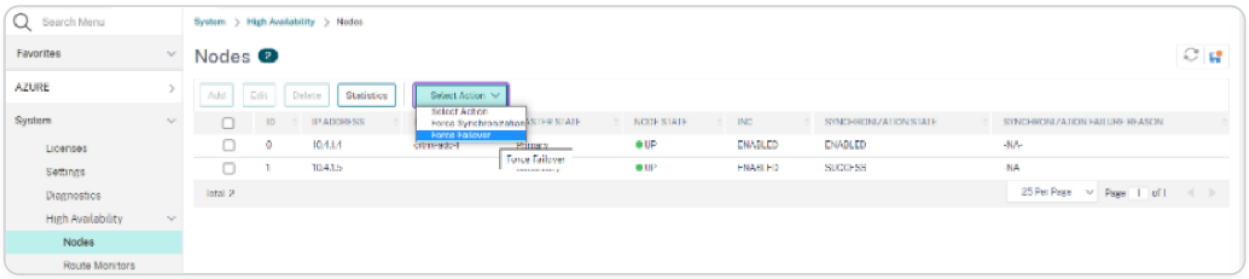
否则，在重新启动或即时重启后，所有配置都将丢失。

步骤 8. 验证配置。

确保在故障转移后 ALB 前端 IP 地址可访问。

1. 复制 ALB 前端 IP 地址。
2. 在浏览器中粘贴 IP 地址，并确保后端服务器可访问。
3. 在主实例上，执行故障转移：

   从 NetScaler GUI，导航到 **配置 > 系统 > 高可用性 > 操作 > 强制故障转移**。



4. 确保在故障转移后，通过之前使用的 ALB 前端 IP，后端服务器可访问。

配置 NetScaler VPX 实例以使用 Azure 加速网络

加速网络使单根 I/O 虚拟化 (SR-IOV) 虚拟功能 (VF) NIC 能够连接到虚拟机，从而提高网络性能。您可以在需要以更高吞吐量发送或接收数据、具有可靠流式传输和更低 CPU 利用率的繁重工作负载中使用此功能。 当 NIC 启用加速网络时，Azure 会将 NIC 现有的半虚拟化 (PV) 接口与 SR-IOV VF 接口捆绑在一起。对 SR-IOV VF 接口的支持可启用并增强 NetScaler VPX 实例的吞吐量。

加速网络提供以下优势：

- 更低的延迟

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 更高的每秒数据包 (pps) 性能
- 增强的吞吐量
- 减少抖动
- 降低 CPU 利用率

注意：

从版本 13.0 build 76.29 开始，NetScaler VPX 实例支持 Azure 加速网络。

先决条件

- 确保您的 VM 大小符合 Azure 加速网络的要求。
- 在任何 NIC 上启用加速网络之前，请停止 VM（单个或可用性集中的 VM）。

限制

加速网络只能在某些实例类型上启用。有关更多信息，请参阅 支持的实例类型。

支持加速网络的网卡

Azure 提供 SR-IOV 模式的 Mellanox ConnectX3、ConnectX4 和 ConnectX5 网卡，用于加速网络。

当在 NetScaler VPX 接口上启用加速网络时，Azure 会将 ConnectX3、ConnectX4 或 ConnectX5 接口与 NetScaler VPX 设备现有的 PV 接口捆绑在一起。

注意：

NetScaler VPX 从 13.1 build 37.x 版本开始支持 ConnectX5 网卡。

有关在将接口附加到 VM 之前启用加速网络的更多信息，请参阅 创建具有加速功能的网络接口。

有关在 VM 上现有接口上启用加速网络的更多信息，请参阅 在 VM 上启用现有接口。

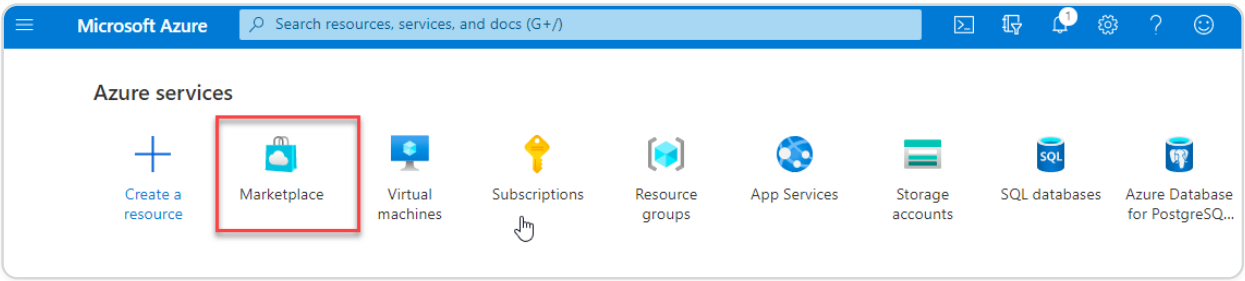
如何使用 Azure 控制台在 NetScaler VPX 实例上启用加速网络

您可以使用 Azure 控制台或 Azure PowerShell 在特定接口上启用加速网络。

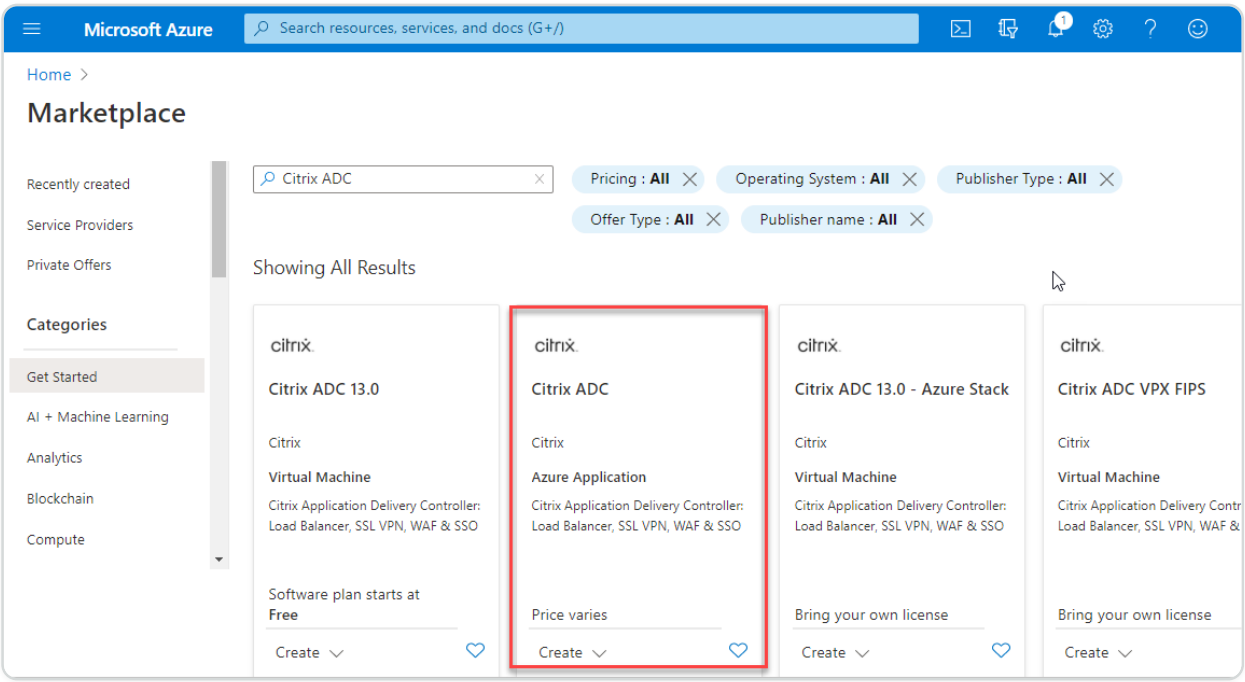
执行以下步骤，通过使用 Azure 可用性集或可用性区域来启用加速网络。

1. 登录 Azure 门户，然后导航到 **Azure 应用商店**。

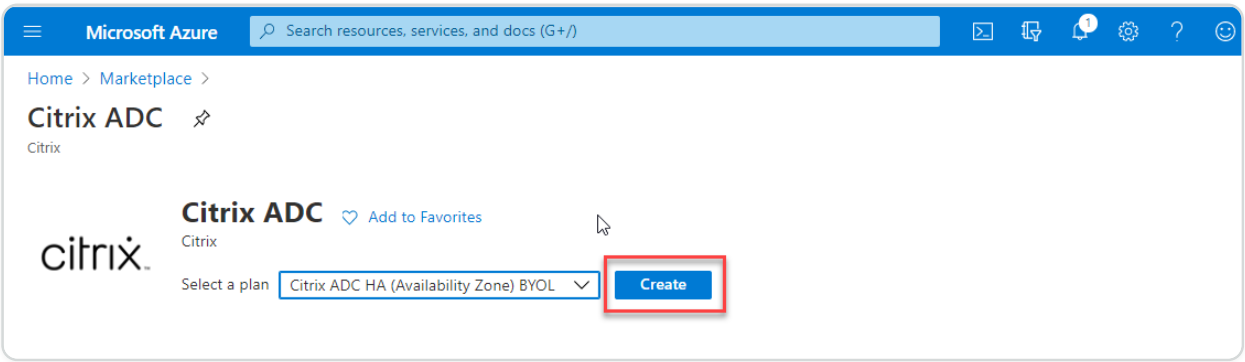
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 在 **Azure 应用商店**中，搜索 **NetScaler**。



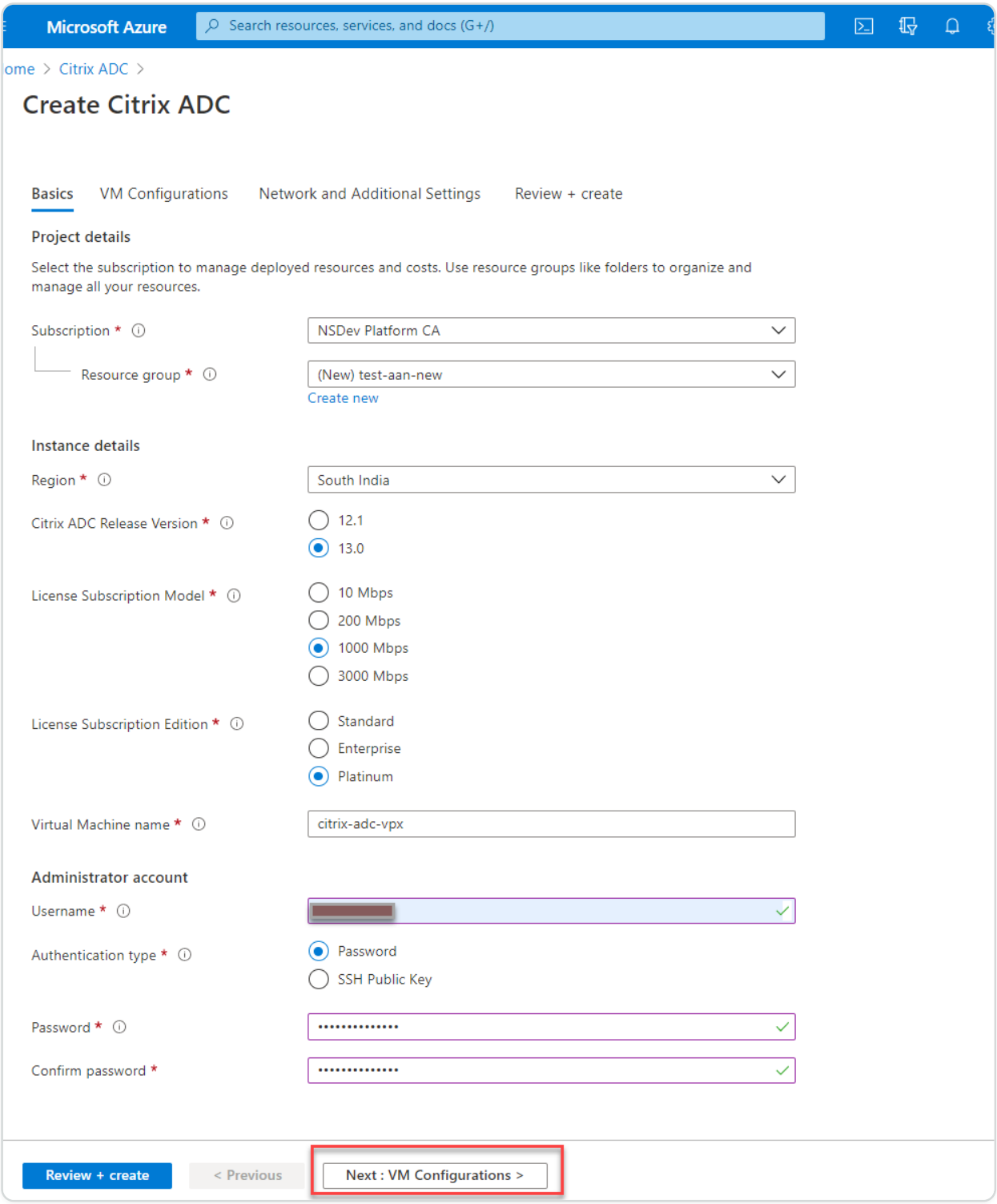
3. 选择一个非 FIPS 的 NetScaler 计划以及许可证，然后单击“**创建**”。



随即显示**创建 NetScaler**页面。

4. 在**基本信息**选项卡中，创建资源组。在**参数**选项卡下，输入区域、管理员用户名、管理员密码、许可证类型 (VM SKU) 和其他字段的详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 单击**下一步：VM 配置 >**。

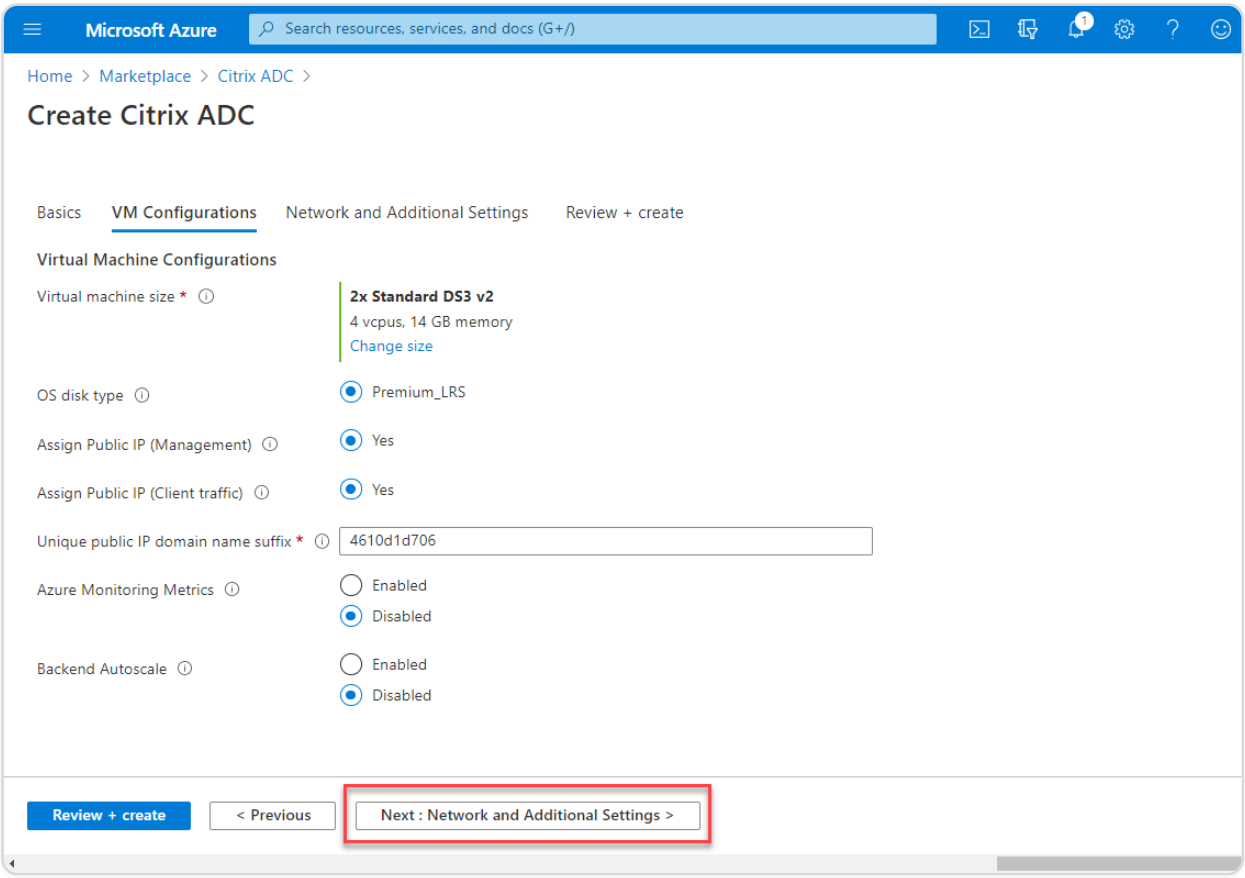
   在**VM 配置**页面上，执行以下操作：

   a. 配置公共 IP 域名后缀。

   b. 启用或禁用**Azure 监视指标**。

   c. 启用或禁用**后端自动缩放™**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

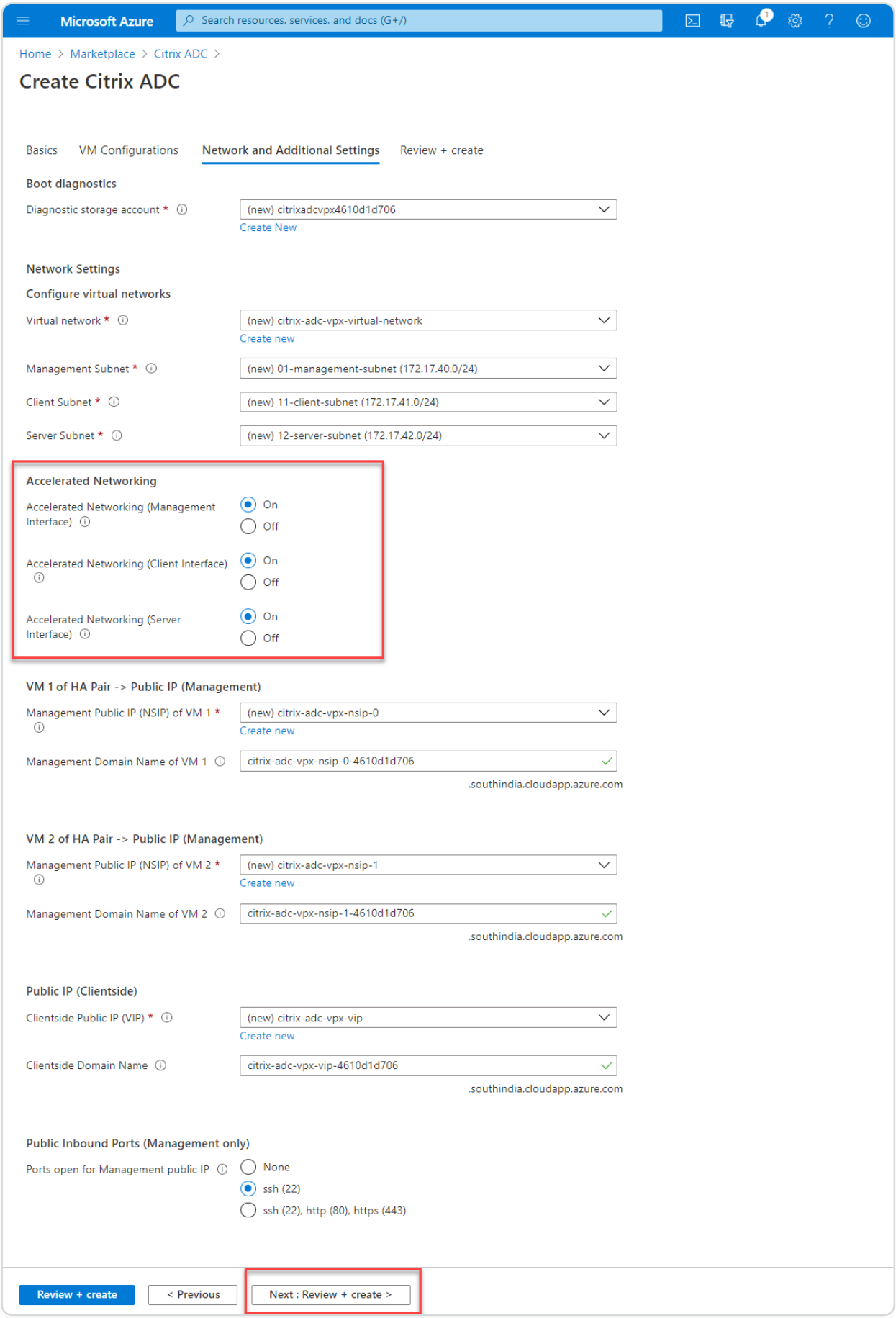


6. 单击**下一步：网络和附加设置 >**。

   在**网络和附加设置**页面上，创建启动诊断帐户并配置网络设置。

   在**加速网络**部分下，您可以选择分别为管理接口、客户端接口和服务器接口启用或禁用加速网络。

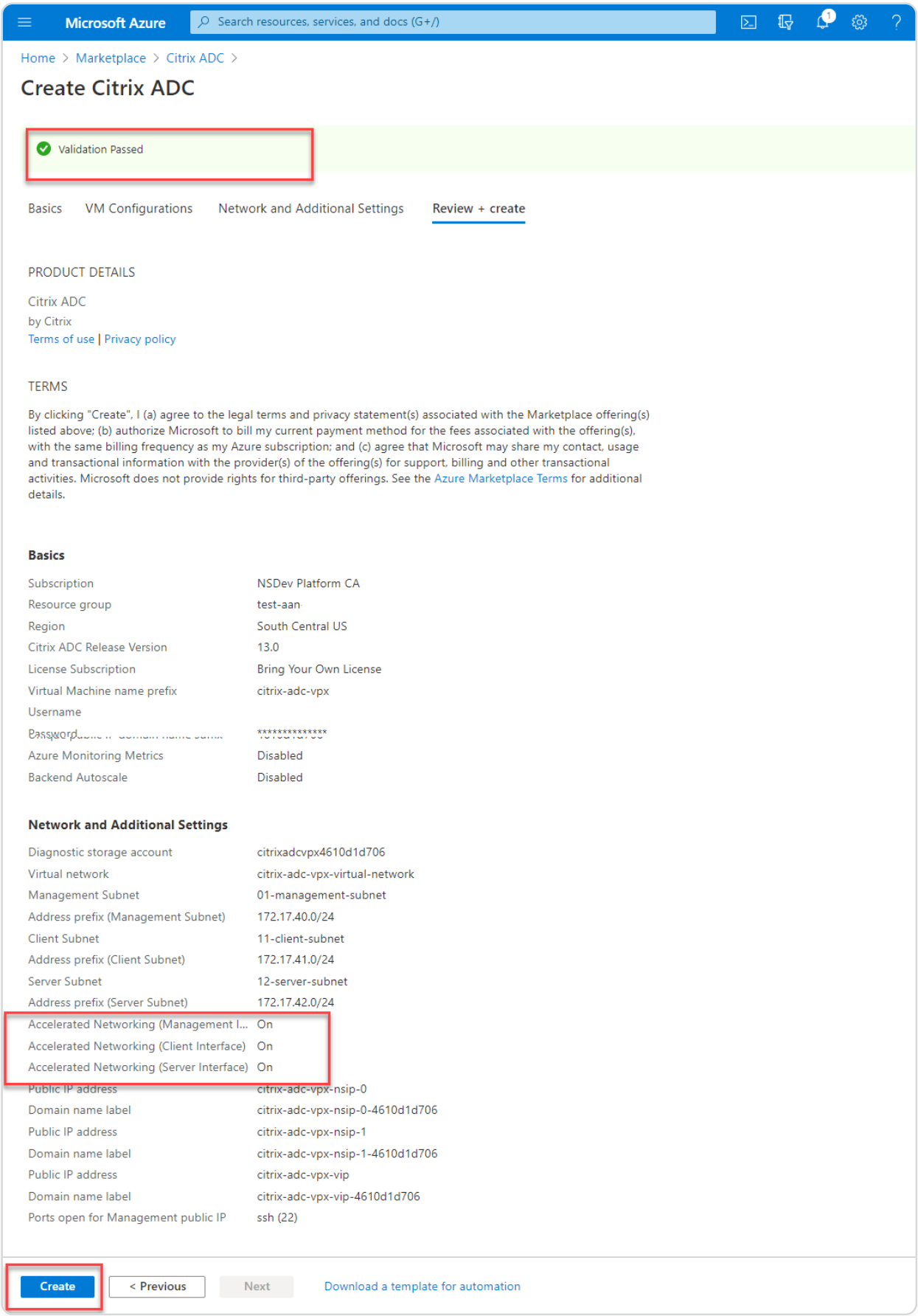
© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. 单击**下一步：审核 + 创建 >**。

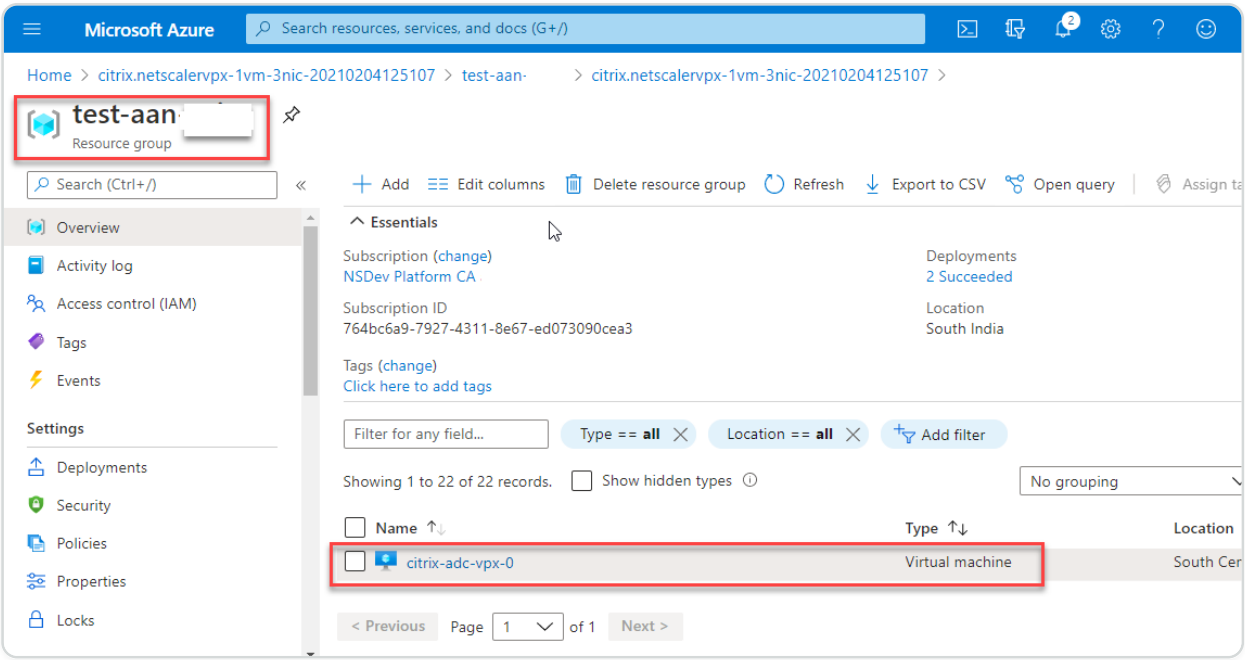
© 1997–2026 Citrix Systems, Inc. All rights reserved.

验证成功后，查看基本设置、VM 配置、网络和附加设置，然后单击**创建**。Azure 资源组可能需要一些时间才能使用所需配置创建成功。

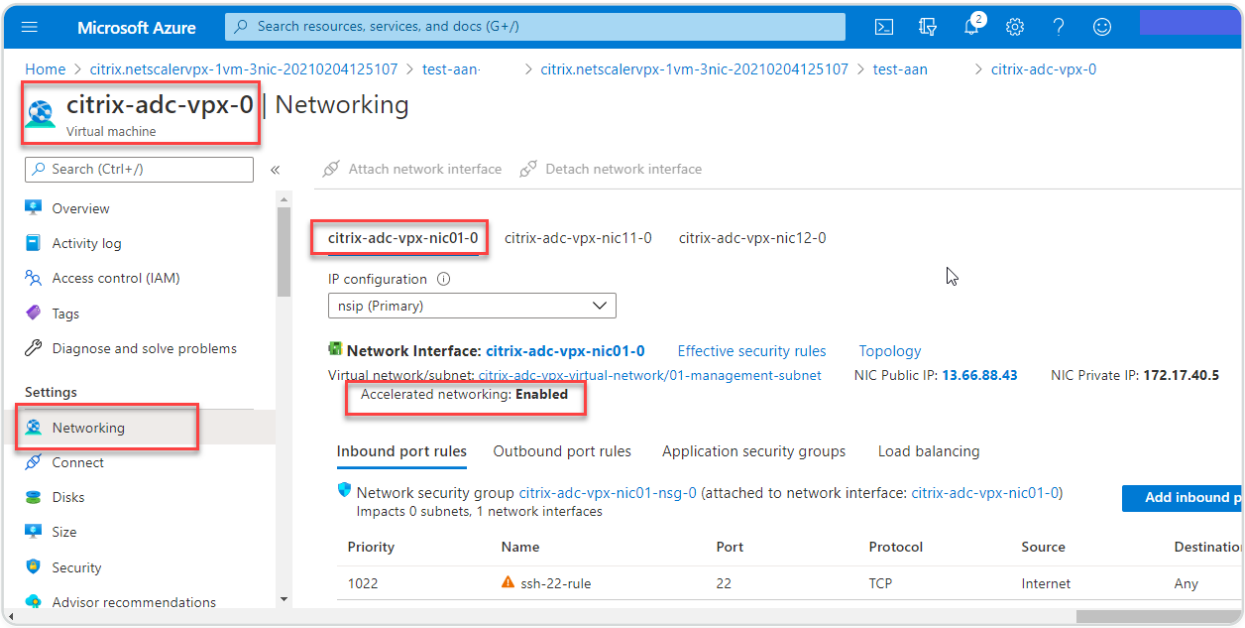


© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. 部署完成后，选择**资源组**以查看配置详细信息。



9. 要验证加速网络配置，请选择**虚拟机 > 网络**。每个 NIC 的加速网络状态显示为**已启用**或**已禁用**。



使用 Azure PowerShell 启用加速网络

如果在创建 VM 后需要启用加速网络，可以使用 Azure PowerShell 来完成。

注意：

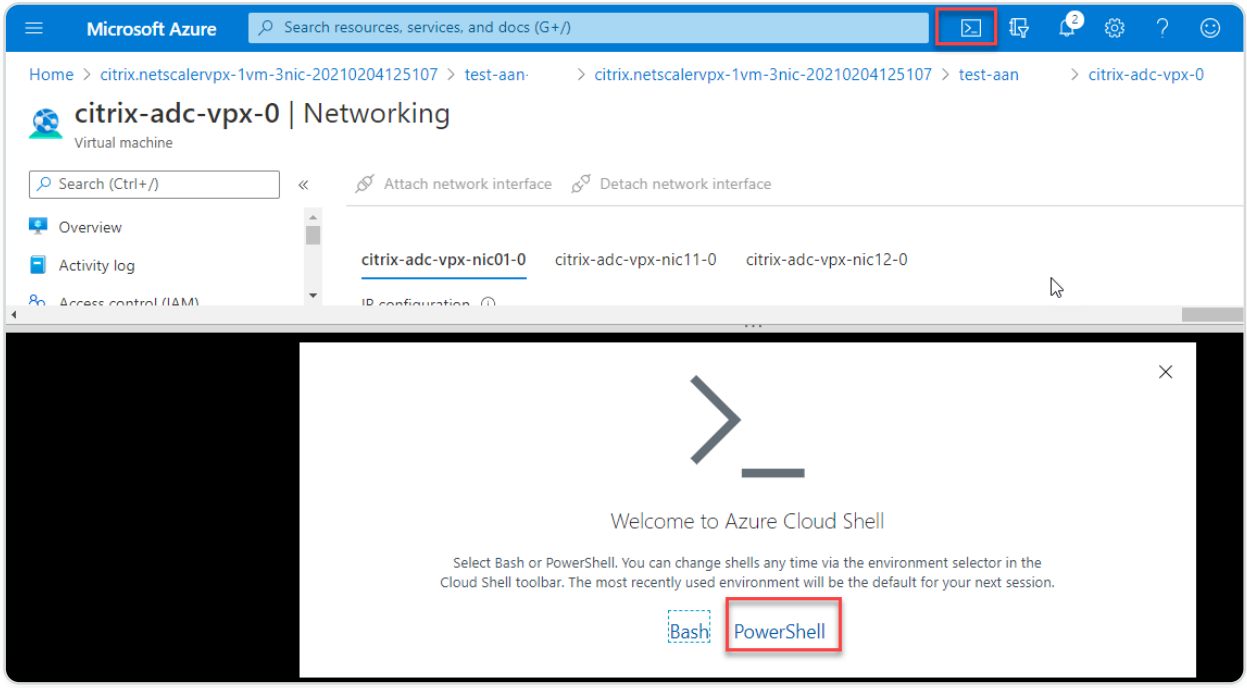
在使用 Azure PowerShell 启用加速网络之前，请务必停止 VM。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

执行以下步骤以使用 Azure PowerShell 启用加速网络。

1. 导航到 **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>
```

加速网络参数接受以下任一值：

- **True**： 在指定的 NIC 上启用加速网络。
- **False**： 在指定的 NIC 上禁用加速网络。

在特定 NIC 上启用加速网络：

```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-
networking true --resource-group rsgp1-aan
```

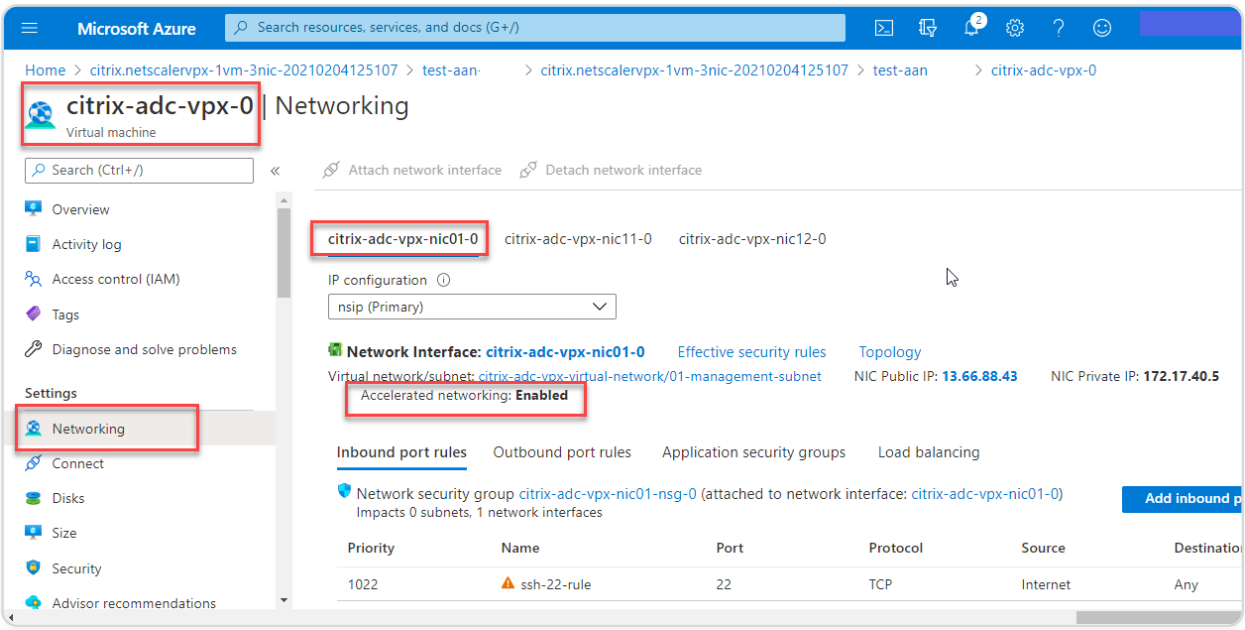
在特定 NIC 上禁用加速网络：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

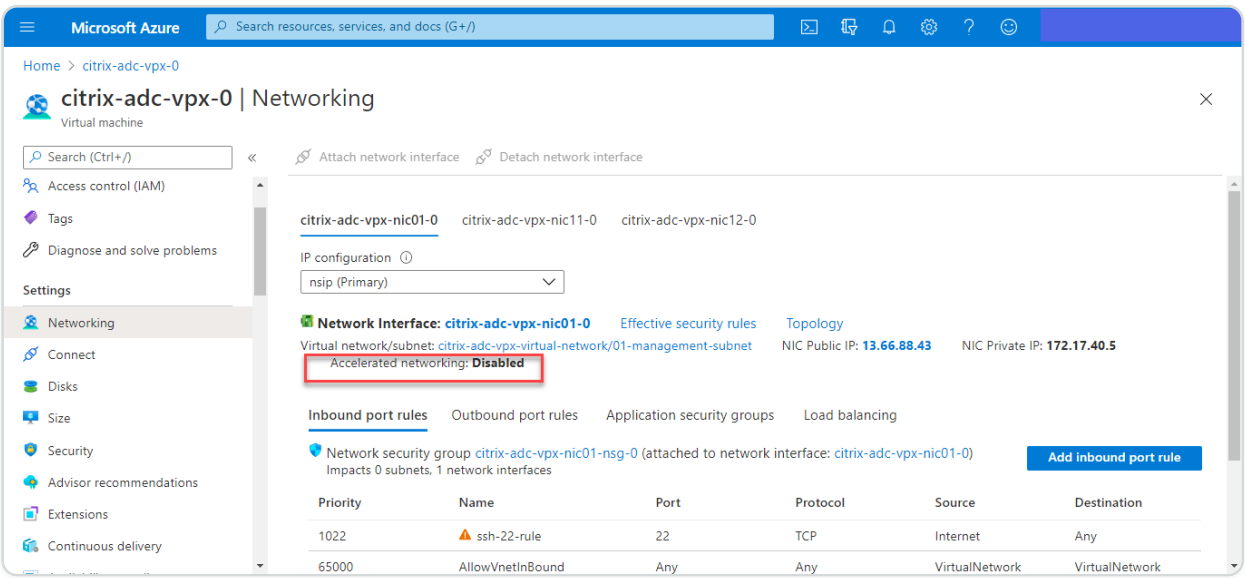
```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-
networking false --resource-group rsgp1-aan
```

3. 要验证部署完成后加速网络的状态，请导航到 **VM > Networking**。

   在以下示例中，您可以看到加速网络已**启用**。



   在以下示例中，您可以看到加速网络已**禁用**。



使用 NetScaler 的 FreeBSD Shell 验证接口上的加速网络

您可以登录到 NetScaler 的 FreeBSD shell，并运行以下命令来验证加速网络状态。

ConnectX3 NIC 示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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)。这表明这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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(1/1) 和 CX4 VF 接口 (100/1) 具有相同的 MAC 地址 (00:0d:3a:9b:f2:1d)。这表明这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 验证接口上的加速网络

ConnectX3 NIC 示例：

以下 show interface 命令输出表明 PV 接口 1/1 与虚拟功能 50/1 捆绑在一起，后者是 SR-IOV VF NIC。1/1 和 50/1 NIC 的 MAC 地址相同。启用加速网络后，1/1 接口的数据通过 50/1 接口（ConnectX3 接口）的数据路径发送。您可以看到 PV 接口 (1/1) 的“show interface”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)。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> 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 示例：

以下 show interface 命令输出表明 PV 接口 1/1 与虚拟功能 100/1 捆绑在一起，后者是 SR-IOV VF NIC。1/1 和 100/1 NIC 的 MAC 地址相同。启用加速网络后，1/1 接口的数据通过 100/1 接口（ConnectX4 接口）的数据路径发送。您可以看到 PV 接口 (1/1) 的“show interface”输出指向 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler 中的注意事项

- PV 接口被视为所有必要操作的主接口。配置只能在 PV 接口上执行。
- VF 接口上的所有“set”操作均被阻止，以下情况除外：
  - 启用接口
  - 禁用接口
  - 重置接口
  - 清除统计信息

> **注意：**
>
> Citrix® 建议您不要对 VF 接口执行任何操作。

- 您可以使用 `show interface` 命令验证 PV 接口与 VF 接口的绑定。
- 从 NetScaler 13.1-33.x 版本开始，NetScaler VPX 实例可以无缝处理 Azure 加速网络中 NIC 的动态移除和重新连接。Azure 可以为了主机维护活动而移除加速网络的 SR-IOV VF NIC。每当 NIC 从 Azure VM 中移除时，NetScaler VPX 实例会将接口状态显示为“链路断开”，并且流量仅通过虚拟接口传输。移除的 NIC 重新连接后，VPX 实例将使用重新连接的 SR-IOV VF NIC。此过程是无缝的，不需要任何配置。

将 VLAN 配置到 PV 接口

当 PV 接口绑定到 VLAN 时，关联的加速 VF 接口也会绑定到与 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) 捆绑的 VF 接口 (100/1) 也绑定到 VLAN 20。

示例：

1. 创建 VLAN。

```
add vlan 20
```

2. 将 VLAN 绑定到 PV 接口。

```
bind vlan 20 –ifnum 1/1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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 VF 接口上执行 VLAN 绑定操作。

```
bind vlan 1 -ifnum 100/1

ERROR: Operation not permitted
```

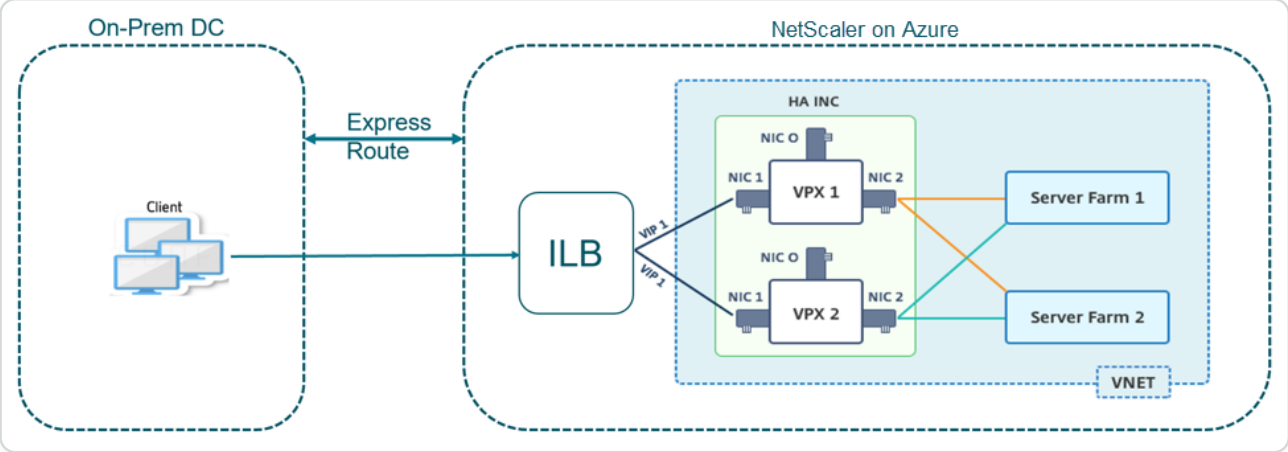
使用 NetScaler® 高可用性模板和 Azure ILB 配置 HA-INC 节点

您可以使用用于内部网应用程序的标准模板，以 HA-INC 模式快速高效地部署一对 VPX 实例。Azure 内部负载均衡器 (ILB) 使用内部或专用 IP 地址作为前端，如图 1 所示。该模板创建两个节

© 1997–2026 Citrix Systems, Inc. All rights reserved.

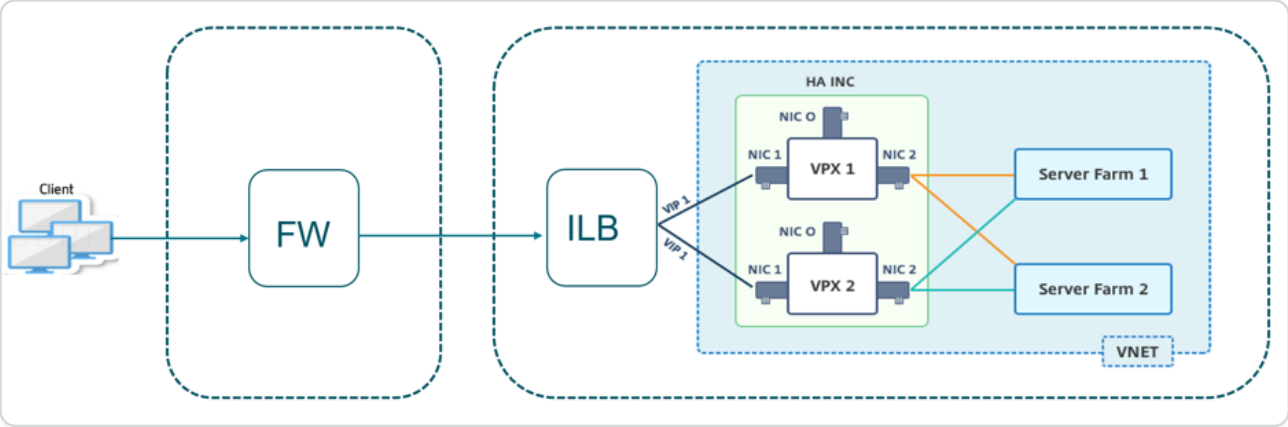
点，具有三个子网和六个 NIC。这些子网分别用于管理、客户端和服务器端流量，每个子网属于每个设备上的不同 NIC。

图 1：内部网络中客户端的 NetScaler HA 对



当 NetScaler HA 对位于防火墙后面时，您也可以使用此部署，如图 2 所示。公共 IP 地址属于防火墙，并 NAT 到 ILB 的前端 IP 地址。

图 2：具有公共 IP 地址的防火墙的 NetScaler HA 对

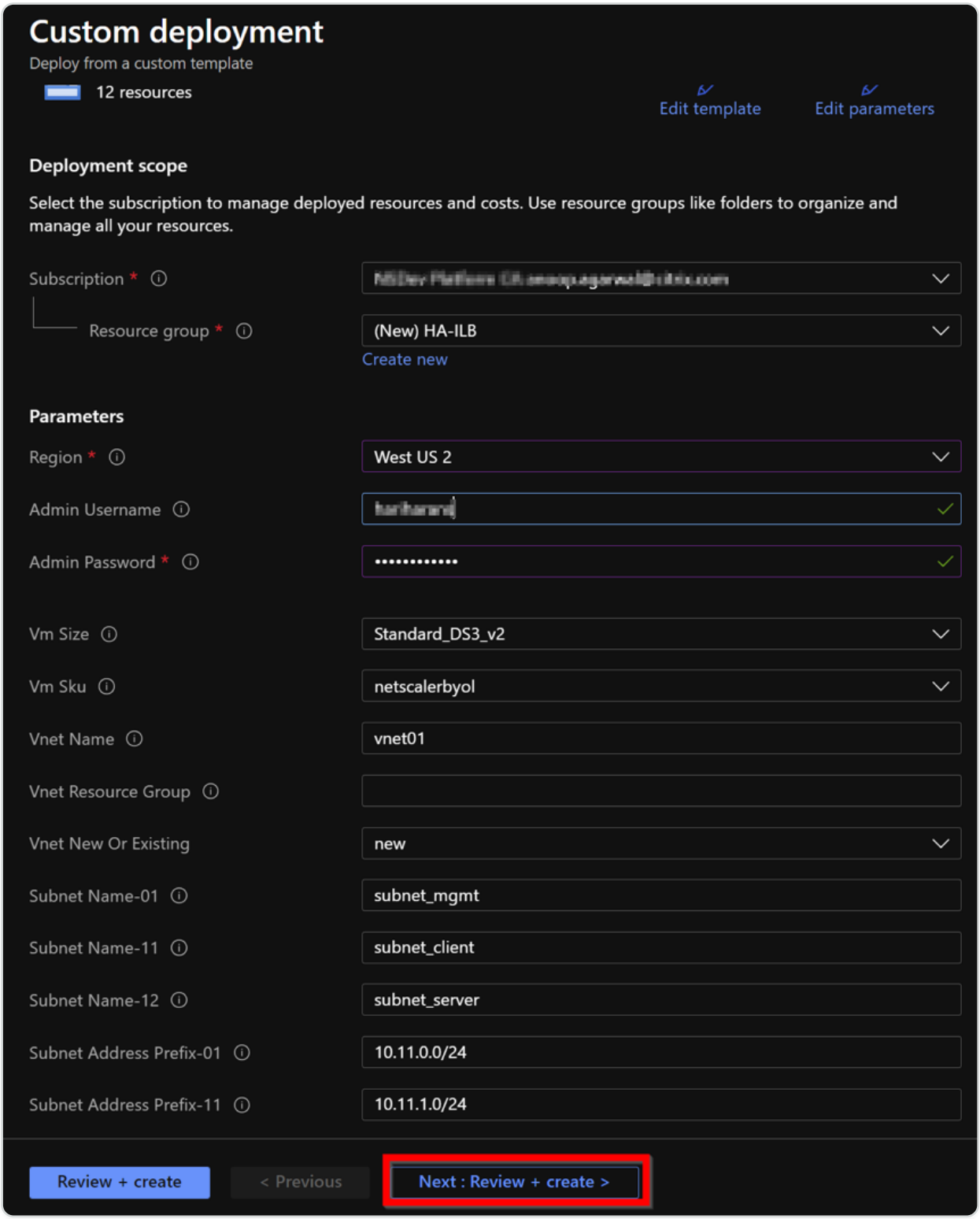


您可以在 Azure 门户 获取用于内部网应用程序的 NetScaler HA 对模板

完成以下步骤以启动模板并使用 Azure 可用性集部署高可用性 VPX 对。

1. 在 Azure 门户中，导航到“**自定义部署**”页面。
2. 出现“**基本信息**”页面。创建一个资源组。在“**参数**”选项卡下，输入区域、管理员用户名、管理员密码、许可证类型 (`VM sku`) 和其他字段的详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 单击“**下一步：审核 + 创建 >**”。

   Azure 资源组可能需要一些时间才能使用所需的配置创建。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。

   如果您的 HA 设置需要进一步修改，例如创建更多安全规则和端口，您可以从 Azure 门户进行操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

所需配置完成后，将创建以下资源。

HA ILB 资源组(/en-us/vpx/media/ha-ilb-resource-group.png)

4. 登录到 **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，您应该会看到两个 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，ADC-VPX-0 和 ADC-VPX-1 VM 的 SNIP 地址在同一子网中是不同的，这与经典的本地 ADC HA 部署中两者相同的情况不同。 为了支持 VPX 对 SNIP 位于不同子网中的部署，或者当 VIP 不与 SNIP 位于同一子网中时，您必须启用基于 Mac 的转发 (MBF)，或为每个 VIP 向每个 VPX 节点添加静态主机路由。

   在主节点 (ADC-VPX-0) 上

   在主节点上显示 IP CLI(/en-us/vpx/media/primary-node1.png)

   在主节点上显示高可用性节点 CLI(/en-us/vpx/media/primary-node2.png)

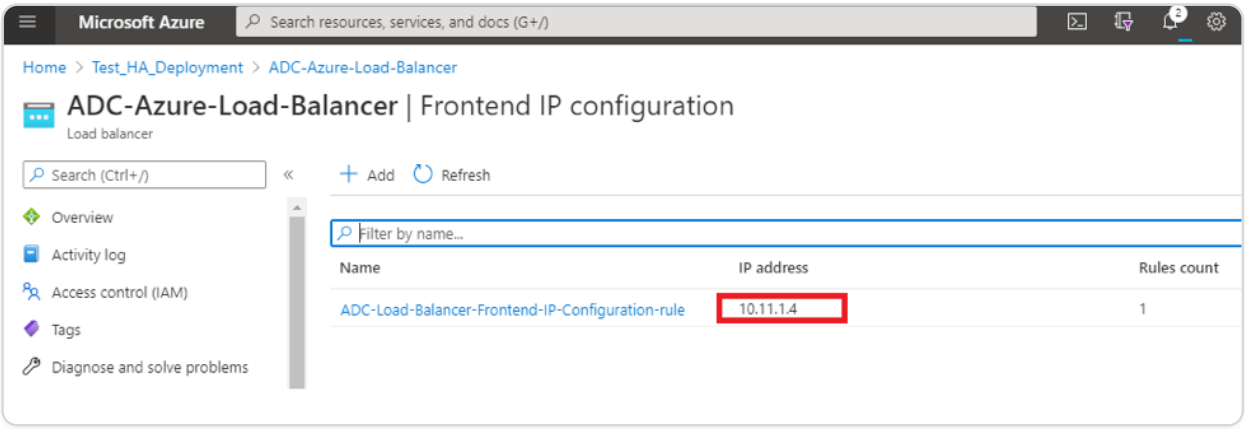
   在辅助节点 (ADC-VPX-1) 上

   在辅助节点上显示 IP CLI(/en-us/vpx/media/secondary-node1.png)

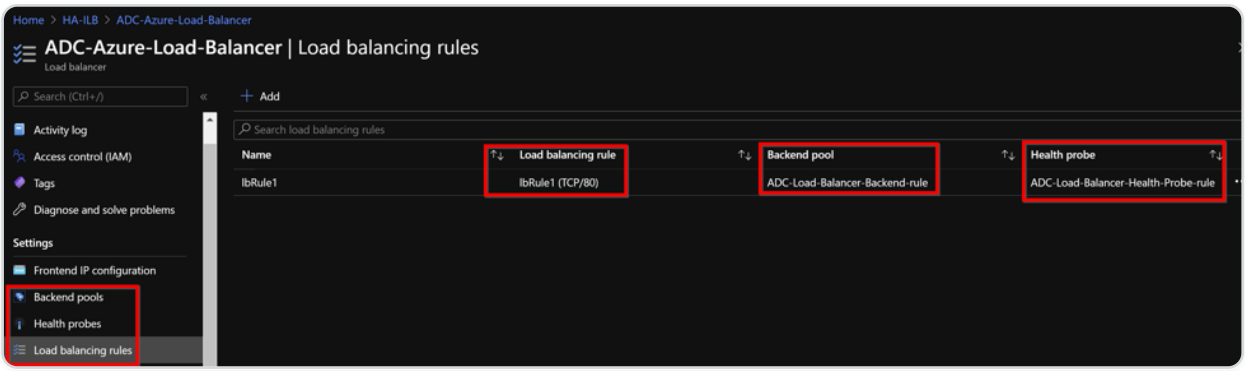
   在辅助节点上显示高可用性节点 CLI(/en-us/vpx/media/secondary-node2.png)

5. 在主节点和辅助节点启动且同步状态为 **SUCCESS** 后，您必须在主节点 (ADC-VPX-0) 上使用 ADC Azure 负载均衡器的私有浮动 IP (FIP) 地址配置负载均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 负载均衡器的私有 IP 地址，请导航到 **Azure 门户 > ADC Azure 负载均衡器 > 前端 IP 配置**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

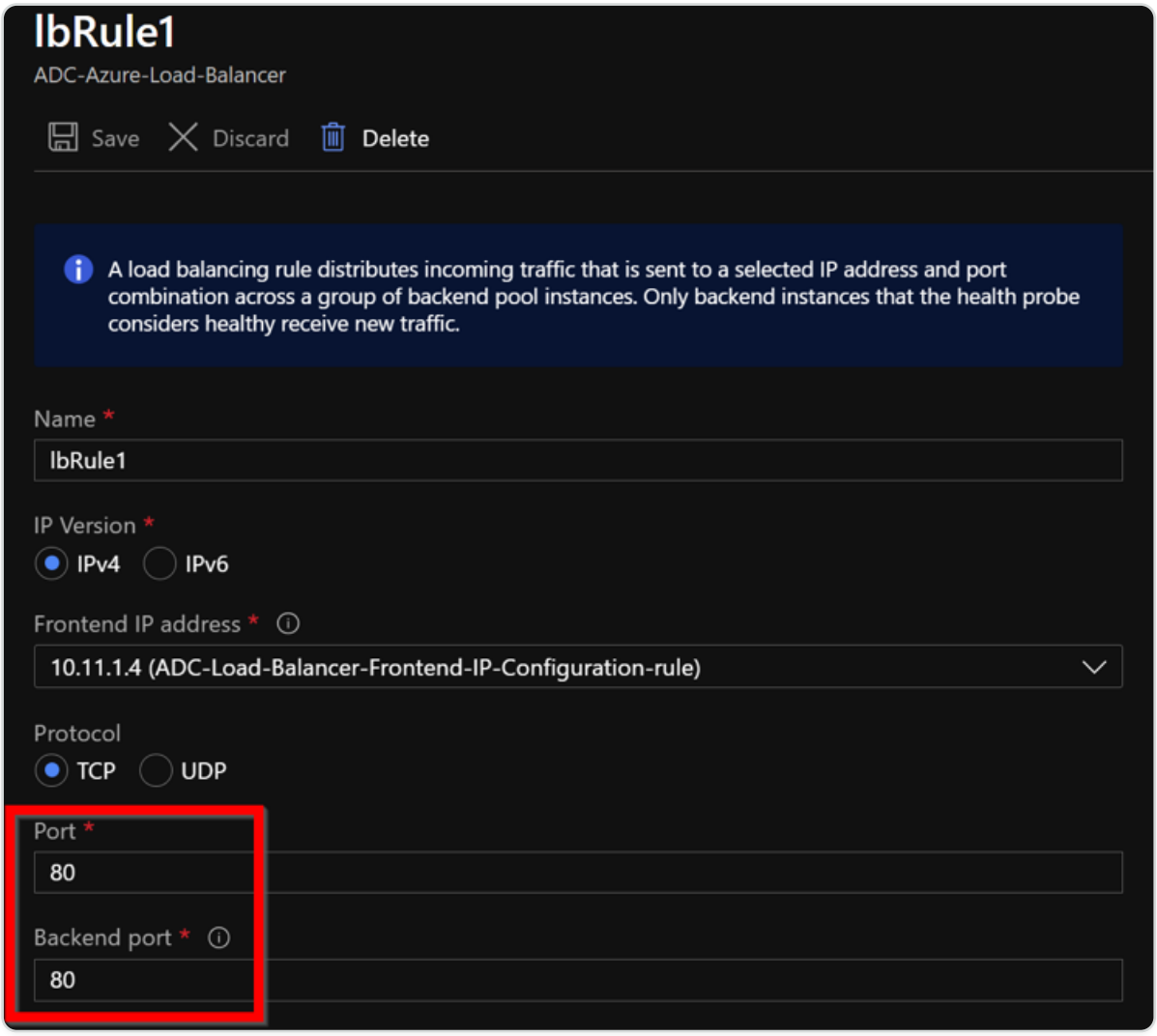


7. 在 **Azure 负载均衡器** 配置页面中，ARM 模板部署有助于创建 LB 规则、后端池和运行状况探测。



- LB 规则 (LbRule1) 默认使用端口 80。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

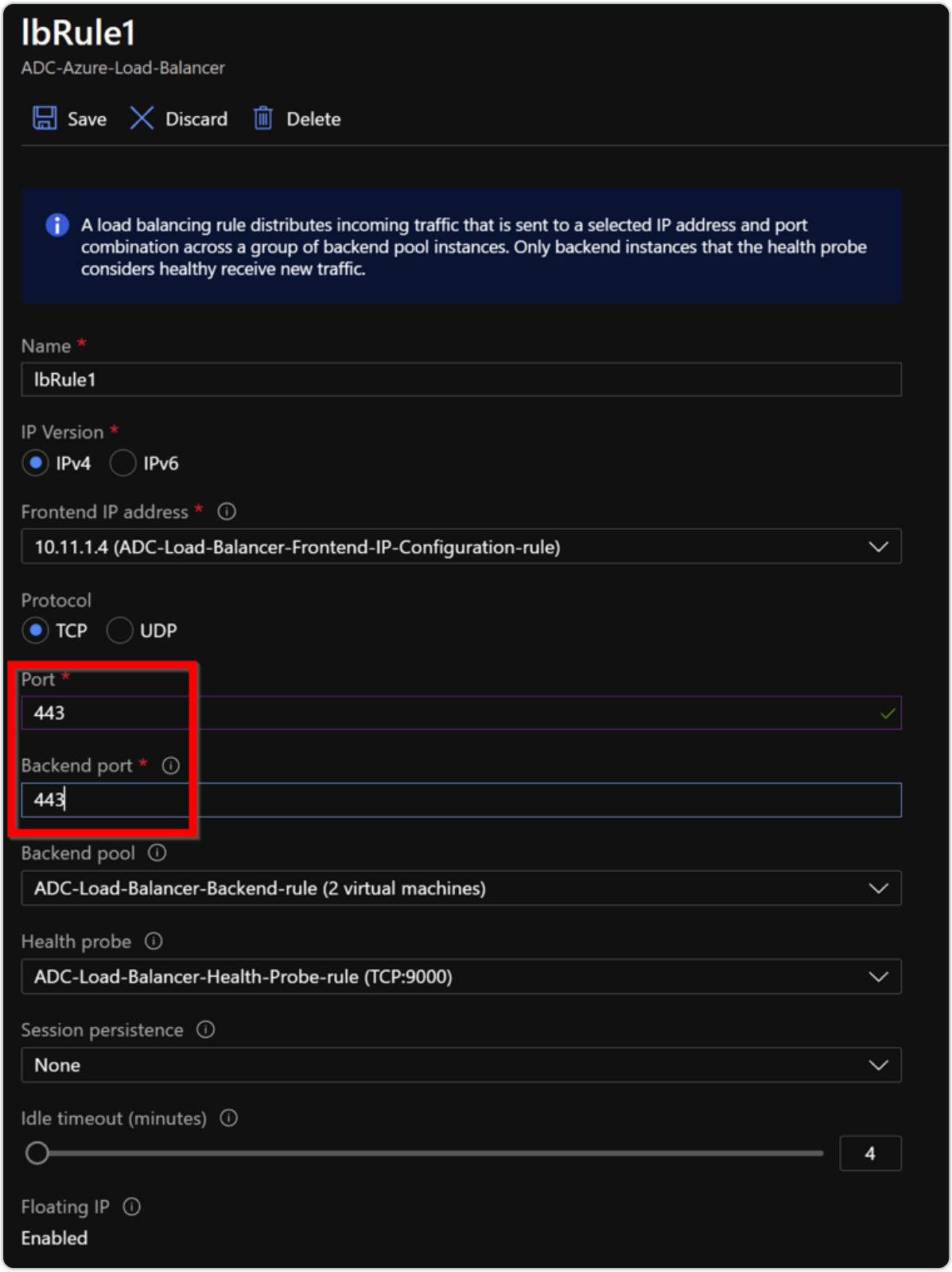


- 编辑规则以使用端口 443，并保存更改。

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。

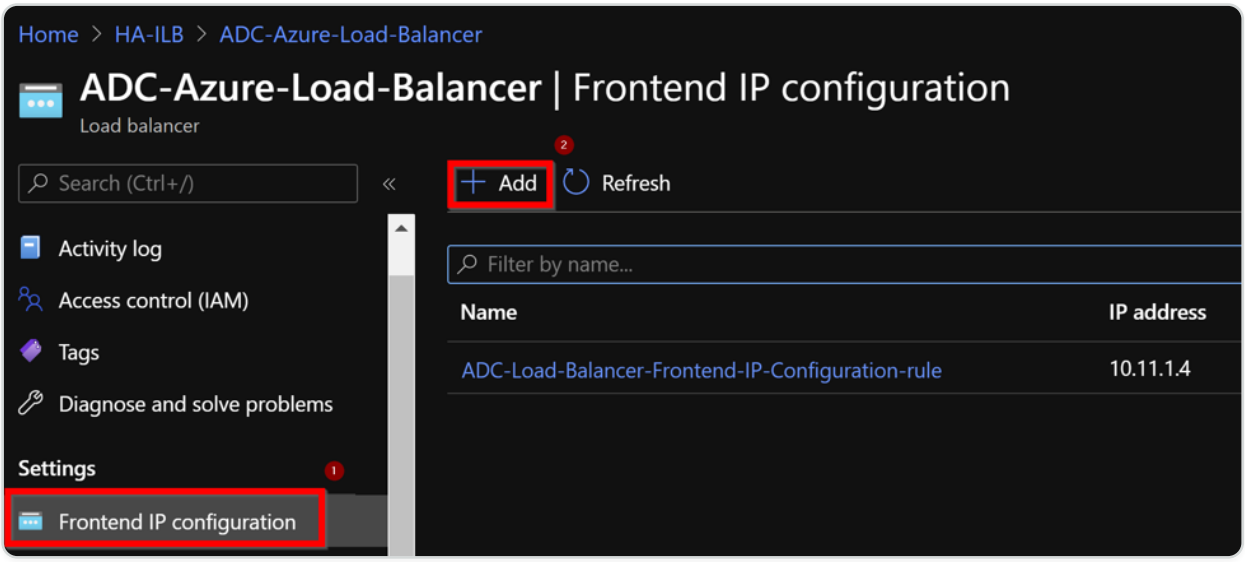
© 1997–2026 Citrix Systems, Inc. All rights reserved.



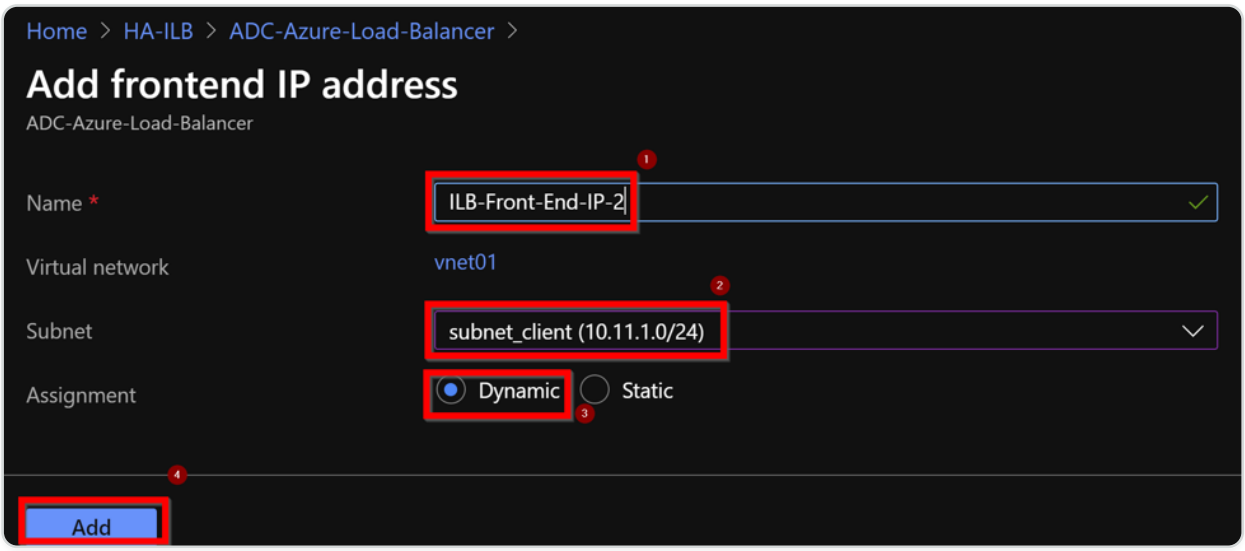
要在 ADC 上添加更多 VIP 地址，请执行以下步骤：

1. 导航到 **Azure 负载均衡器 > 前端 IP 配置**，然后单击**添加**以创建新的内部负载均衡器 IP 地址。

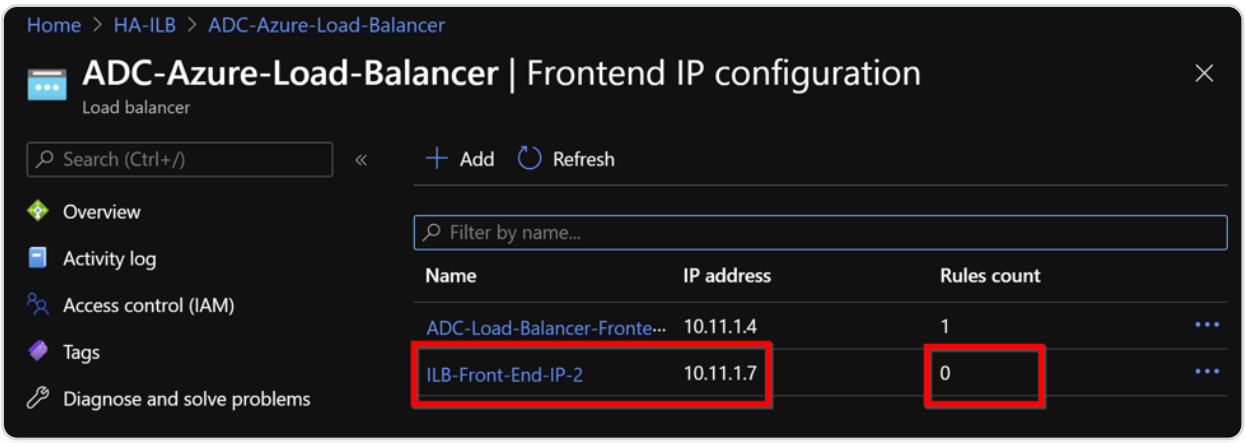
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 在**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**添加**。

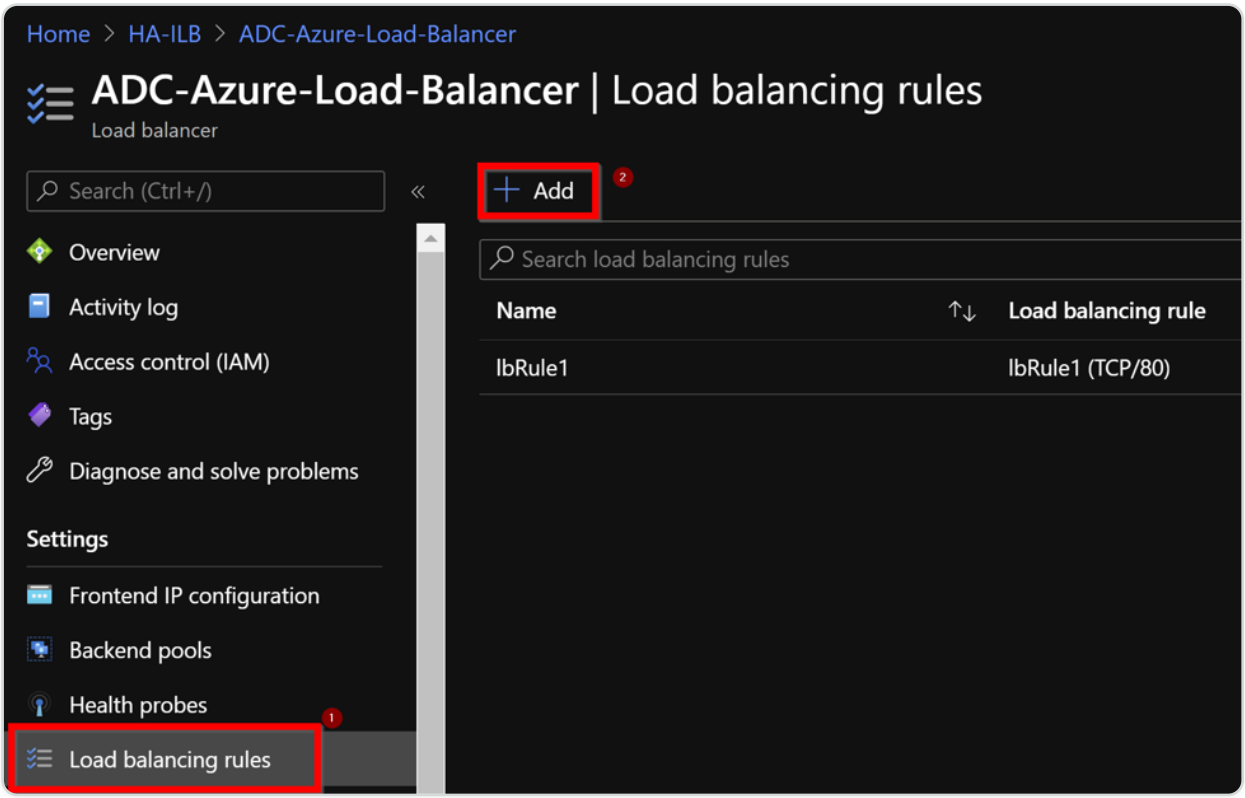


3. 前端 IP 地址已创建，但未关联 LB 规则。创建新的负载均衡规则，并将其与前端 IP 地址关联。



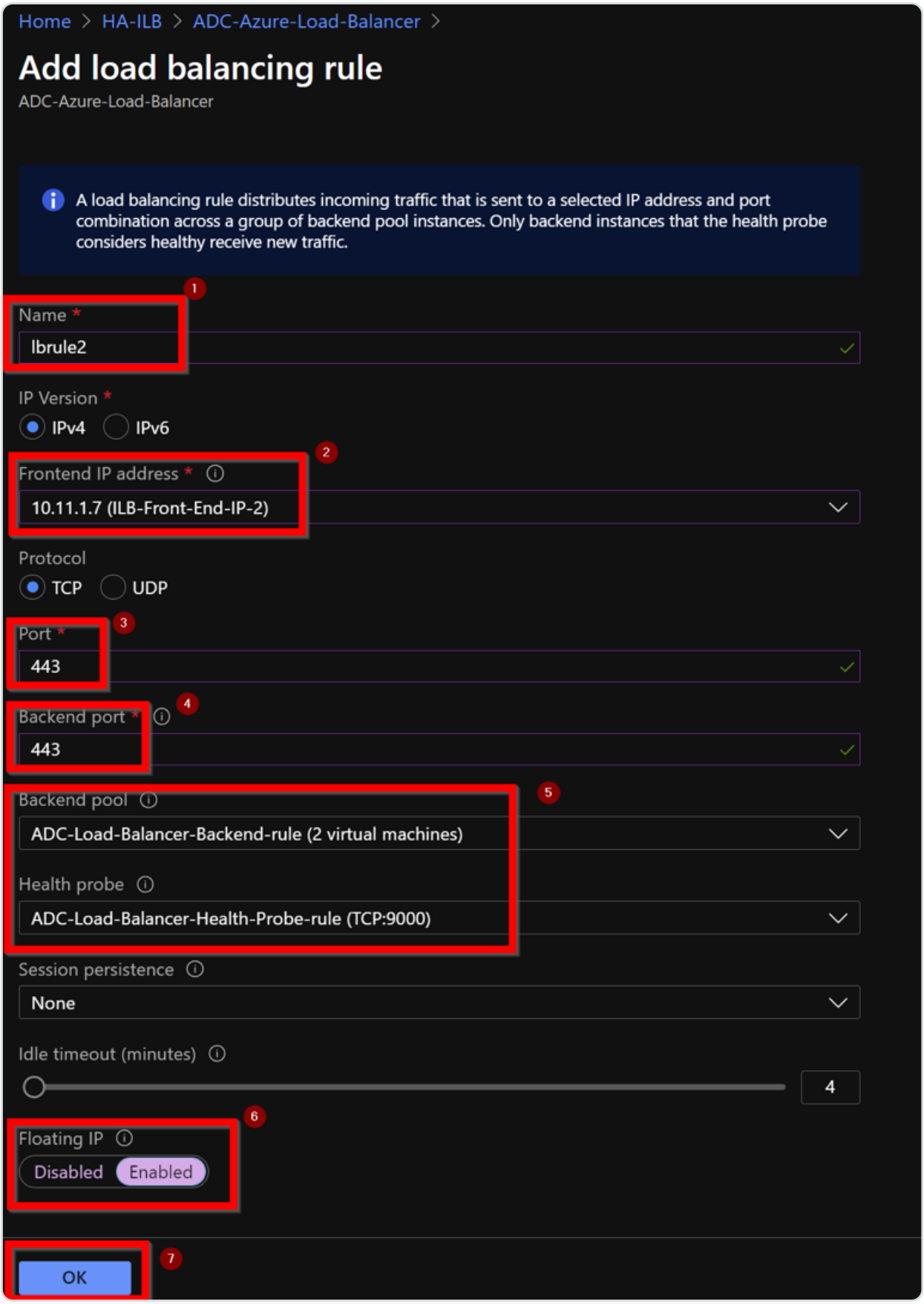
4. 在 **Azure 负载均衡器** 页面中，选择 **负载均衡规则**，然后单击 **添加**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



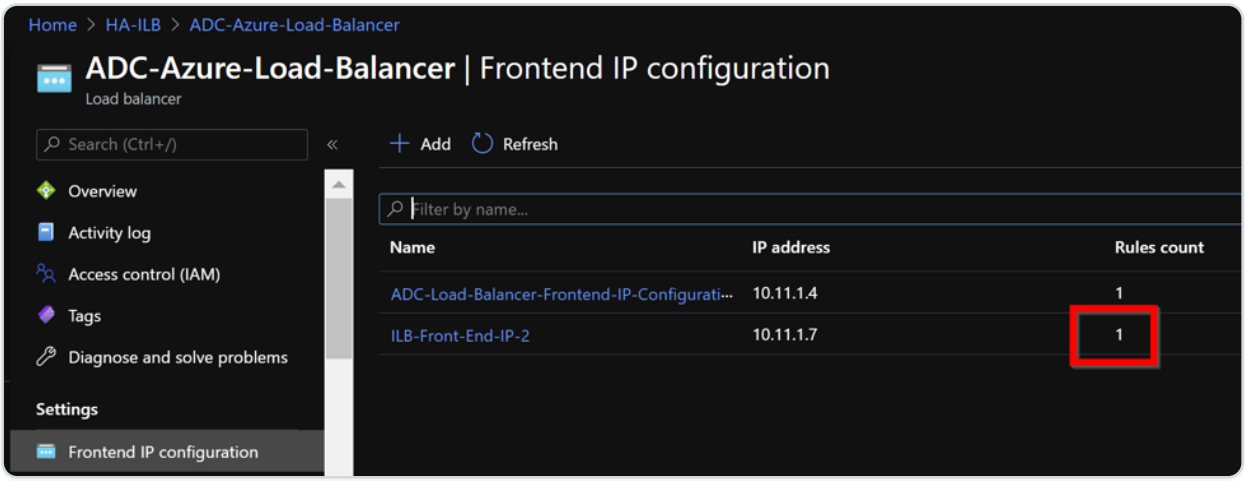
5. 通过选择新的前端 IP 地址和端口来创建新的 LB 规则。**浮动 IP** 字段必须设置为 **已启用**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 现在，**前端 IP 配置** 显示了已应用的 LB 规则。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



示例配置

要配置网关 VPN 虚拟服务器和负载均衡虚拟服务器，请在主节点 (ADC-VPX-0) 上运行以下命令。配置会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
```

负载均衡示例配置

```
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
```

您现在可以使用与 ILB 内部 IP 地址关联的完全限定域名 (FQDN) 访问负载均衡或 VPN 虚拟服务器。

有关如何配置负载均衡虚拟服务器的更多信息，请参阅 **资源** 部分。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

资源：

以下链接提供了有关 HA 部署和虚拟服务器配置的更多信息：

- 在不同子网中配置高可用性节点
- 设置基本负载均衡

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 HA 部署中配置 GSLB

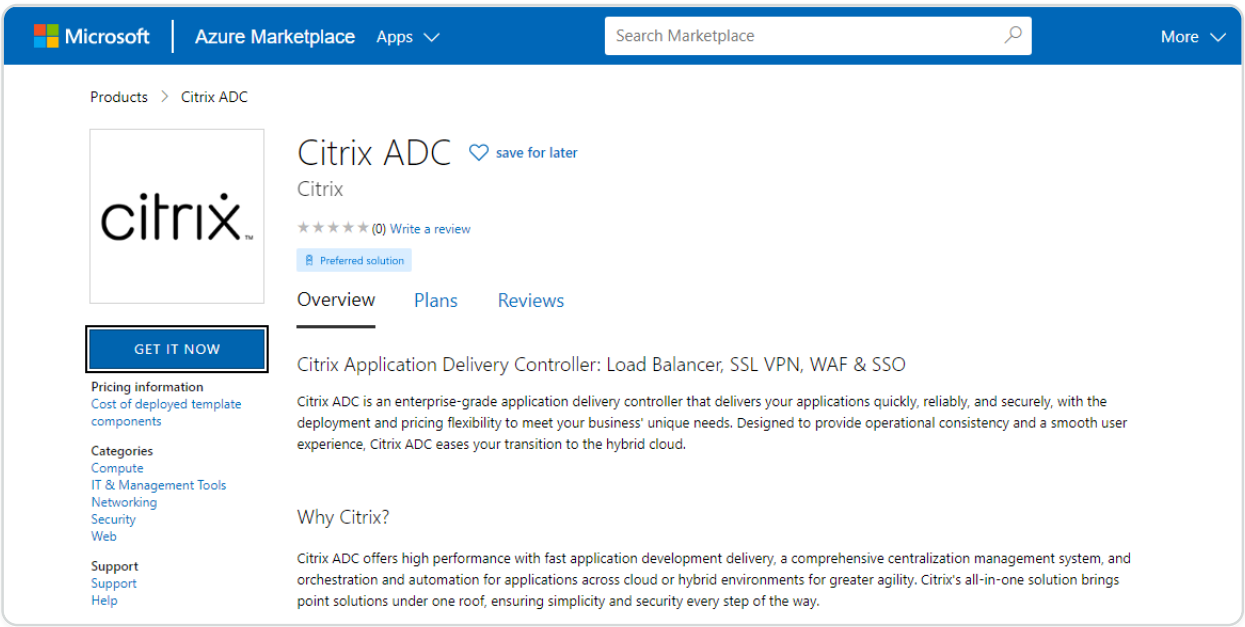
使用 NetScaler® 高可用性模板为面向 Internet 的应用程序配置 HA-INC 节点

您可以使用面向 Internet 应用程序的标准模板，快速高效地以 HA-INC 模式部署一对 VPX 实例。Azure 负载均衡器 (ALB) 使用公共 IP 地址作为前端。该模板创建两个节点，包含三个子网和六个 NIC。这些子网用于管理、客户端和服务器端流量。每个子网都有两个 NIC，分别用于两个 VPX 实例。

您可以在 Azure Marketplace 获取面向 Internet 应用程序的 NetScaler HA 对模板。

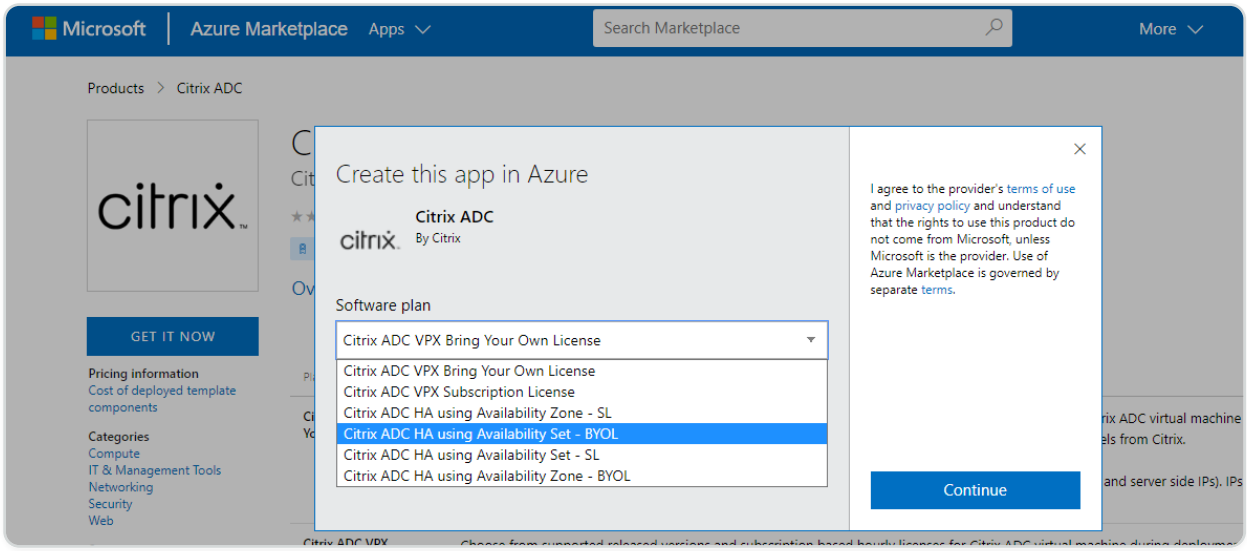
完成以下步骤以启动模板并使用 Azure 可用性集或可用性区域部署高可用性 VPX 对。

1. 在 Azure Marketplace 中，搜索 **NetScaler**。
2. 单击 **立即获取**。



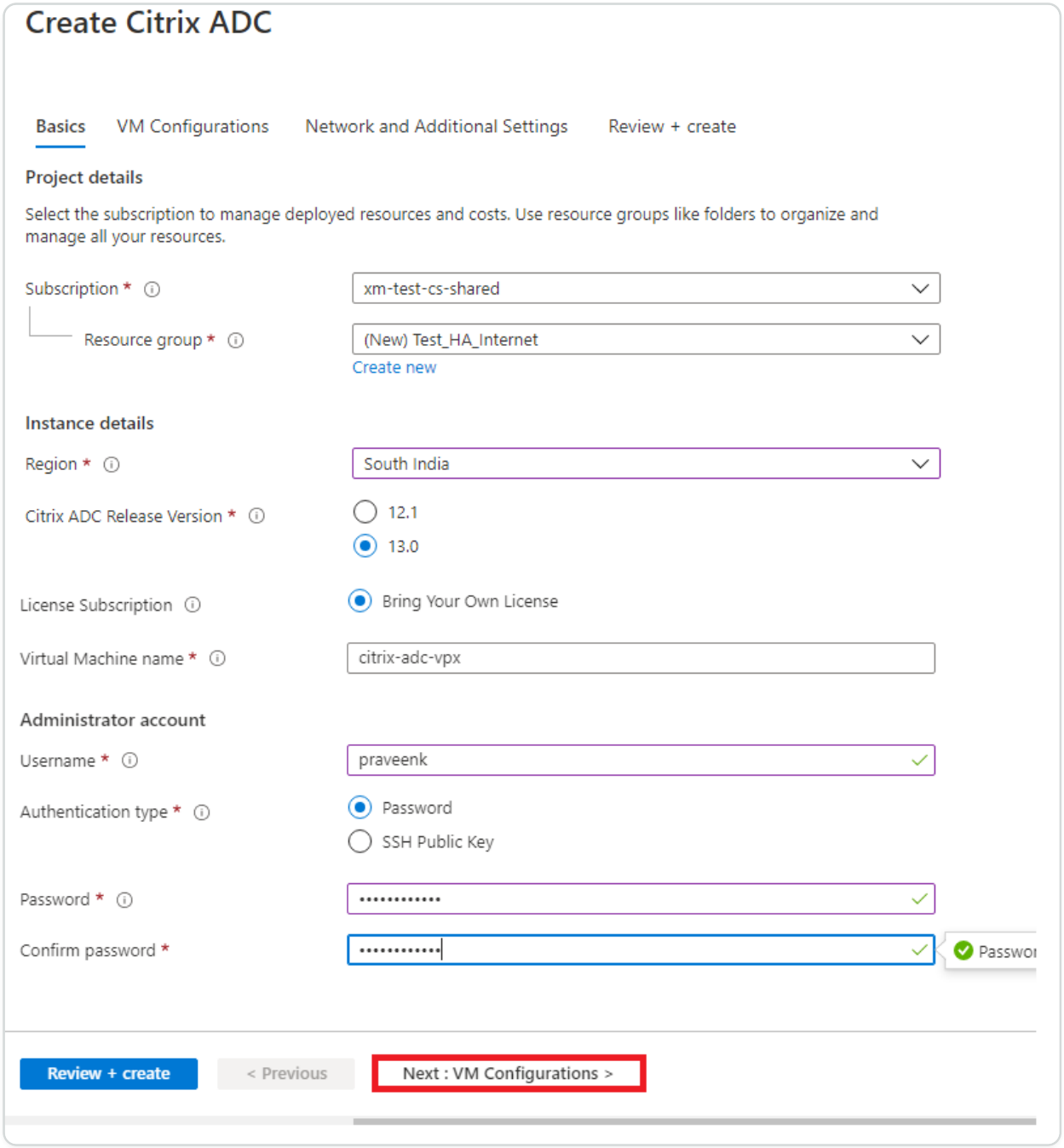
3. 选择所需的 HA 部署以及许可证，然后单击 **继续**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



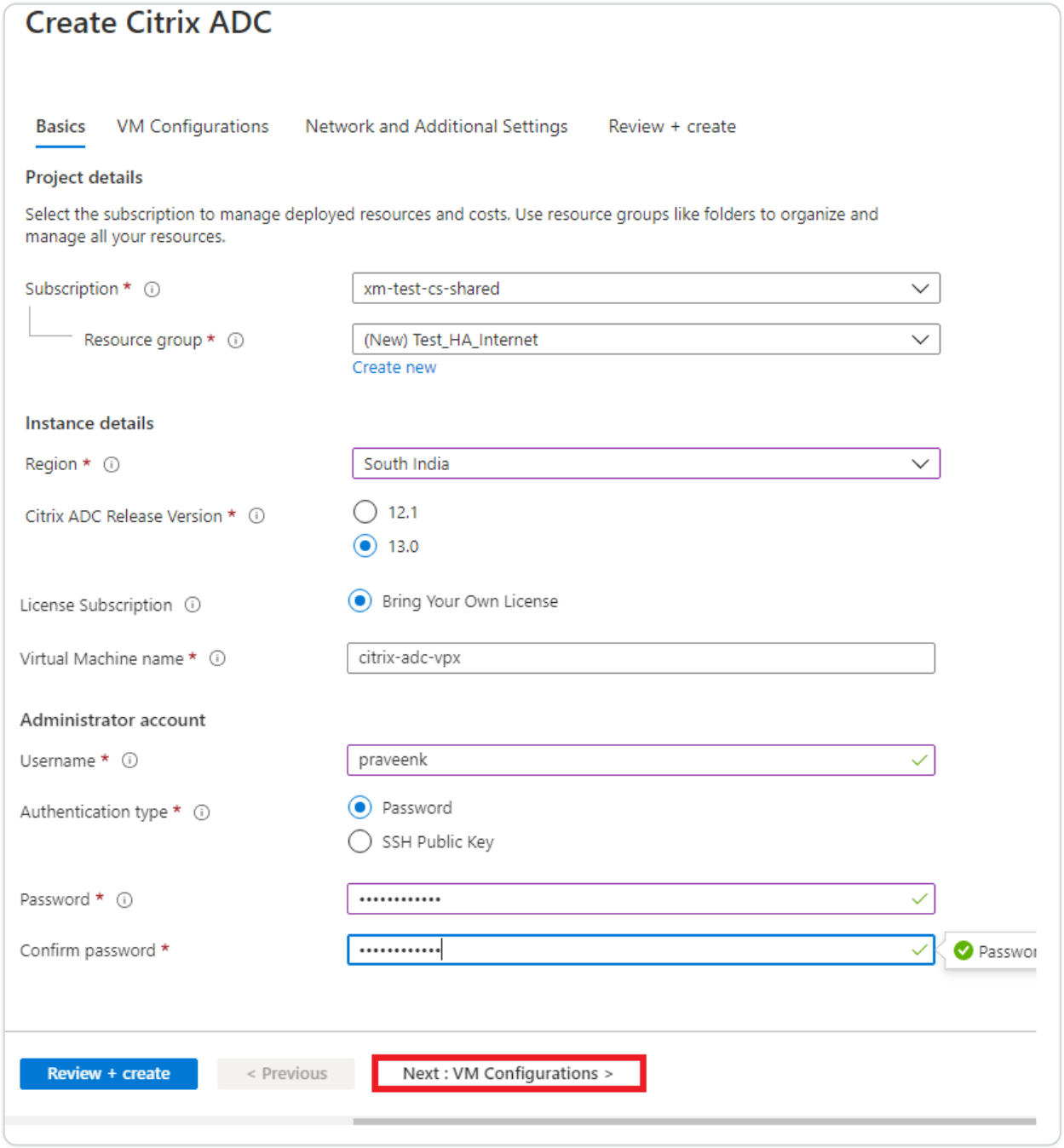
4. 出现“**基本信息**”页面。创建一个资源组。在“**参数**”选项卡下，输入区域、管理员用户名、管理员密码、许可证类型 (VM SKU) 和其他字段的详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 单击 **下一步：VM 配置 >**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

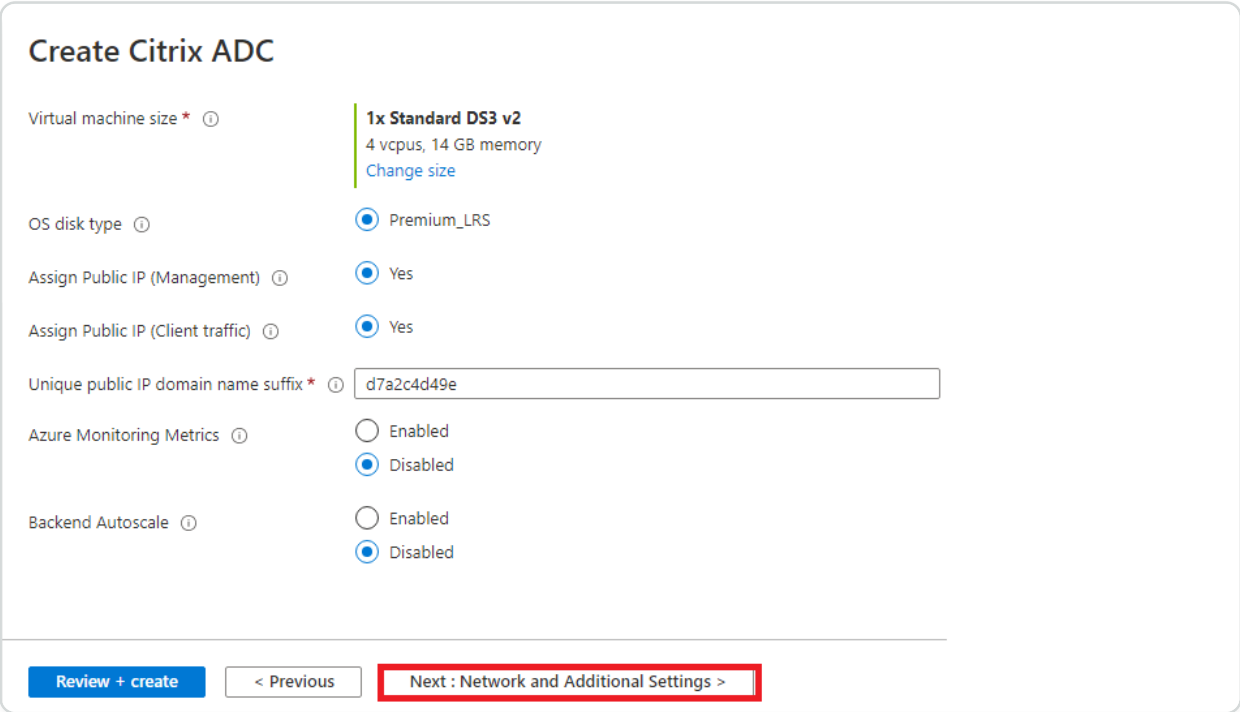


6. 在“**VM 配置**”页面上，执行以下操作：

   - 配置公共 IP 域名后缀
   - 启用或禁用 **Azure 监控指标**
   - 启用或禁用 **后端自动扩缩™**

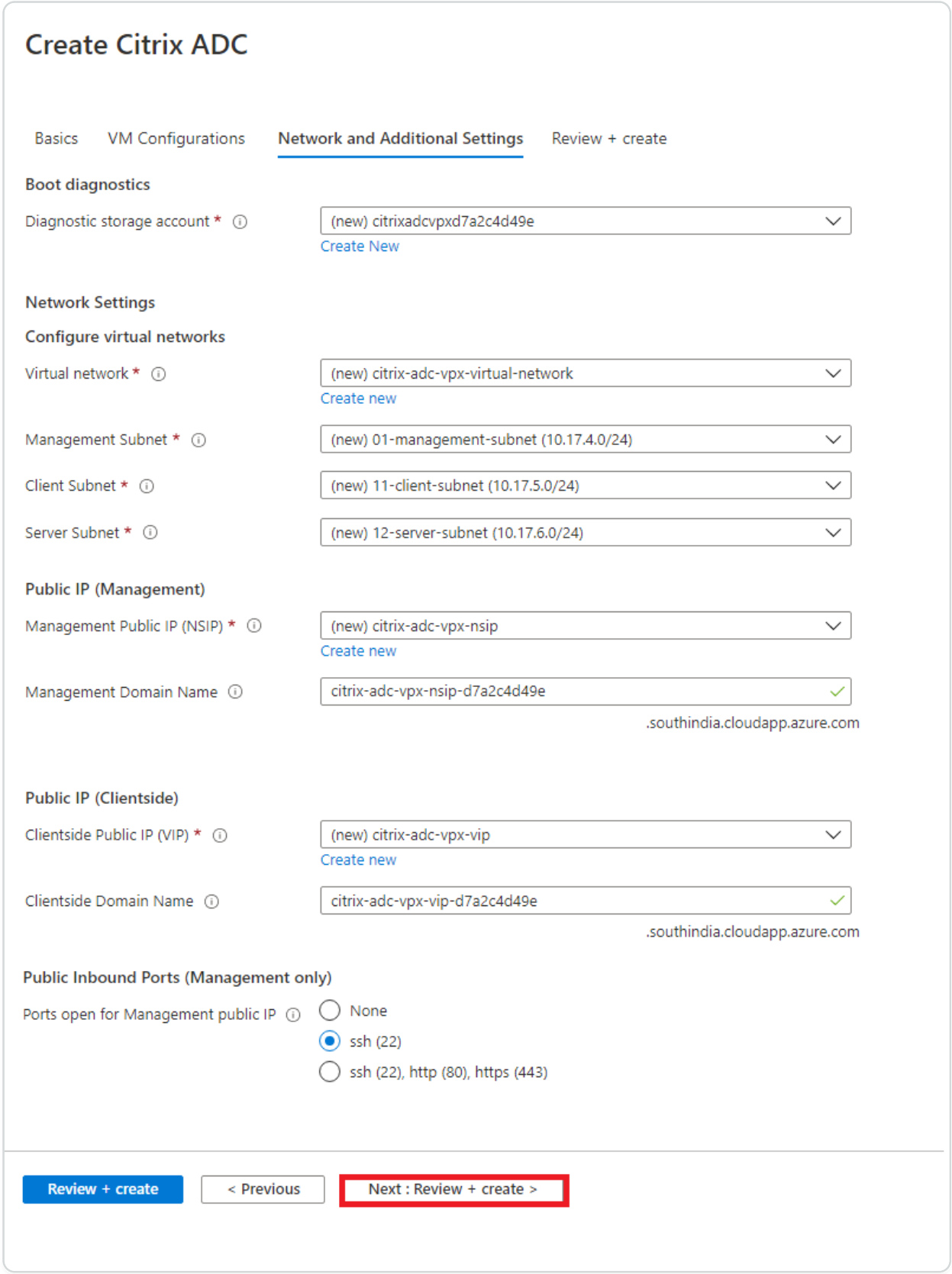
7. 单击 **下一步：网络和附加设置 >**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. 在 **网络和附加设置** 页面上，创建启动诊断帐户并配置网络设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



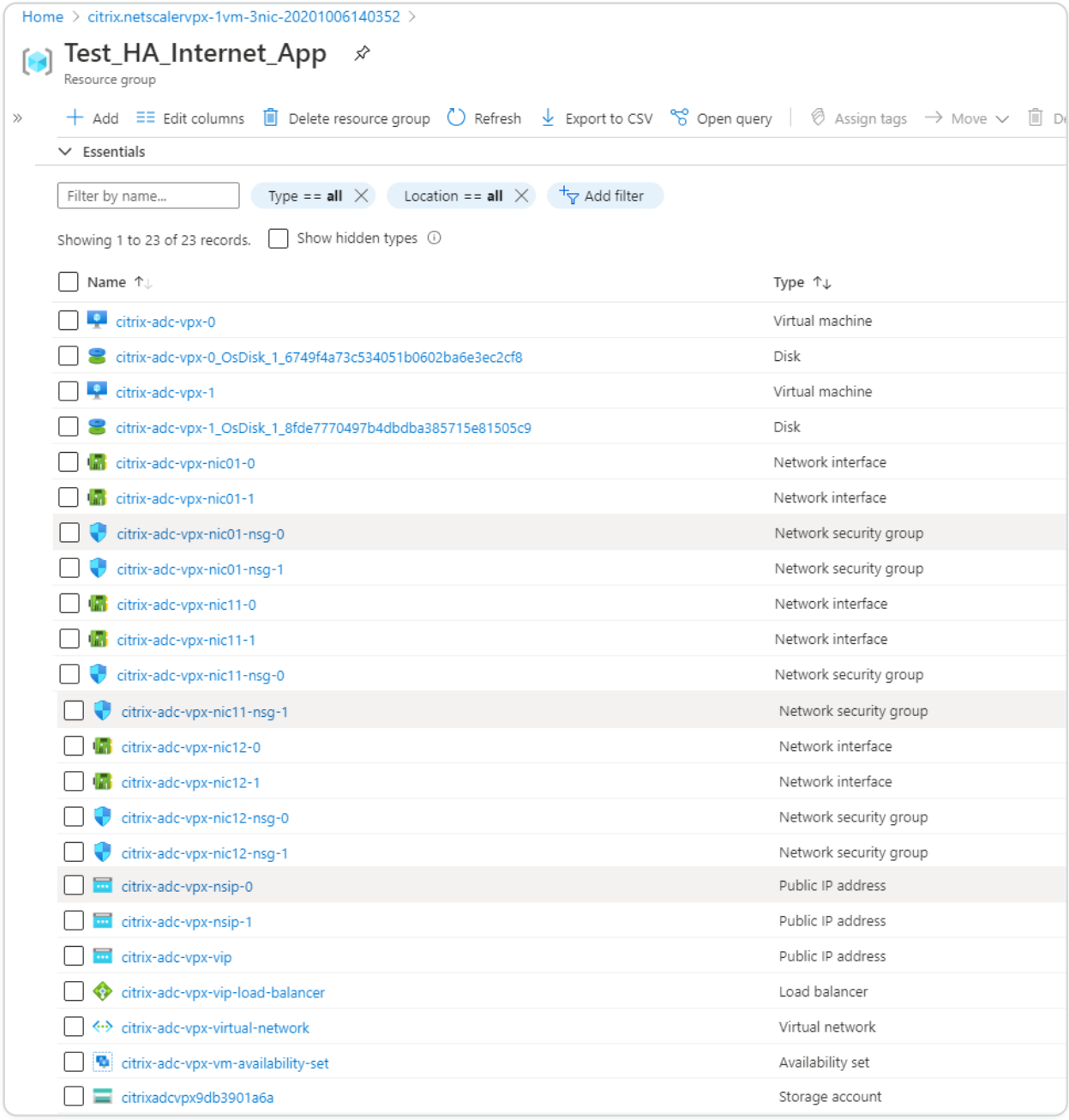
9. 单击 **下一步：审核 + 创建 >**。
10. 查看基本设置、VM 配置、网络和附加设置，然后单击 **创建**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure 资源组可能需要一些时间才能使用所需的配置创建。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、后端池和运行状况探测。高可用性对显示为 **citrix-adc-vpx-0** 和 **citrix-adc-vpx-1**。

如果您的 HA 设置需要进一步修改，例如创建更多安全规则和端口，您可以从 Azure 门户进行操作。

完成所需配置后，将创建以下资源。



11. 您必须登录到 **citrix-adc-vpx-0** 和 **citrix-adc-vpx-1** 节点以验证以下配置：

    - 两个节点的 NSIP 地址都必须在管理子网中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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，这与经典的本地 ADC 高可用性部署不同，在经典部署中两者是相同的。

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)

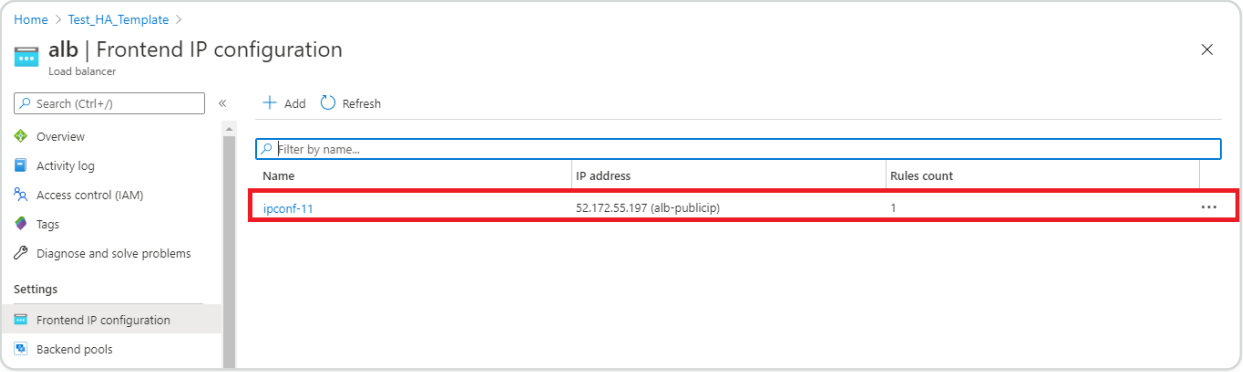
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> 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
>
```

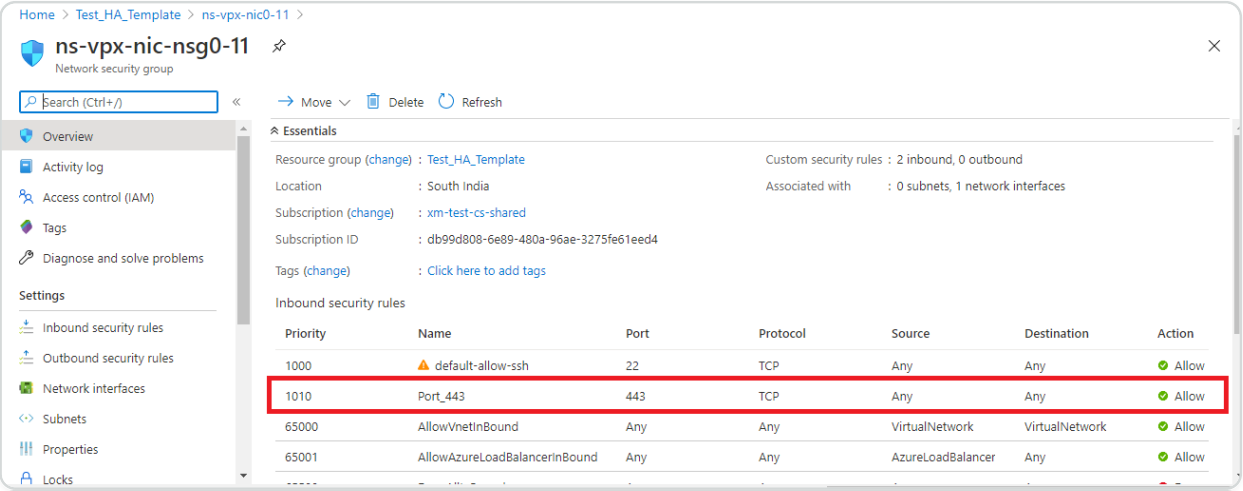
12. 在主节点和辅助节点启动且同步状态为 **SUCCESS** 后，您必须使用 ALB 虚拟服务器的公共 IP 地址在主节点 (citrix-adc-vpx-0) 上配置负载平衡虚拟服务器或网关虚拟服务器。有关详细信息，请参阅 示例配置 部分。

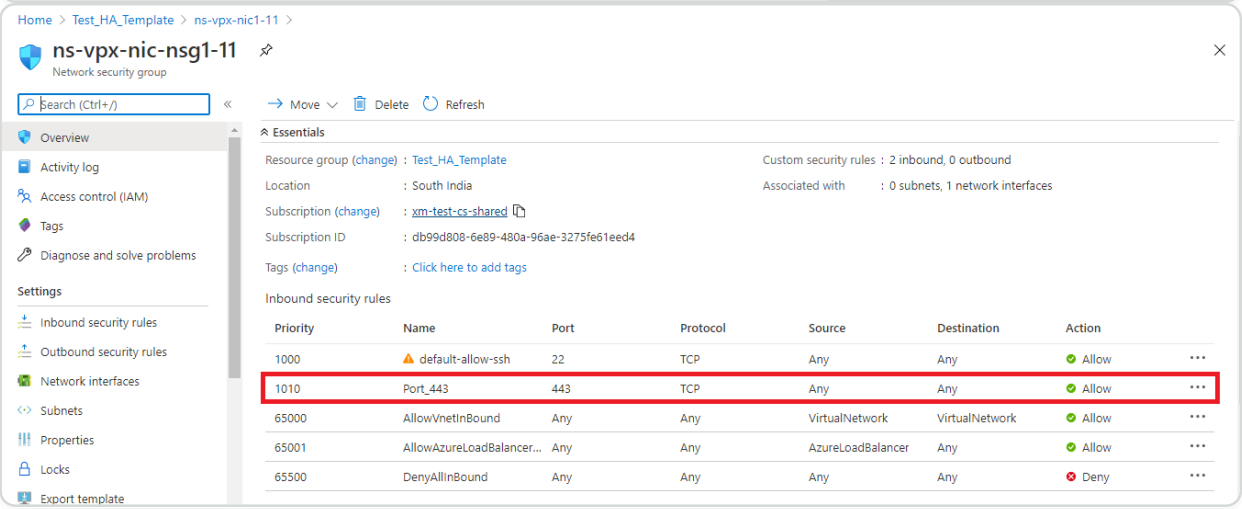
13. 要查找 ALB 虚拟服务器的公共 IP 地址，请导航到 **Azure 门户 > Azure 负载均衡器 > 前端 IP 配置**。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

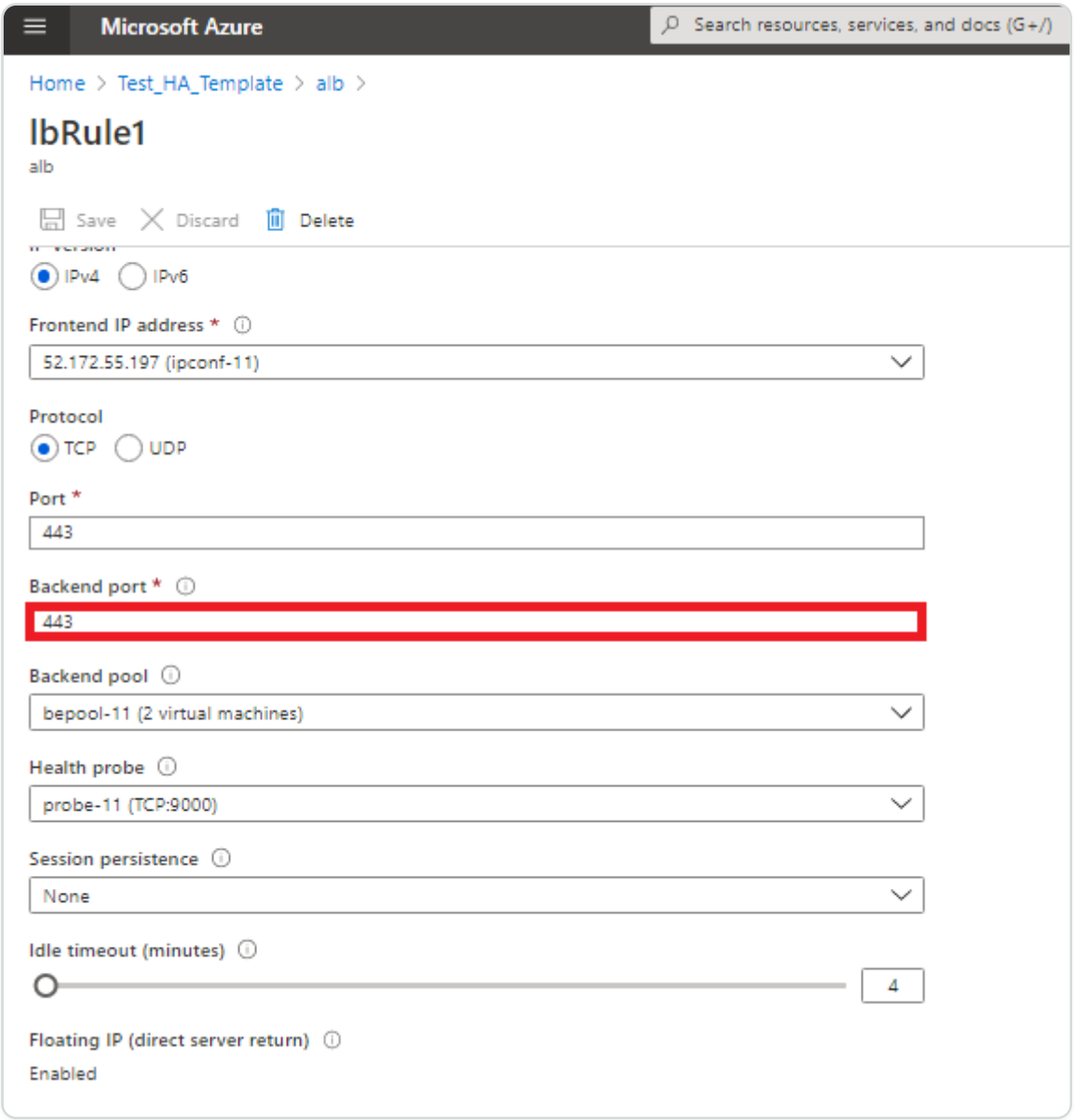
14. 在两个客户端接口的网络安全组上，为虚拟服务器端口 443 添加入站安全规则。



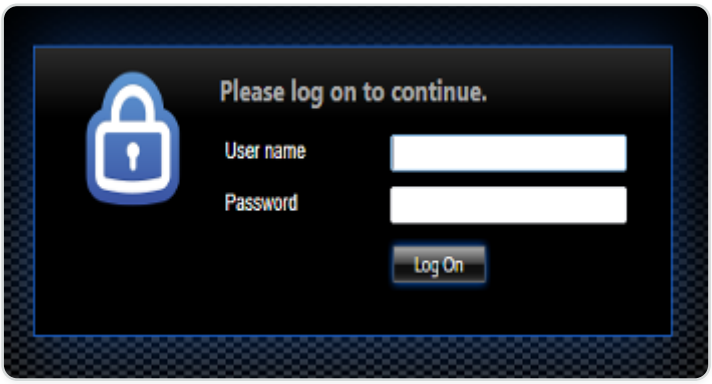


15. 配置您要访问的 ALB 端口，并为指定端口创建入站安全规则。后端端口是您的负载平衡虚拟服务器端口或 VPN 虚拟服务器端口。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



16. 现在，您可以使用与 ALB 公共 IP 地址关联的完全限定域名 (FQDN) 来访问负载均衡虚拟服务器或 VPN 虚拟服务器。



示例配置

要配置网关 VPN 虚拟服务器和负载均衡虚拟服务器，请在主节点 (ADC-VPX-0) 上运行以下命令。配置会自动同步到辅助节点 (ADC-VPX-1)。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
```

负载均衡示例配置

```
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
```

您现在可以使用与 ALB 公共 IP 地址关联的 FQDN 来访问负载均衡或 VPN 虚拟服务器。

有关如何配置负载均衡虚拟服务器的更多信息，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更多信息：

- 创建虚拟服务器
- 设置基本负载均衡

同时配置带有 Azure 外部和内部负载均衡器的高可用性设置

Azure 上的高可用性对同时支持外部和内部负载均衡器。

您可以通过以下两种选项配置同时使用 Azure 外部和内部负载均衡器的高可用性对：

- 在 NetScaler 设备上使用两个 LB 虚拟服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 使用一个 LB 虚拟服务器和一个 IP 集。单个 LB 虚拟服务器将流量分发到由 IPset 定义的多个 IP。

请执行以下步骤，在 Azure 上同时配置使用外部和内部负载均衡器的高可用性对：

对于步骤 1 和 2，请使用 Azure 门户。对于步骤 3 和 4，请使用 NetScaler VPX GUI 或 CLI。

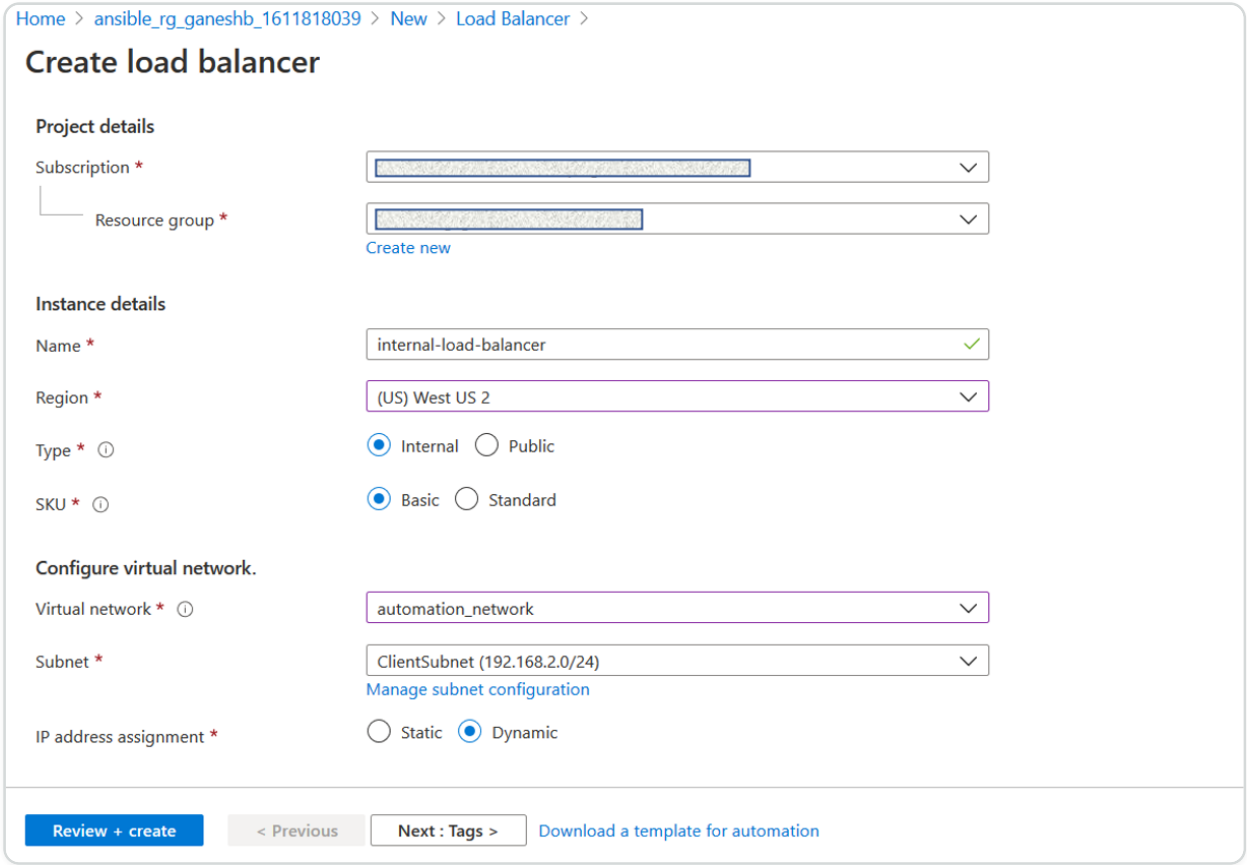
步骤 1. 配置 Azure 负载均衡器，可以是外部负载均衡器或内部负载均衡器。

有关使用 Azure 外部负载均衡器配置高可用性设置的更多信息，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更多信息，请参阅 使用带有 Azure ILB 的 NetScaler 高可用性模板配置 HA-INC 节点。

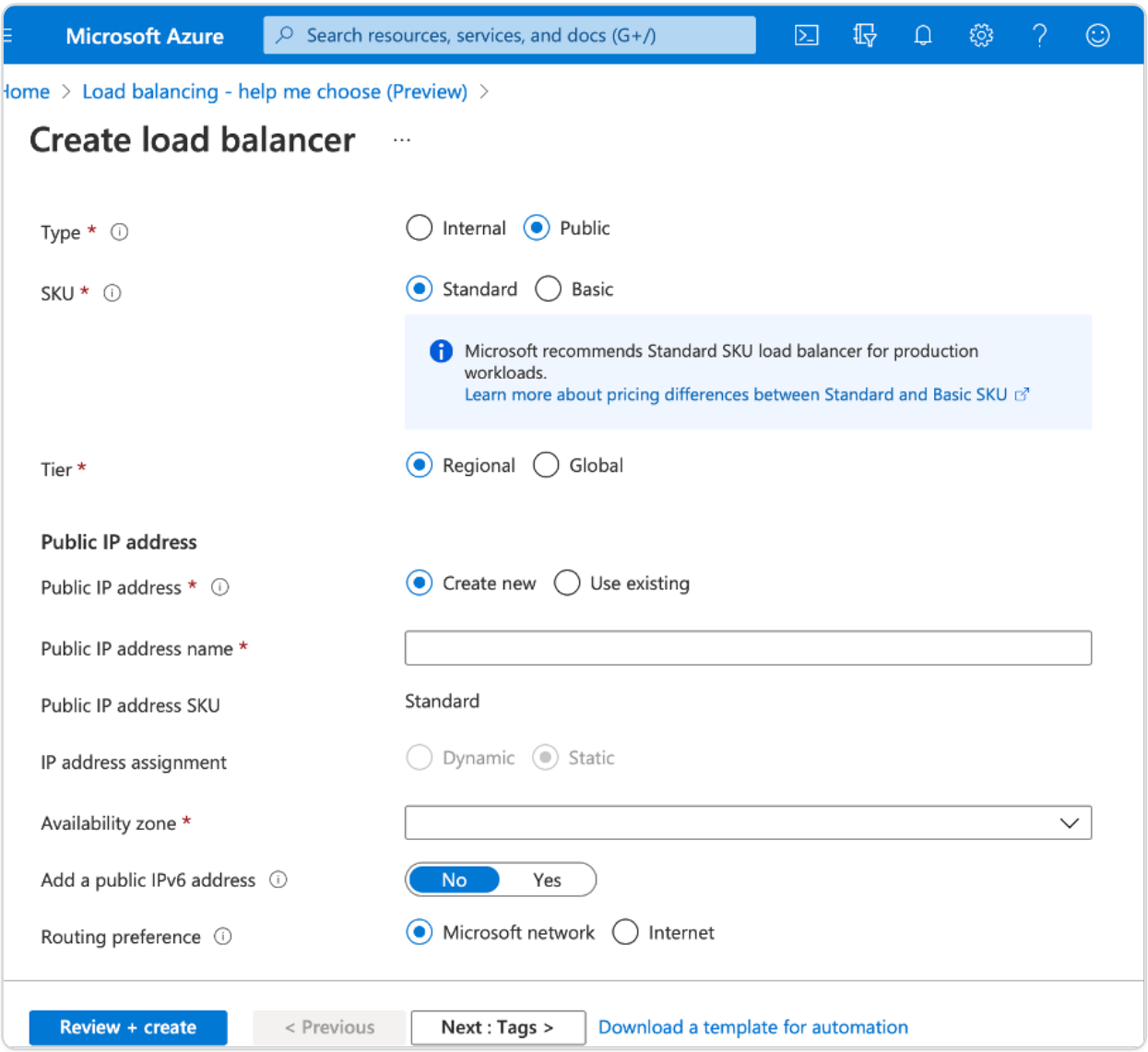
步骤 2. 在资源组中创建额外的负载均衡器 (ILB)。如果在步骤 1 中创建了外部负载均衡器，则现在创建内部负载均衡器，反之亦然。

- 要创建内部负载均衡器，请选择负载均衡器类型为 **Internal**。对于 **Subnet** 字段，您必须选择您的 NetScaler 客户端子网。您可以选择在该子网中提供静态 IP 地址，前提是没有冲突。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为 **Public** 并在此处创建公共 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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。在步骤 3 中创建 ADC 负载均衡虚拟服务器时，必须使用此 IP 地址。

   前端 IP 配置(/en-us/vpx/media/frontend-ip-configuration.png)

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。
3. 将高可用性对客户端 NIC 添加到 ILB 的后端池。
4. 创建运行状况探测（TCP，端口 9000）
5. 创建两个负载均衡规则：

   - 一个用于端口 80 上的 HTTP 流量（Web 应用用例）的 LB 规则。该规则还必须使用后端端口 80。选择已创建的后端池和运行状况探测。必须启用浮动 IP。
   - 另一个用于端口 443 上的 HTTPS 或 CVAD 流量的 LB 规则。此过程与 HTTP 流量相同。

步骤 3. 在 NetScaler 设备的主节点上，为 ILB 创建一个负载均衡虚拟服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 添加负载均衡虚拟服务器。

```
add lb vserver <name> <serviceType> [<ILB Frontend IP address>]
[<port>]
```

示例：

```
add lb vserver vserver_name HTTP 52.172.96.71 80
```

注意：

使用与您在步骤 2 中创建的附加负载均衡器关联的负载均衡器前端 IP 地址。

2. 将服务绑定到负载均衡虚拟服务器。

```
bind lb vserver <name> <serviceName>
```

示例：

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
```

有关更多信息，请参阅设置基本负载平衡

步骤 4： 作为步骤 3 的替代方案，您可以使用 IPset 为 ILB 创建负载平衡虚拟服务器。

1. 添加类型为虚拟服务器 IP (VIP) 的 IP 地址。

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

示例：

```
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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

示例：

```
add ipset ipset1
```

3. 将 IP 地址绑定到 IP 集。

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

示例：

```
bind ipset ipset1 52.172.96.71
```

4. 将现有 LB 虚拟服务器设置为使用 IPset。

```
set lb vserver <vserver name> -ipset <ipset name>
```

示例：

```
set lb vserver vserver_name -ipset ipset1
```

有关更多信息，请参阅配置多 IP 虚拟服务器。

在 Azure VMware Solution 上安装 NetScaler VPX 实例

Azure VMware Solution (AVS) 为您提供包含 vSphere 群集的私有云，这些群集基于专用的裸机 Azure 基础架构构建。最低初始部署为三个主机，但可以一次添加一个额外主机，每个群集最多可达 16 个主机。所有已预配的私有云都具有 vCenter Server、vSAN、vSphere 和 NSX-T。

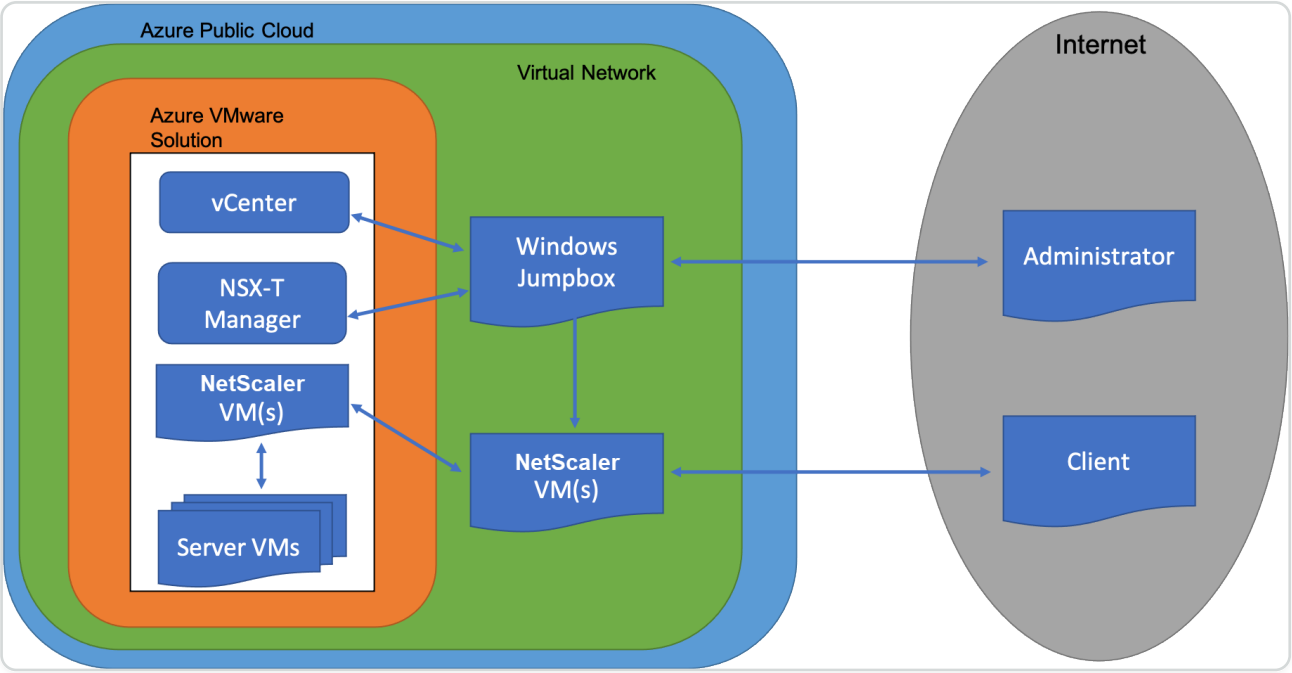
Azure 上的 VMware Cloud (VMC) 使您能够在 Azure 上创建云软件定义数据中心 (SDDC)，并可根据需要配置 ESX 主机数量。Azure 上的 VMC 支持 NetScaler VPX 部署。VMC 提供与本地 vCenter 相同的用户界面。其功能类似于基于 ESX 的 NetScaler VPX 部署。

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 VM。管理员可以从 Windows Jumpbox 访问 AVS 基于 Web 的 vCenter 和 NSX-T Manager。您可以使用 vCenter 在 Azure VMware Solution 中创建 NetScaler VPX 实例（独立或高可用性对）和服务器

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VM，并使用 NSX-T Manager 管理相应的网络。AVS 上的 NetScaler VPX 实例的工作方式类似于本地 VMware 主机群集。AVS 是从在同一虚拟网络中创建的 Windows Jumpbox 进行管理的。

客户端只能通过连接到 ADC 的 VIP 来访问 AVS 服务。另一个位于 Azure VMware Solution 外部但在同一 Azure 虚拟网络中的 NetScaler VPX 实例有助于将 Azure VMware Solution 内的 NetScaler VPX 实例的 VIP 添加为服务。根据要求，您可以配置 NetScaler VPX 实例以通过 Internet 提供服务。



先决条件

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 Solution 文档。
- 有关部署 Azure VMware 解决方案的更多信息，请参阅 部署 Azure VMware Solution 私有云。
- 有关创建 Windows Jump box VM 以访问和管理 Azure VMware Solution 的更多信息，请参阅 访问 Azure VMware Solution 私有云
- 在 Windows Jump box VM 中，下载 NetScaler VPX 设备安装文件。
- 在 VMware SDDC 上创建虚拟机连接的相应 NSX-T 网络段。有关更多信息，请参阅 在 Azure VMware Solution 中添加网络段
- 获取 VPX 许可证文件。
- 创建或迁移到 Azure VMware Solution 私有云的虚拟机 (VM) 必须连接到网络段。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表 1. 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：

这不包括虚拟机管理程序的任何磁盘要求。

对于 VPX 虚拟设备的生产用途，必须保留全部内存分配。

OVF Tool 1.0 系统要求

OVF Tool 是一款可在 Windows 和 Linux 系统上运行的客户端应用程序。下表描述了安装 OVF Tool 的系统要求。

表 2. OVF Tool 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/>` 搜索“OVF Tool 用户指南”PDF 文件。
CPU	最低 750 MHz，建议 1 GHz 或更快
RAM	最低 1 GB，建议 2 GB
网卡	100 Mbps 或更快的网卡

有关安装 OVF 的信息，请在 `<http://kb.vmware.com/>` 搜索“OVF Tool 用户指南”PDF 文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

下载 NetScaler VPX 安装文件

适用于 VMware ESX 的 NetScaler VPX 实例安装包遵循开放式虚拟机 (OVF) 格式标准。您可以从 Citrix 网站下载文件。您需要一个 Citrix 帐户才能登录。如果您没有 Citrix 帐户，请访问主页 http://www.citrix.com。单击“**新用户链接**”，然后按照说明创建一个新的 Citrix 帐户。

登录后，从 Citrix® 主页导航到以下路径：

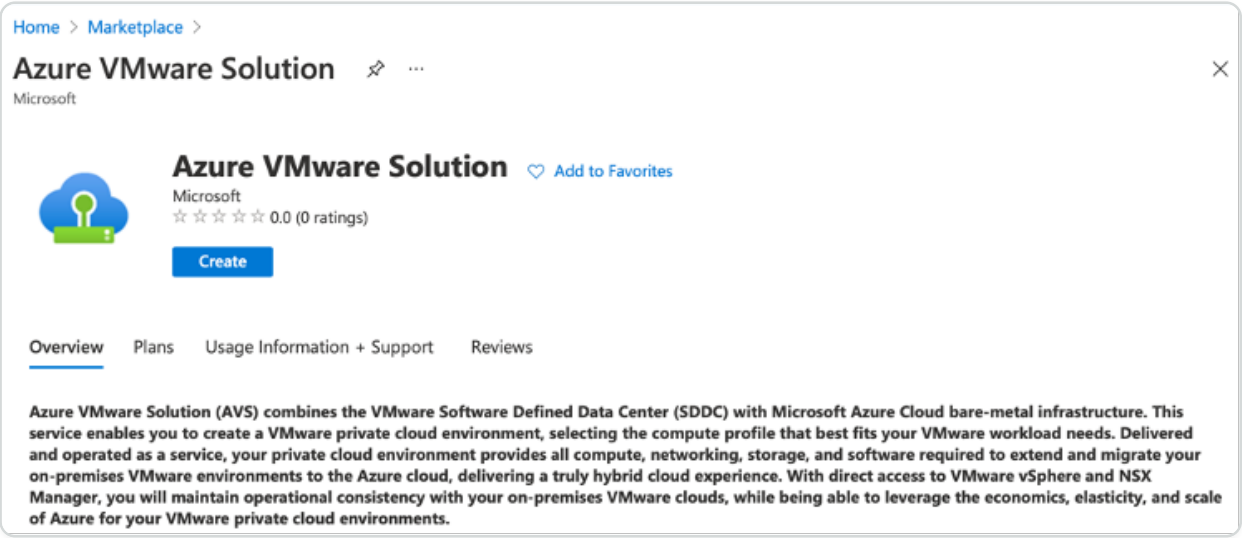
Citrix.com > **下载 > NetScaler > 虚拟设备**。

将以下文件复制到与 ESX 服务器位于同一网络的某个工作站。将所有三个文件复制到同一文件夹中。

- 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 Marketplace**”。
2. 在“**Azure Marketplace**”中，搜索“**Azure VMware Solution**”并单击“**创建**”。



3. 在“**创建私有云**”页面中，输入以下详细信息：
   - 选择至少 3 个 ESXi 主机来创建私有云的默认群集。
   - 对于“**地址块**”字段，使用 **/22** 地址空间。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 对于**虚拟网络**，请确保 CIDR 范围不与您的任何本地或其他 Azure 子网（虚拟网络）或网关子网重叠。
- 网关子网用于通过 ExpressRoute 连接到私有云。

创建私有云(/en-us/vpx/media/avs-create-private-cloud.png)

4. 单击“**审核 + 创建**”。
5. 审核设置。如果必须更改任何设置，请单击“**上一步**”。

   审核私有云设置(/en-us/vpx/media/review-private-cloud-settings.png)

6. 单击“**创建**”。私有云预配过程开始。私有云预配可能需要长达两小时。

   预配私有云(/en-us/vpx/media/provision-private-cloud.png)

7. 单击“**转到资源**”，以验证已创建的私有云。

   AVS 私有云(/en-us/vpx/media/avs-private-cloud.png)

注意

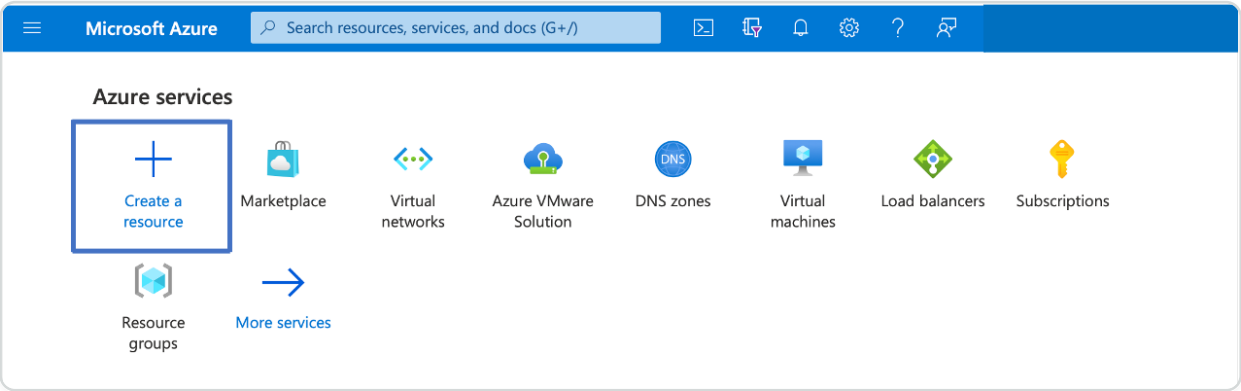
要访问此资源，您需要一台充当跳板机的 Windows 虚拟机。

连接到运行 Windows 的 Azure 虚拟机

此过程演示如何使用 Azure 门户在 Azure 中部署运行 Windows Server 2019 的虚拟机 (VM)。要查看 VM 的运行情况，您需要通过 RDP 连接到该 VM 并安装 IIS Web 服务器。

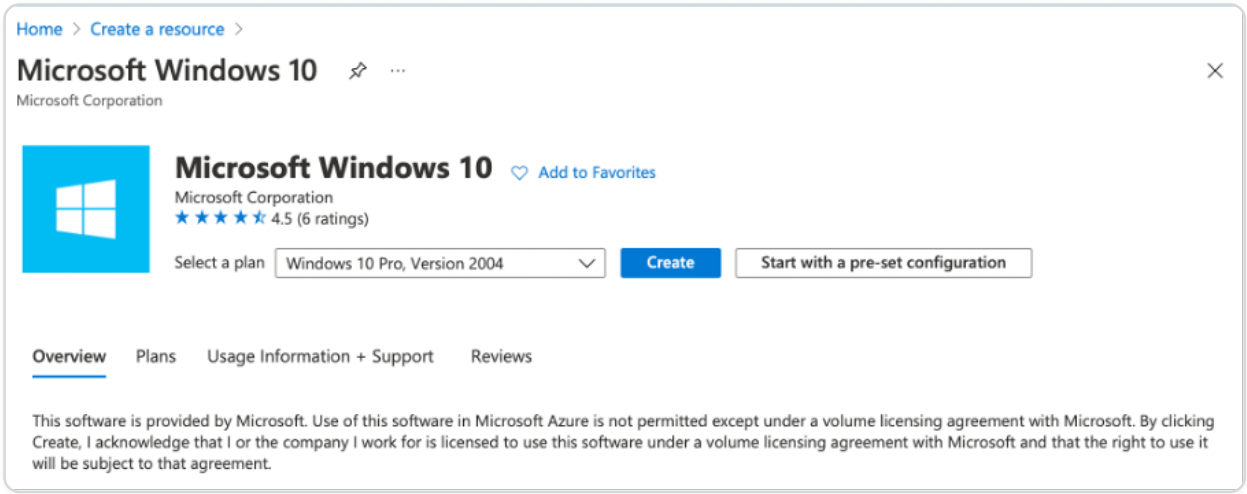
要访问您已创建的私有云，您需要在同一虚拟网络中创建一台 Windows 跳板机。

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**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 创建运行 Windows Server 2019 的虚拟机 (VM)。**创建虚拟机**页面随即出现。在**基本信息**选项卡中输入所有详细信息，并选中**许可**复选框。保留其余默认设置，然后选择页面底部的**查看 + 创建**按钮。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Home > Create a resource > Microsoft Windows 10 >

Create a virtual machine

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

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

Project details

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

Subscription *

Resource group *

Create new

Instance details

Virtual machine name * Windows-jumpbox

Region * (US) East US

Availability options No infrastructure redundancy required

Image * Windows 10 Pro, Version 2004 - Gen1

See all images

Azure Spot instance

Size * Standard_D2 - 2 vcpus, 7 GiB memory (US$67.16/m...

See all sizes

Administrator account

Username *

Password * ••••••••••••••

Confirm password * ••••••••••••••

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports *
- None
- Allow selected ports

Select inbound ports * RDP (3389)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Licensing

I confirm I have an eligible Windows 10 license with multi-tenant hosting rights. *

Review multi-tenant hosting rights for Windows 10 compliance

Review + create | < Previous | Next : Disks >

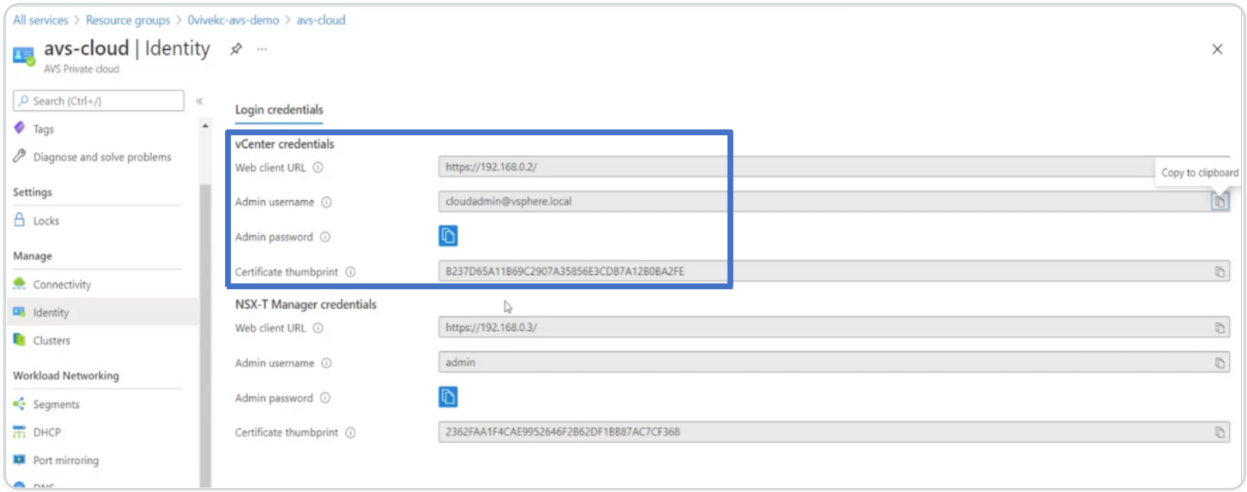
4. 验证运行后，选择页面底部的**创建**按钮。
5. 部署完成后，选择**转到资源**。
6. 转到您已创建的 Windows VM。使用 Windows VM 的公共 IP 地址并通过 RDP 连接。

   使用 Azure 门户中的**连接**按钮从 Windows 桌面启动远程桌面 (RDP) 会话。首先连接到虚拟机，然后登录。

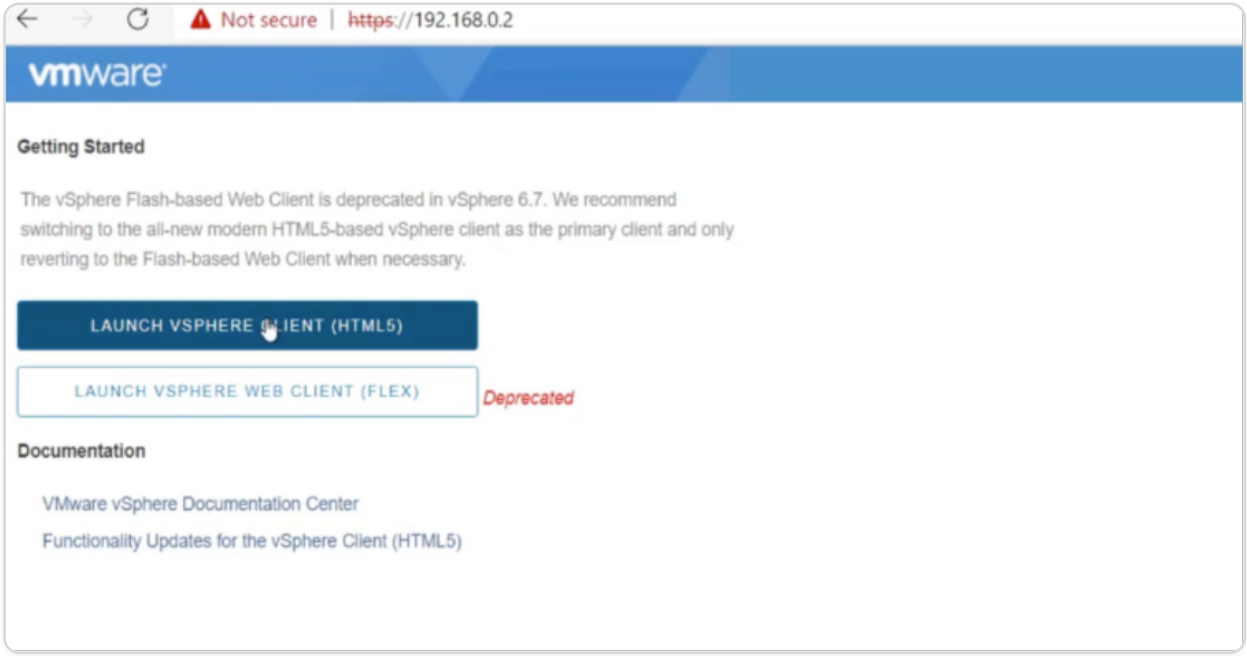
   要从 Mac 连接到 Windows VM，您必须安装适用于 Mac 的 RDP 客户端，例如 Microsoft 远程桌面。有关详细信息，请参阅如何连接并登录到运行 Windows 的 Azure 虚拟机。

访问您的私有云 vCenter 门户

1. 在您的 Azure VMware Solution 私有云中，在**管理**下，选择**身份**。记下 vCenter 凭据。

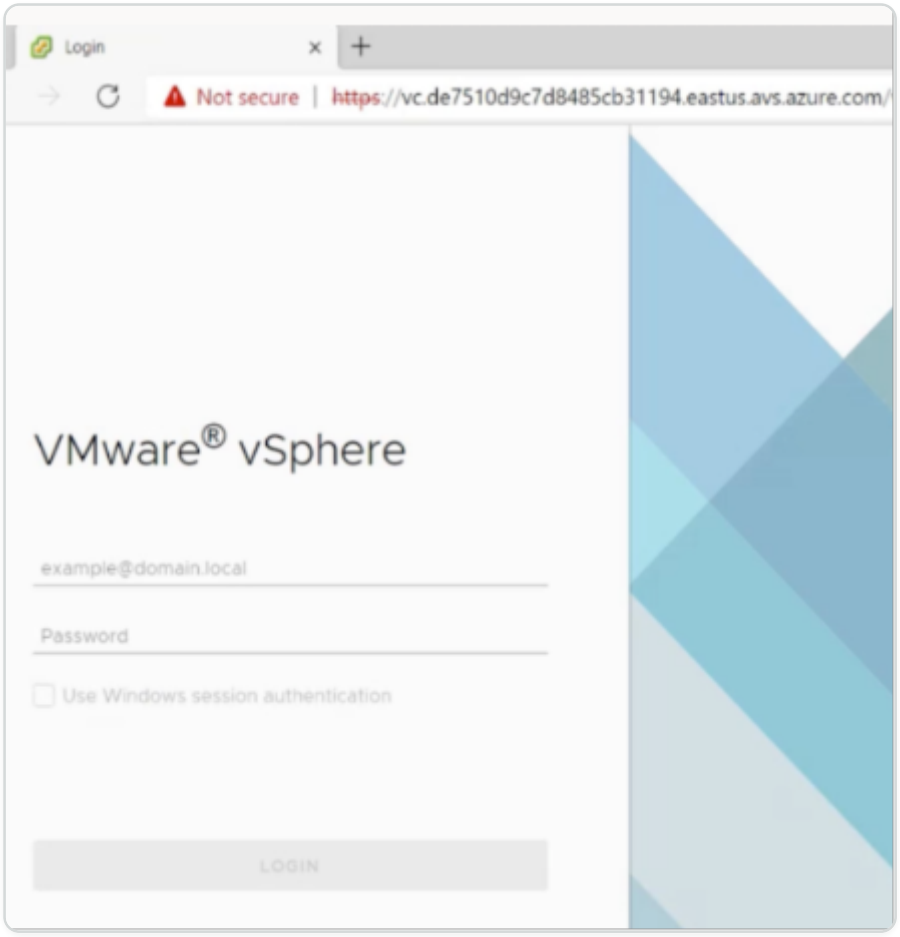


2. 通过键入 vCenter Web 客户端 URL 启动 vSphere 客户端。

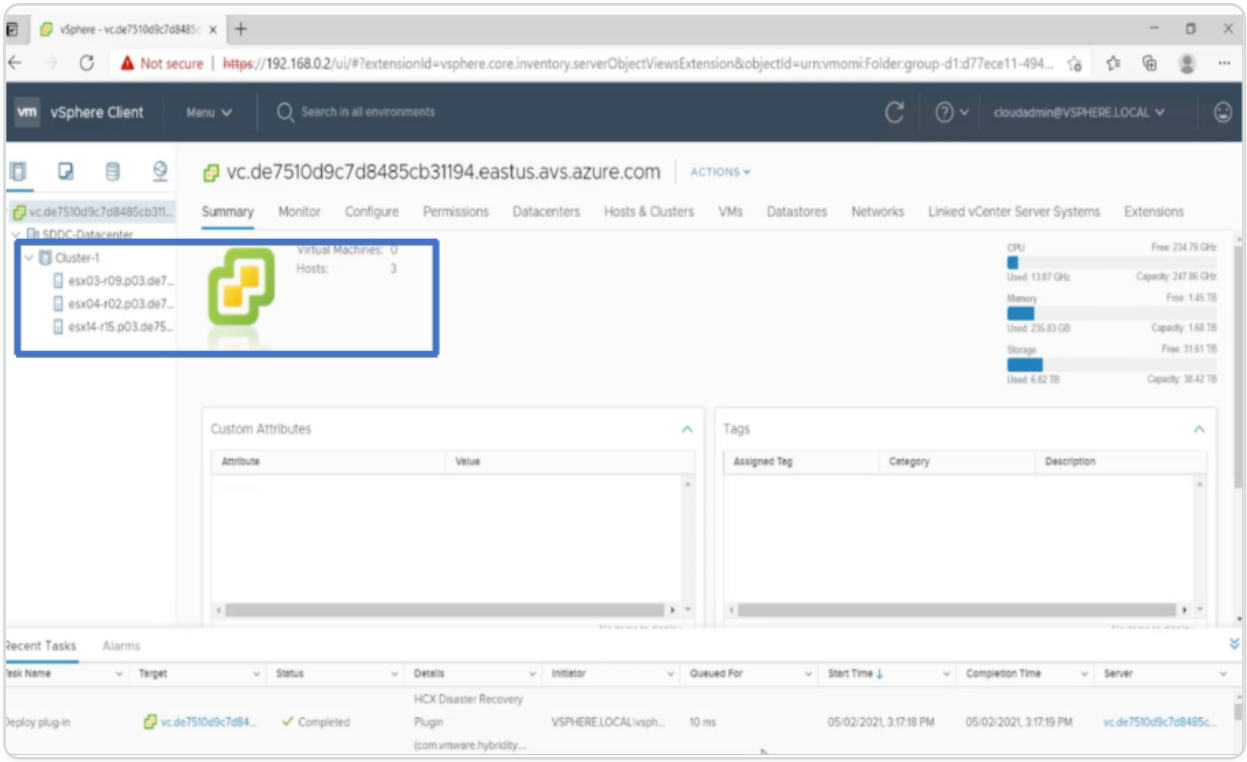


3. 使用您的 Azure VMware Solution 私有云的 vCenter 凭据登录到 VMware vSphere。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 在 vSphere 客户端中，您可以验证在 Azure 门户中创建的 ESXi 主机。



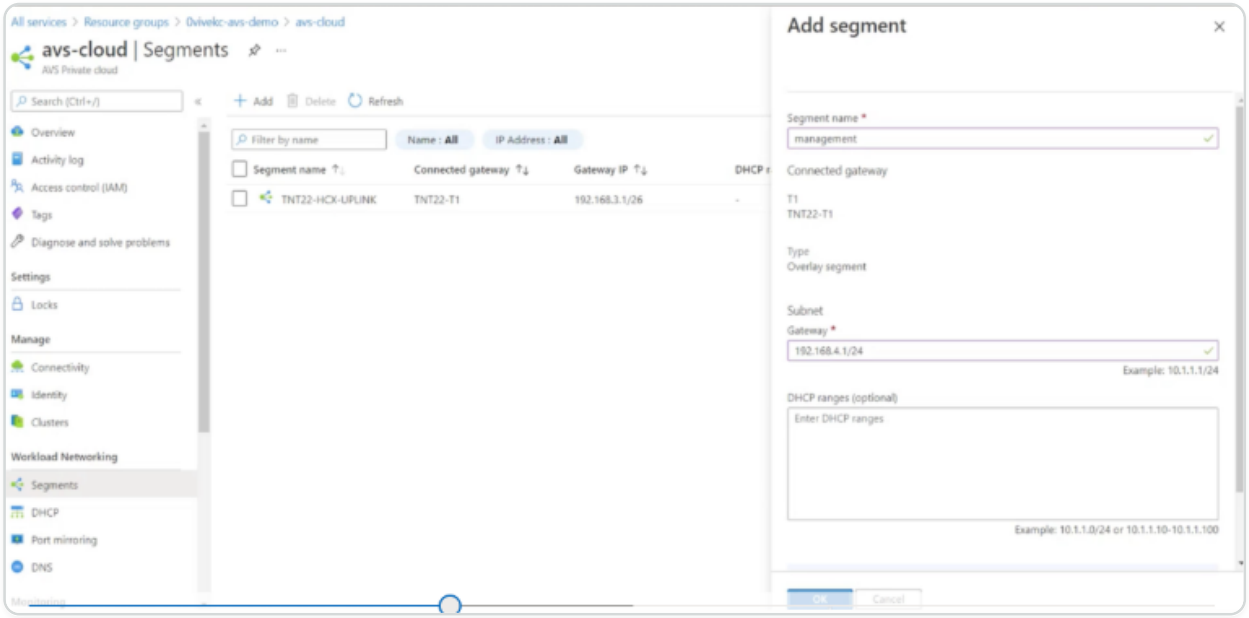
有关详细信息，请参阅 访问您的私有云 vCenter 门户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

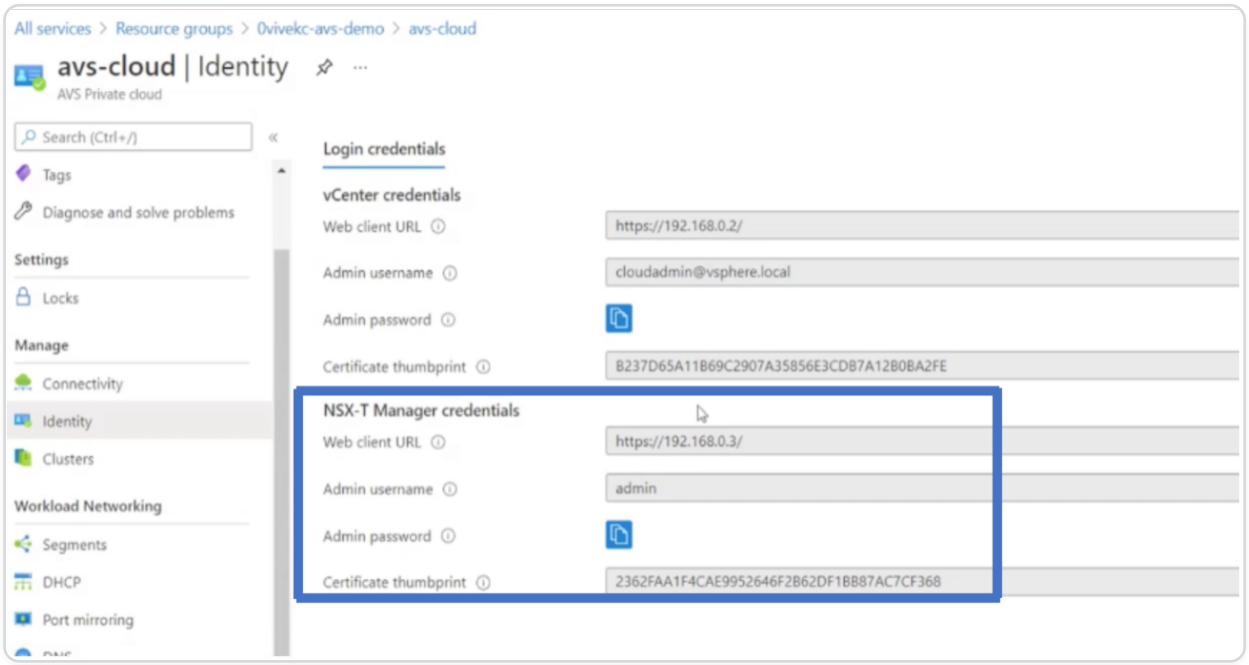
在 Azure 门户中创建 NSX-T 段

您可以在 Azure 门户中的 Azure VMware Solution 控制台中创建和配置 NSX-T 段。这些段连接到默认的 Tier-1 网关，这些段上的工作负载获得东西向和南北向连接。创建段后，它会显示在 NSX-T Manager 和 vCenter 中。

1. 在您的 Azure VMware Solution 私有云中，在“**工作负载网络**”下，选择“**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、管理和服务器接口创建三个单独的段。

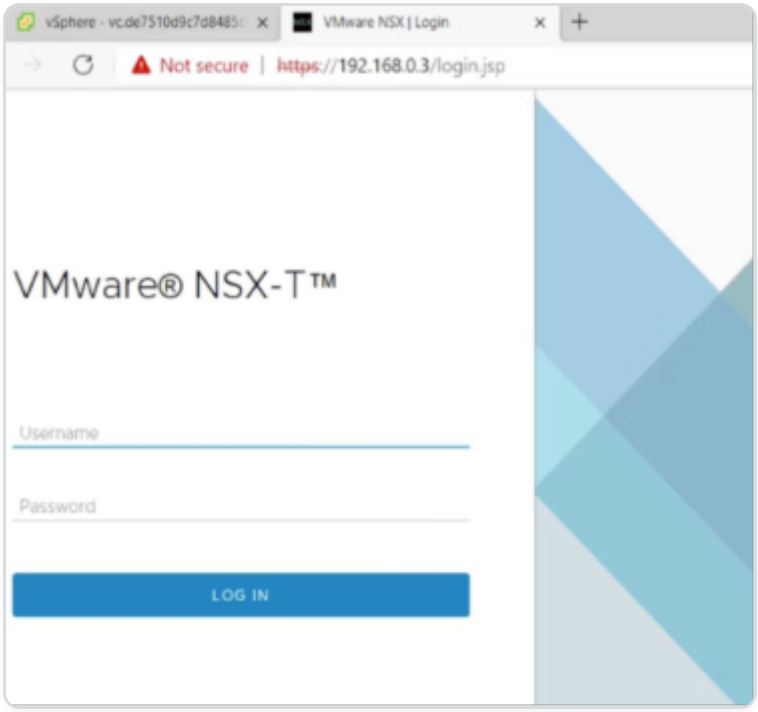


2. 在您的 Azure VMware Solution 私有云中，在“**管理**”下，选择“**身份**”。记下 NSX-T Manager 凭据。

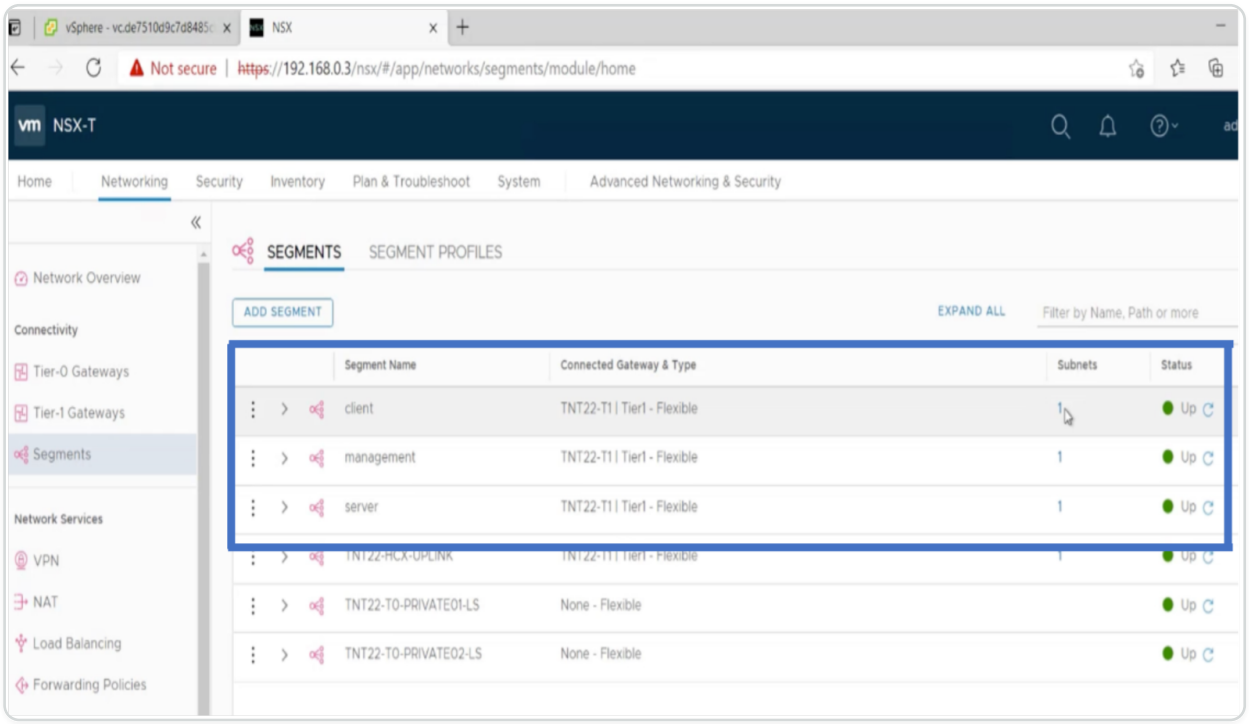


3. 通过键入 NSX-T Web 客户端 URL 启动 VMware NSX-T Manager。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 在 NSX-T Manager 中，在“**网络 > 段**”下，您可以看到所有已创建的段。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 分段。

在 VMware 云上安装 NetScaler VPX 实例

安装并配置 VMware 软件定义数据中心 (SDDC) 后，您可以使用 SDDC 在 VMware 云上安装虚拟设备。您可以安装的虚拟设备数量取决于 SDDC 上可用的内存量。

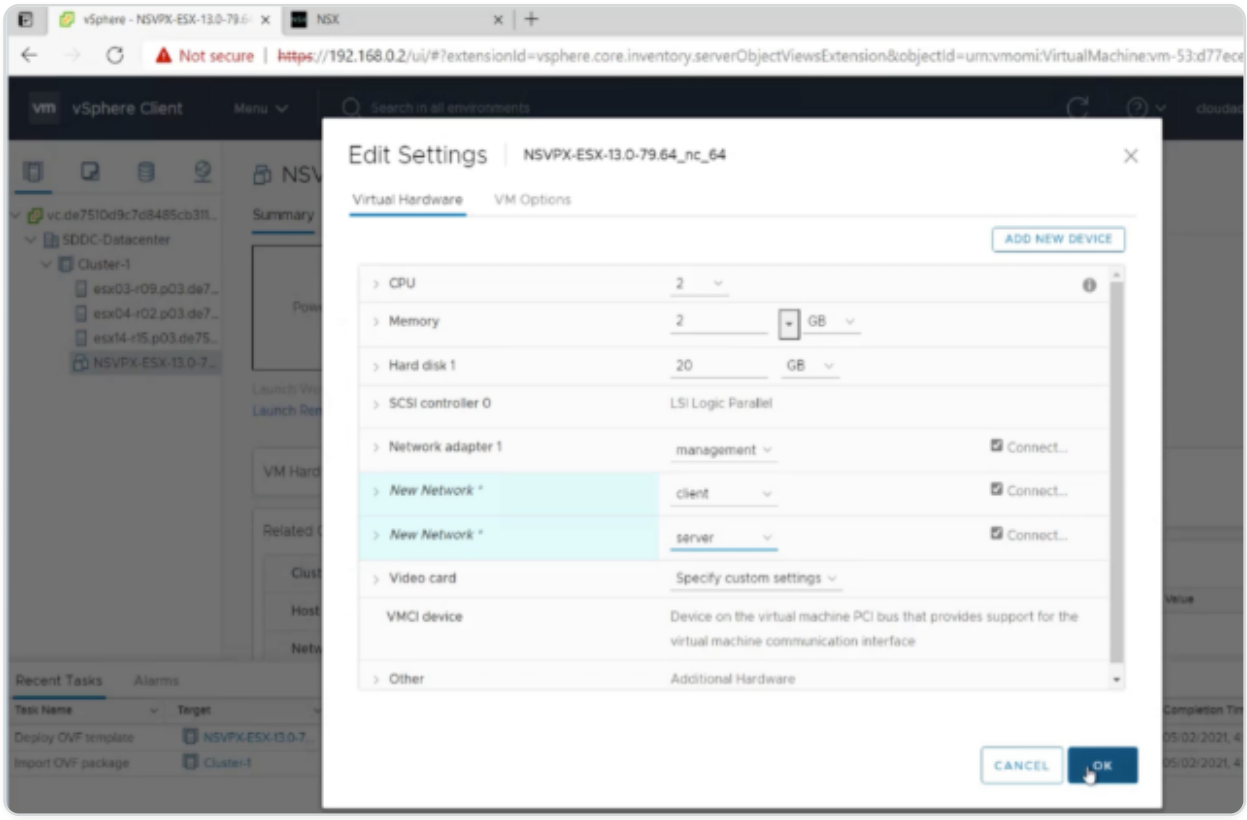
要在 VMware 云上安装 NetScaler VPX 实例，请在 Windows Jumpbox 虚拟机中执行以下步骤：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 从 NetScaler 下载站点下载适用于 ESXi 主机的 NetScaler VPX 实例安装文件。
2. 在 Windows Jumpbox 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“**文件**”菜单上，单击“**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，请修改 OVF 以使用 VMXNET3 接口而不是 E1000。VMXNET3 接口的可用性受 Azure 基础设施限制，并且可能在 Azure VMware Solution 中不可用。

6. 将虚拟设备 OVF 模板中显示的网络映射到您在 VMware SDDC 上配置的网络。单击“**确定**”。



7. 单击“**完成**”以开始在 VMware SDDC 上安装虚拟设备。

   部署 OVF 模板(/en-us/vpx/media/deploy-ovf-template.png)

8. 您现在可以启动 NetScaler VPX 实例了。在导航窗格中，选择您已安装的 NetScaler VPX 实例，然后从右键菜单中选择 **Power On**。单击 **Console** 选项卡以模拟控制台端口。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

启动 VPX 实例(/en-us/vpx/media/power-on-vpx-instance.png)

9. 您现在已通过 vSphere 客户端连接到 NetScaler VM。

   连接到 NetScaler VM(/en-us/vpx/media/avs-adc-vm.png)

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>
```

示例：

```
ssh nsroot@192.168.4.5
```

11. 您可以使用 `show ns ip` 命令验证 ADC 配置。

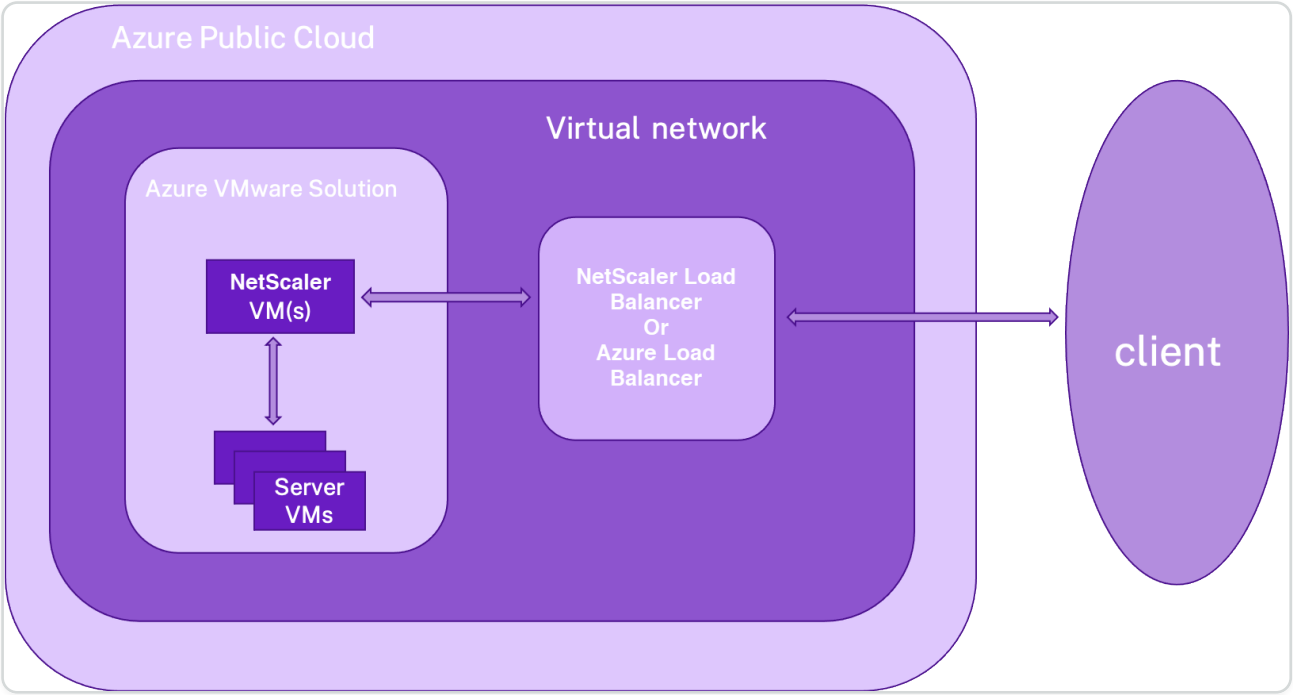
    使用 `show nsip` 命令进行验证(/en-us/vpx/media/avs-show-nsip-citrix.png)

在 Azure VMware 解决方案上配置 NetScaler VPX 独立实例

您可以在 Azure VMware 解决方案 (AVS) 上为面向 Internet 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 内部 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 虚拟网络中预置 NetScaler 负载均衡器或 Azure 负载均衡器实例来实现此目的。配置负载均衡器以访问 AVS 服务中 NetScaler VPX 实例的 VIP。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



先决条件

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 Solution 文档。
- 有关部署 Azure VMware 解决方案的更多信息，请参阅 部署 Azure VMware Solution 私有云。
- 有关创建 Windows Jump box VM 以访问和管理 Azure VMware 解决方案的更多信息，请参阅 访问 Azure VMware Solution 私有云。
- 在 Windows Jump box VM 中，下载 NetScaler VPX 设备安装文件。
- 在 VMware SDDC 上创建适当的 NSX-T 网络段，虚拟机将连接到这些网络段。有关更多信息，请参阅 在 Azure VMware Solution 中添加网络段
- 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 负载均衡器在 AVS 上配置 NetScaler VPX 独立实例

请按照以下步骤使用 NetScaler 负载均衡器在 AVS 上为面向 Internet 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

确保它部署在与 Azure VMware Cloud 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. 添加一个负载均衡虚拟服务器。

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

   示例：

   ```
   add lb vserver lb1 HTTPS 172.31.0.6 443
   ```

   b. 添加一个连接到部署在 AVS 上的 NetScaler VPX 的 VIP 的服务。

   ```
   add service <name> <ip> <serviceType> <port>
   ```

   示例：

   ```
   add service webserver1 192.168.4.10 HTTP 80
   ```

   c. 将服务绑定到负载均衡虚拟服务器。

   ```
   bind lb vserver <name> <serviceName>
   ```

   示例：

   ```
   bind lb vserver lb1 webserver1
   ```

使用 Azure 负载均衡器在 AVS 上配置 NetScaler VPX 独立实例

按照以下步骤，使用 Azure 负载均衡器在 AVS 上为面向 Internet 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。有关更多信息，请参阅有关创建负载均衡器的 Azure 文档。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 将部署在 AVS 上的 NetScaler VPX 实例的 VIP 地址添加到后端池。

   以下 Azure 命令将一个后端 IP 地址添加到负载均衡后端地址池中。

```
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：

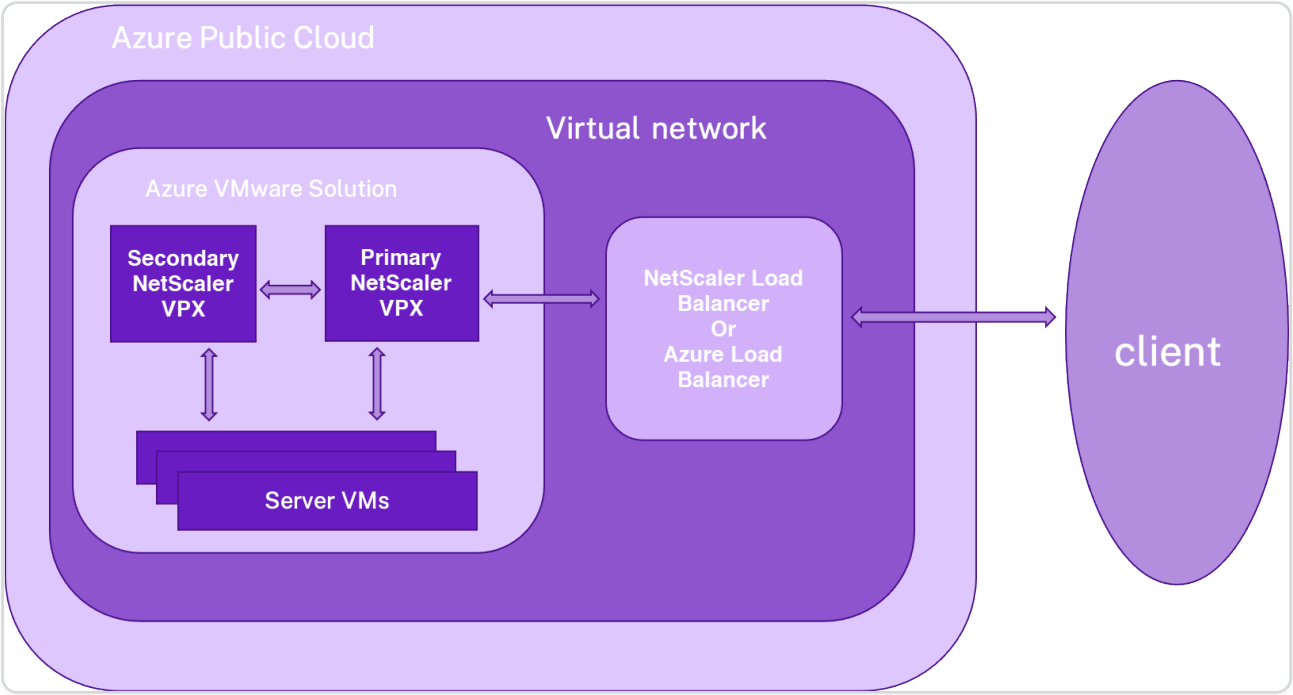
确保 Azure 负载均衡器部署在与 Azure VMware 云相同的虚拟网络中。

在 Azure VMware 解决方案上配置 NetScaler VPX 高可用性设置

您可以在 Azure VMware 解决方案 (AVS) 上为面向 Internet 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 内部主 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 虚拟网络中预置 NetScaler 负载均衡器或 Azure 负载均衡器实例来实现此目的。配置负载均衡器以访问 AVS 服务内主 ADC 节点的 VIP。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



先决条件

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 Solution 文档。
- 有关部署 Azure VMware 解决方案的更多信息，请参阅 部署 Azure VMware Solution 私有云。
- 有关创建 Windows Jump box VM 以访问和管理 Azure VMware 解决方案的更多信息，请参阅 访问 Azure VMware Solution 私有云。
- 在 Windows Jump box VM 中，下载 NetScaler VPX 设备安装文件。
- 在 VMware SDDC 上创建虚拟机连接到的相应 NSX-T 网络段。有关更多信息，请参阅 在 Azure VMware Solution 中添加网络段。

配置步骤

请按照以下步骤在 AVS 中为面向 Internet 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. 配置 NetScaler HA 设置，使其可供面向互联网的应用程序访问。
    - 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。

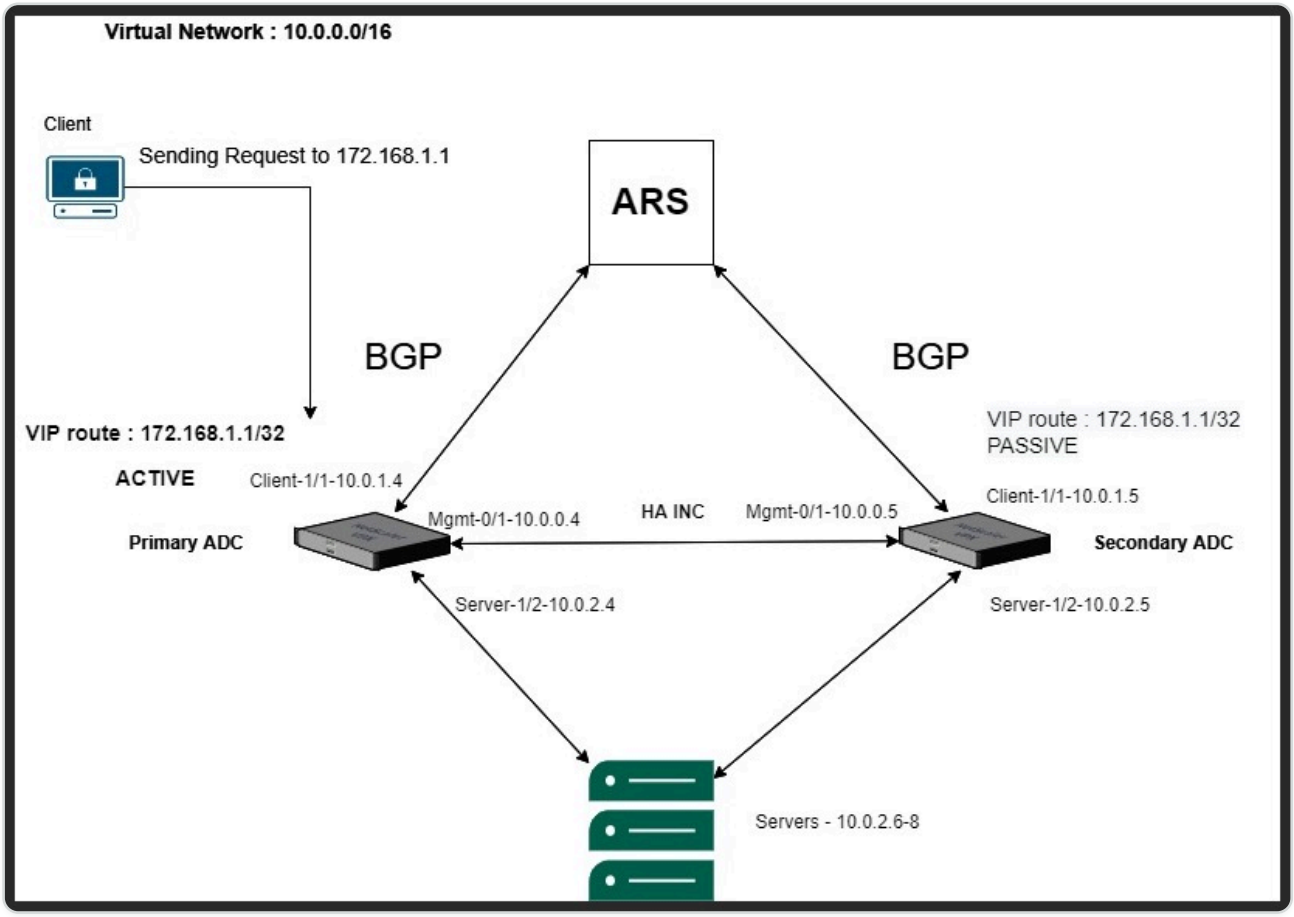
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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。

配置 Azure 路由服务器与 NetScaler VPX HA 对

您可以将 Azure 路由服务器与 NetScaler VPX 实例配置，以使用 BGP 协议交换配置了虚拟网络的 VIP 路由。NetScaler 可以部署为独立模式或 HA-INC 模式，然后配置 BGP。此部署不需要在 ADC HA 对前面部署 Azure 负载均衡器 (ALB)。

下图描述了 VPX HA 拓扑如何与 Azure 路由服务器集成。每个 ADC 实例有 3 个接口：一个用于管理，一个用于客户端流量，一个用于服务器流量。



拓扑图使用以下 IP 地址。

主 ADC 实例的示例 IP 配置：

```
NSIP: 10.0.0.4/24

SNIP on 1/1: 10.0.1.4/24

SNIP on 1/2: 10.0.2.4/24
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
VIP: 172.168.1.1/32
```

辅助 ADC 实例的示例 IP 配置：

```
NSIP: 10.0.0.5/24

SNIP on 1/1: 10.0.1.5/24

SNIP on 1/2: 10.0.2.5/24

VIP: 172.168.1.1/32
```

先决条件

在 Azure 上部署 NetScaler VPX 实例之前，您必须熟悉以下信息。

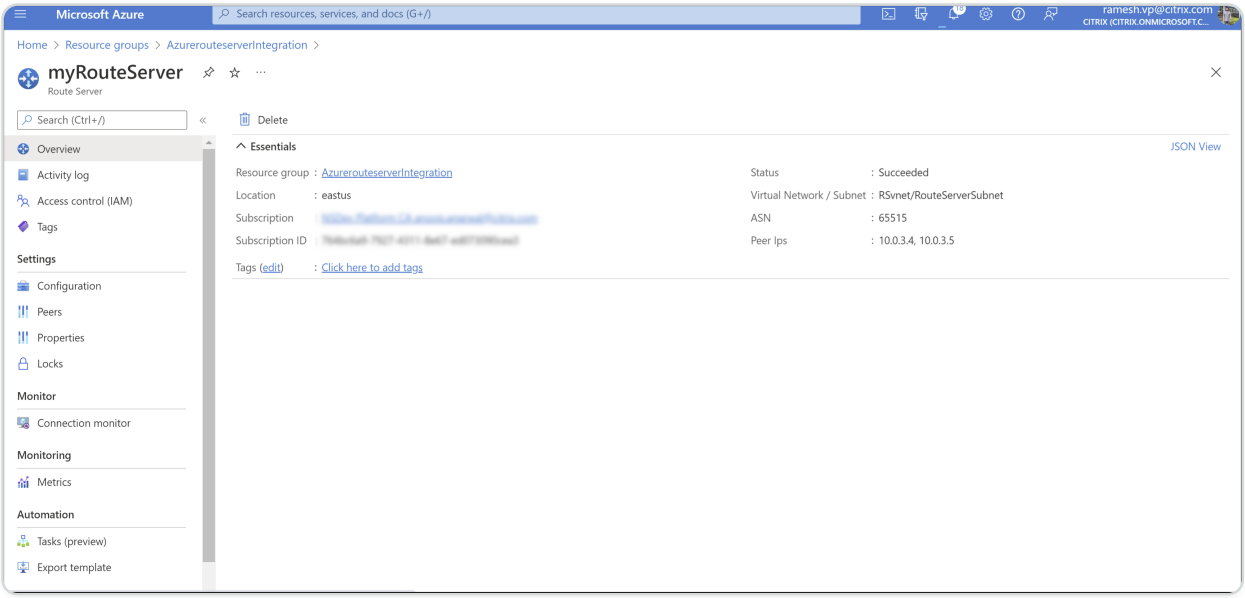
- Azure 术语和网络详细信息。有关更多信息，请参阅 Azure 术语。
- Azure 路由服务器概述。有关更多信息，请参阅 什么是 Azure 路由服务器？。
- NetScaler 设备的工作原理。有关更多信息，请参阅 NetScaler 文档。
- NetScaler 网络。有关更多信息，请参阅 ADC 网络。

如何配置 Azure 路由服务器与 NetScaler VPX HA 对

1. 在 Azure 门户中创建路由服务器。有关更多信息，请参阅 使用 Azure 门户创建和配置路由服务器。

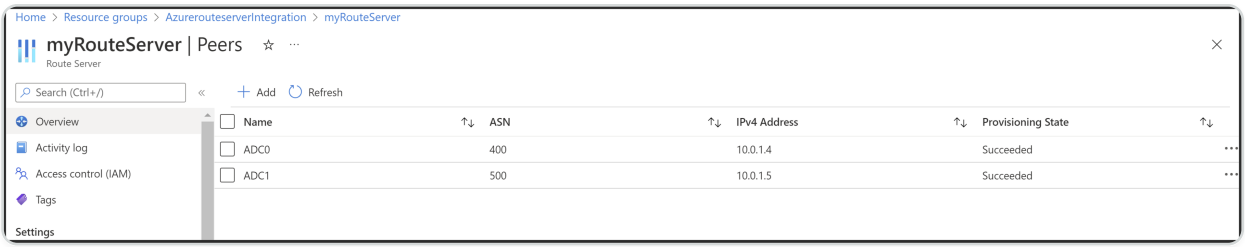
   在以下示例中，子网 10.0.3.0/24 用于部署 Azure 服务器。创建路由服务器后，获取路由服务器 IP 地址，例如：10.0.3.4、10.0.3.5。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 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，添加对等体时使用了 1/1 接口上的 ADC SNIP：10.0.1.4 和 10.0.1.5，以及 ASN：400 和 500。



3. 为 HA 配置添加两个 NetScaler VPX 实例。

   完成以下步骤：

   a. 在 Azure 上部署两个 VPX 实例（主实例和辅助实例）。
   b. 在两个实例上添加客户端和服务器 NIC。
   c. 使用 NetScaler GUI 在两个实例上配置 HA 设置。

4. 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
ENABLED

VTYSH

configure terminal

router BGP 400

timers bgp 1 3

neighbor 10.0.3.4 remote-as 65515

neighbor 10.0.3.4 advertisement-interval 3

neighbor 10.0.3.4 fall-over  bfd

neighbor 10.0.3.5 remote-as 65515

neighbor 10.0.3.5 advertisement-interval 3

neighbor 10.0.3.5 fall-over  bfd

address-family ipv4

redistribute kernel

redistribute static
```

5. 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
router BGP 500

timers bgp 1 3

neighbor 10.0.3.4 remote-as 65515

neighbor 10.0.3.4 advertisement-interval 3

neighbor 10.0.3.4 fall-over  bfd

neighbor 10.0.3.5 remote-as 65515

neighbor 10.0.3.5 advertisement-interval 3

neighbor 10.0.3.5 fall-over  bfd

address-family ipv4

redistribute kernel

redistribute static
```

6. 使用 VTY shell 界面中的 BGP 命令验证已建立的 BGP 对等体。有关更多信息，请参阅验证 BGP 配置。

```
show ip bgp neighbors
```

7. 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

位于与 NetScaler VPX 实例相同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。

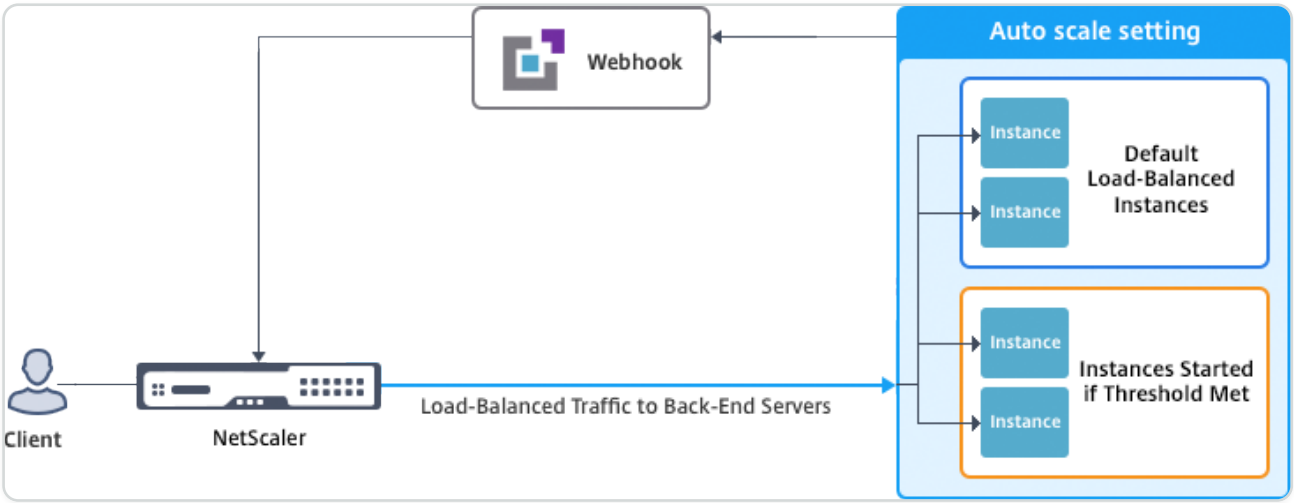
添加 Azure Autoscale™ 设置

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。为满足不断增长的需求，您必须向上扩展网络资源。无论需求是否减弱，您都必须向下扩展以避免空闲资源造成不必要的成本。为了最大限度地降低应用程序运行成本，您必须持续监控流量、内存和 CPU 使用情况等。然而，手动监控流量很麻烦。为了使应用程序环境能够动态地向上或向下扩展，您必须在必要时自动化监控流量以及向上和向下扩展资源的过程。

您可以将 Autoscale 与 Azure 虚拟机规模集 (VMSS) 结合使用，用于在 Azure 上进行 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，提供了以下优势：

- 负载平衡和管理：根据需求自动配置服务器以进行向上和向下扩展。NetScaler VPX 实例会自动检测部署 VPX 实例的同一虚拟网络中或同一 Azure 订阅中的对等虚拟网络中的 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 应用中的自动缩放概述

© 1997–2026 Citrix Systems, Inc. All rights reserved.

开始之前

1. 阅读 Azure 相关使用指南。有关详细信息，请参阅 在 Microsoft Azure 上部署 NetScaler VPX 实例。
2. 根据您的要求（独立部署或高可用性部署），在 Azure 上创建一个或多个具有三个网络接口的 NetScaler VPX 实例。
3. 在 VPX 实例的 0/1 接口的网络安全组上打开 TCP 9001 端口。VPX 实例使用此端口接收横向扩展和横向缩减通知。
4. 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。
   - 两个虚拟网络必须使用 Azure 的虚拟网络对等互连功能进行连接。

   如果您没有现有的 VMSS 配置，请完成以下任务：

   a) 创建 VMSS

   b) 在 VMSS 上启用自动缩放

   c) 在 VMSS 自动缩放设置中创建缩减和扩展策略

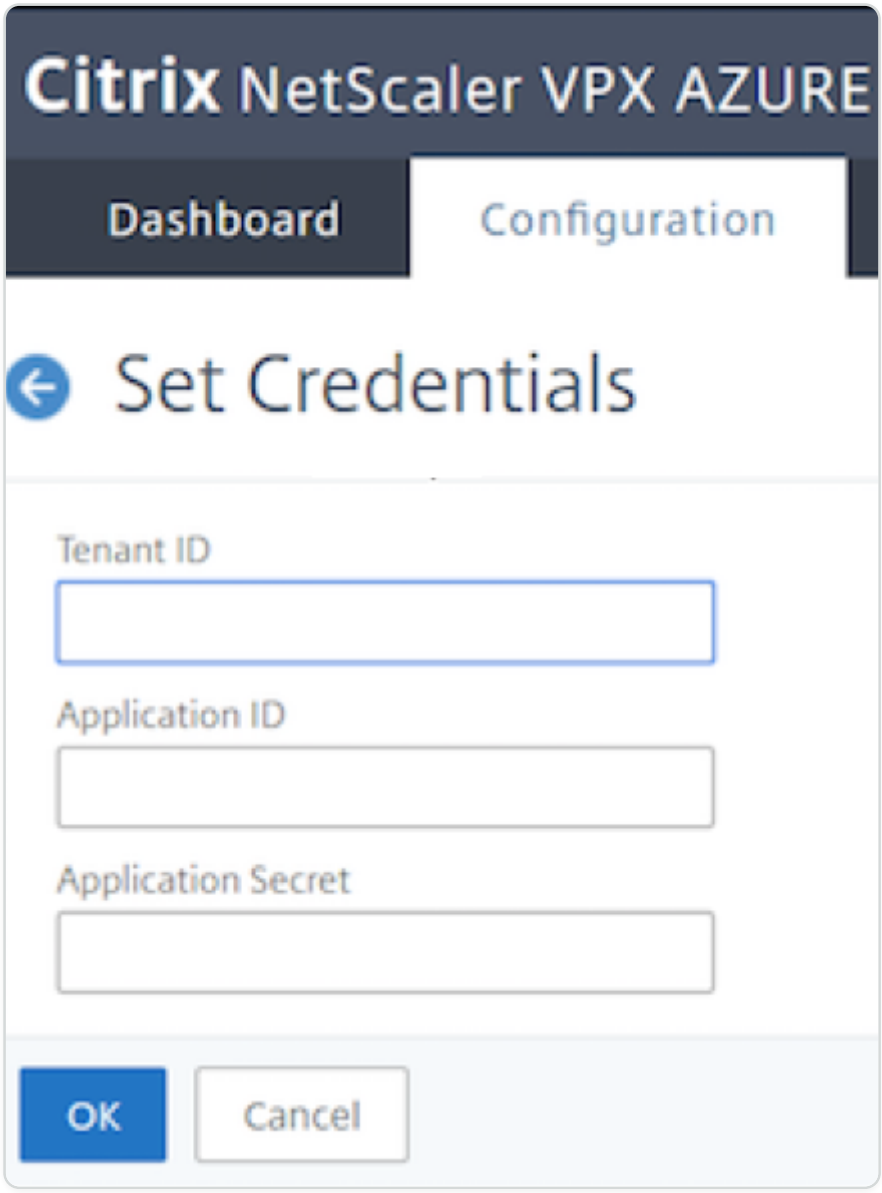
   有关更多信息，请参阅 Azure 虚拟机规模集的自动缩放概述。
5. 创建可以访问资源的 Azure Active Directory (AAD) 应用程序和服务主体。为新创建的 AAD 应用程序分配参与者角色。有关更多信息，请参阅 使用门户创建可以访问资源的 Azure Active Directory 应用程序和服务主体。

将 VMSS 添加到 NetScaler VPX 实例

您可以使用 GUI 一键将自动缩放设置添加到 VPX 实例。完成以下步骤以将自动缩放设置添加到 VPX 实例：

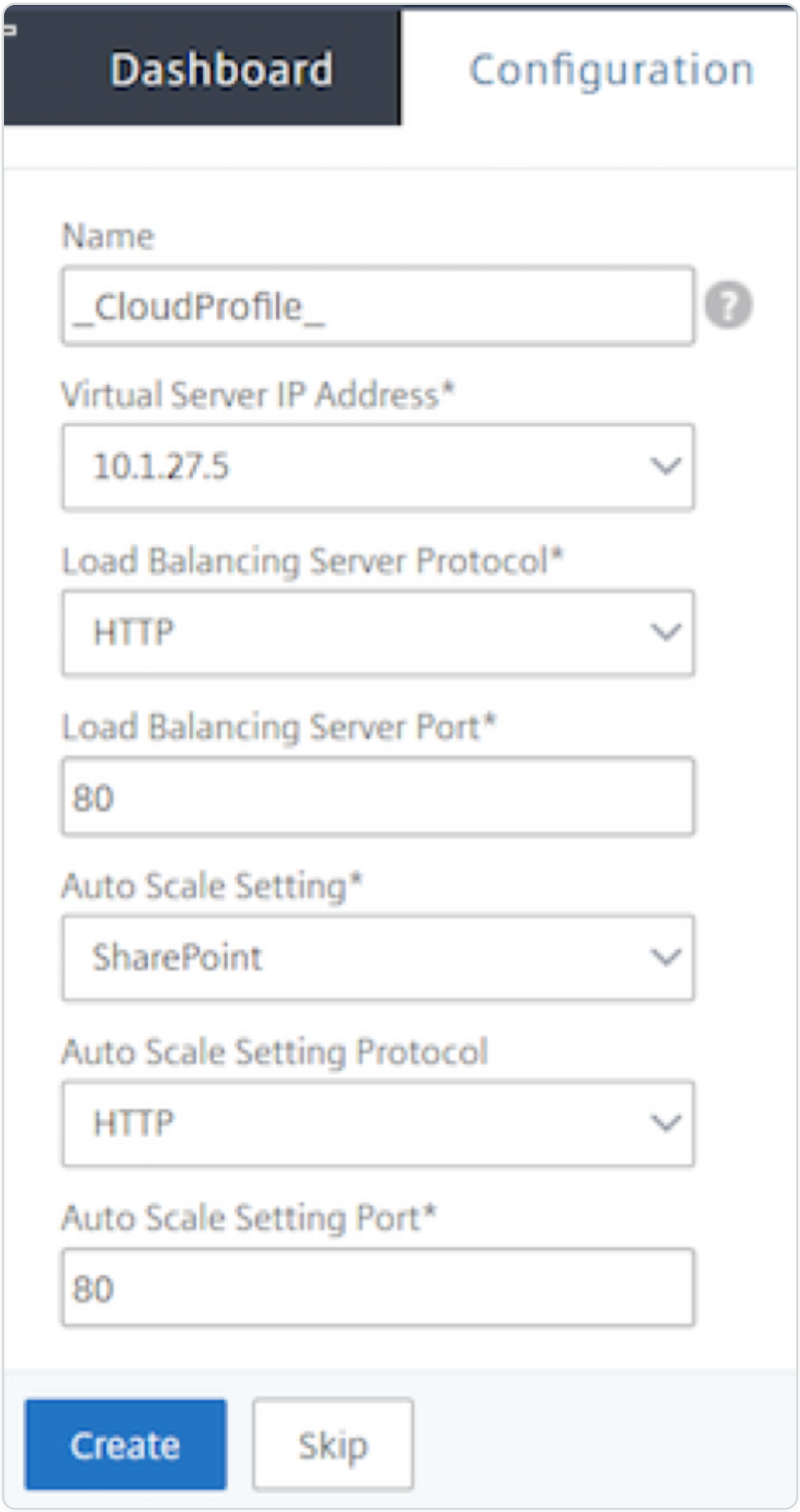
1. 登录到 VPX 实例。
2. 首次登录 NetScaler VPX 实例时，您会看到“设置凭据”页面。添加所需的 Azure 凭据以使自动缩放功能正常工作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 在默认云配置文件页面中，输入详细信息（如以下示例所示），然后单击“创建”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

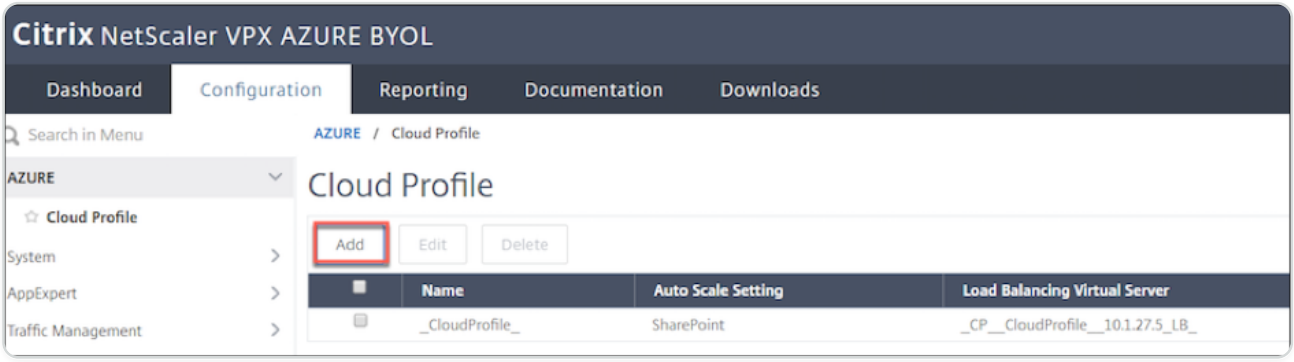


© 1997–2026 Citrix Systems, Inc. All rights reserved.

创建云配置文件时需要注意的事项

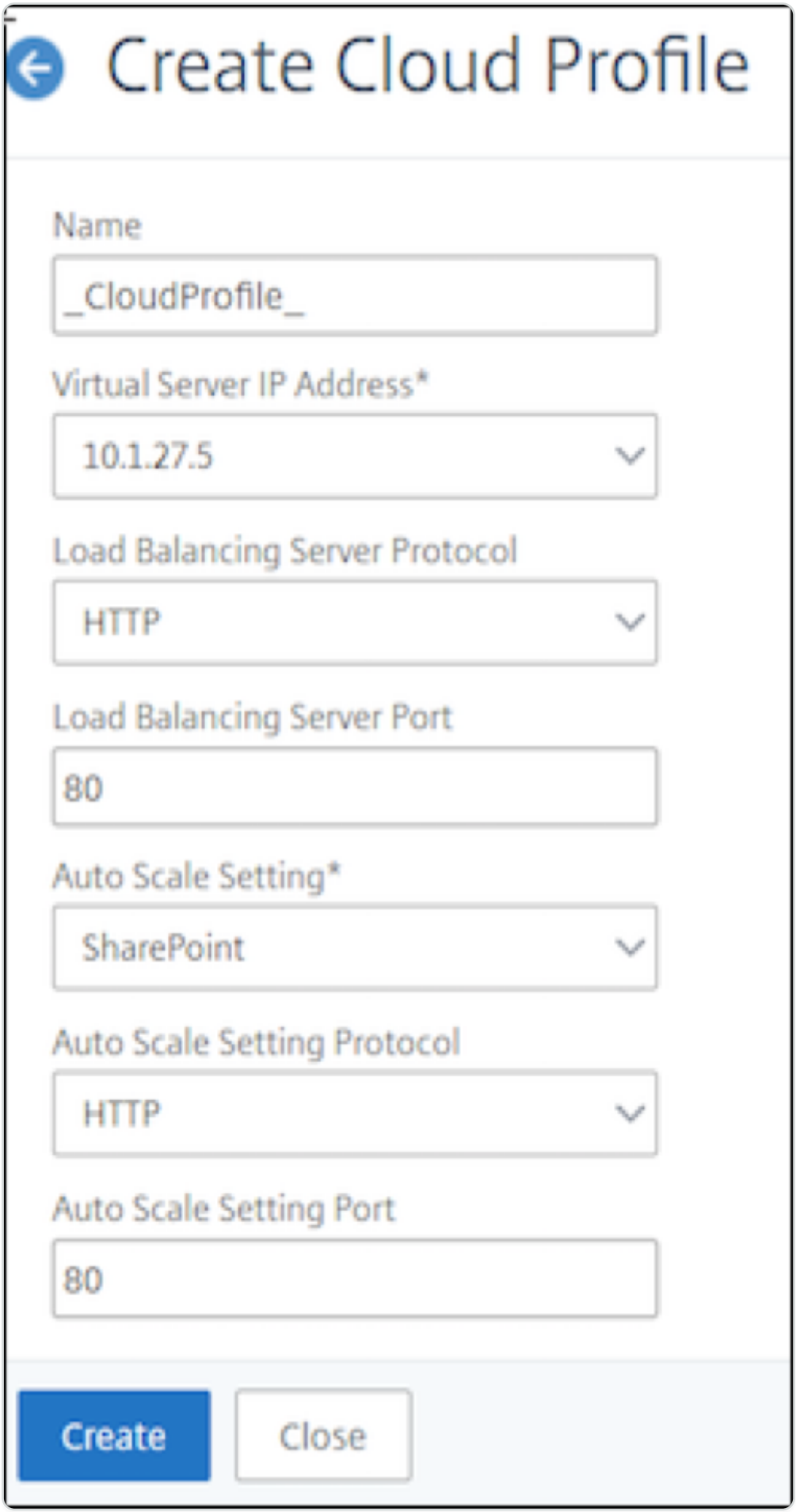
- 虚拟服务器 IP 地址将从 VPX 实例可用的空闲 IP 地址自动填充。有关详细信息，请参阅 使用 Azure 门户为虚拟机分配多个 IP 地址。
- 自动缩放设置将从连接到 NetScaler VPX 实例的 VMSS 实例预填充，该实例位于同一虚拟网络或对等虚拟网络中。有关详细信息，请参阅 Azure 虚拟机规模集自动缩放概述。
- 选择自动缩放组协议和端口时，请确保您的服务器侦听这些协议和端口，并且您在服务组中绑定了正确的监视器。默认情况下，使用 TCP 监视器。
- 对于 SSL 协议类型的自动缩放，创建云配置文件后，由于缺少证书，负载均衡虚拟服务器或服务组将处于关闭状态。您可以手动将证书绑定到虚拟服务器或服务组。

首次登录后，如果要创建云配置文件，请在 GUI 中转到 **System > Azure > Cloud Profile**，然后单击 **Add**。



此时将显示“创建云配置文件”配置页面。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

云配置文件会创建一个 NetScaler 负载均衡虚拟服务器和一个服务组，其成员（服务器）即为自动缩放组的服务器。您的后端服务器必须可通过在 VPX 实例上配置的 SNIP 访问。

注意：

从 NetScaler 13.1-42.x 版本开始，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 实例在公有云中支持具有相同自动缩放组的多个服务。

要在 Azure 门户中查看与自动缩放相关的信息，请转到 **All service > Virtual machine scale set > Select Virtual machine scale set > Scaling**。

在 Azure 中从非托管磁盘迁移到托管磁盘

如果您的 NetScaler VPX 实例或 VMSS 使用非托管磁盘部署，则需要迁移到托管磁盘以适应 Azure 云的变化。有关迁移指南和相关常见问题，请参阅以下 Azure 文档：

- 将 Linux 虚拟机从非托管磁盘迁移到托管磁盘
- 常见问题

参考

有关使用 NetScaler Application Delivery and Management 在 Microsoft Azure 中自动缩放 NetScaler VPX 的信息，请参阅 使用 NetScaler ADM 进行 Azure 自动缩放。

用于 NetScaler VPX 部署的 Azure 标签

在 Azure 云门户中，您可以为资源添加名称:值对标签（例如，部门:财务），以便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，标记功能会很有帮助。

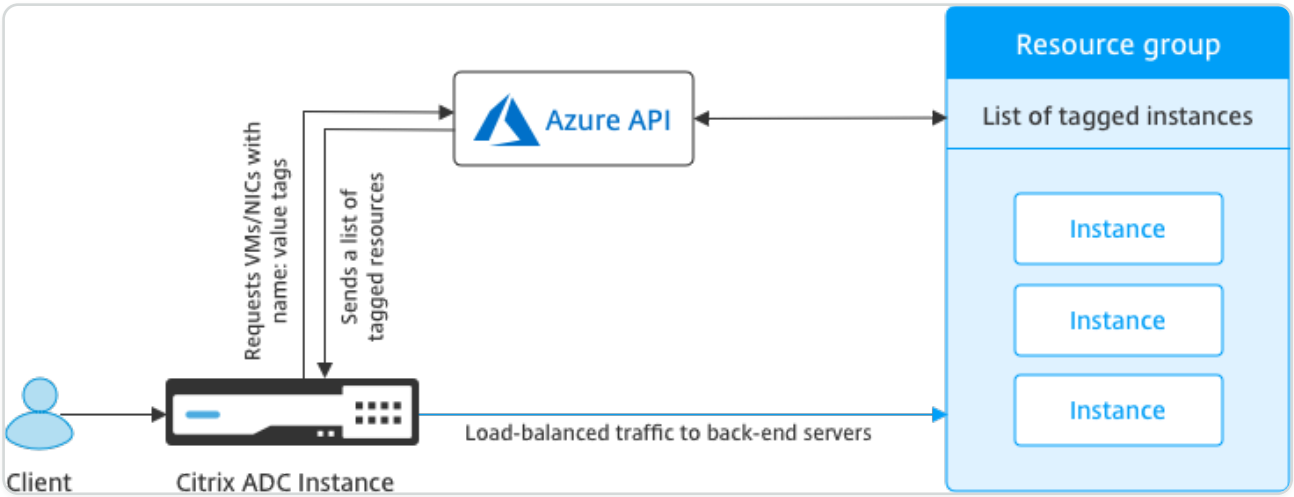
Azure 标签如何用于 VPX 部署

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 实例会持续监控带有相应标签的 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 实例使用标签创建负载平衡后端服务器的服务组。该实例查询 Azure API，以查找所有带有特定标签名称和标签值的资源。根据分配的轮询周期（默认为 60 秒），VPX 实例会定期轮询 Azure

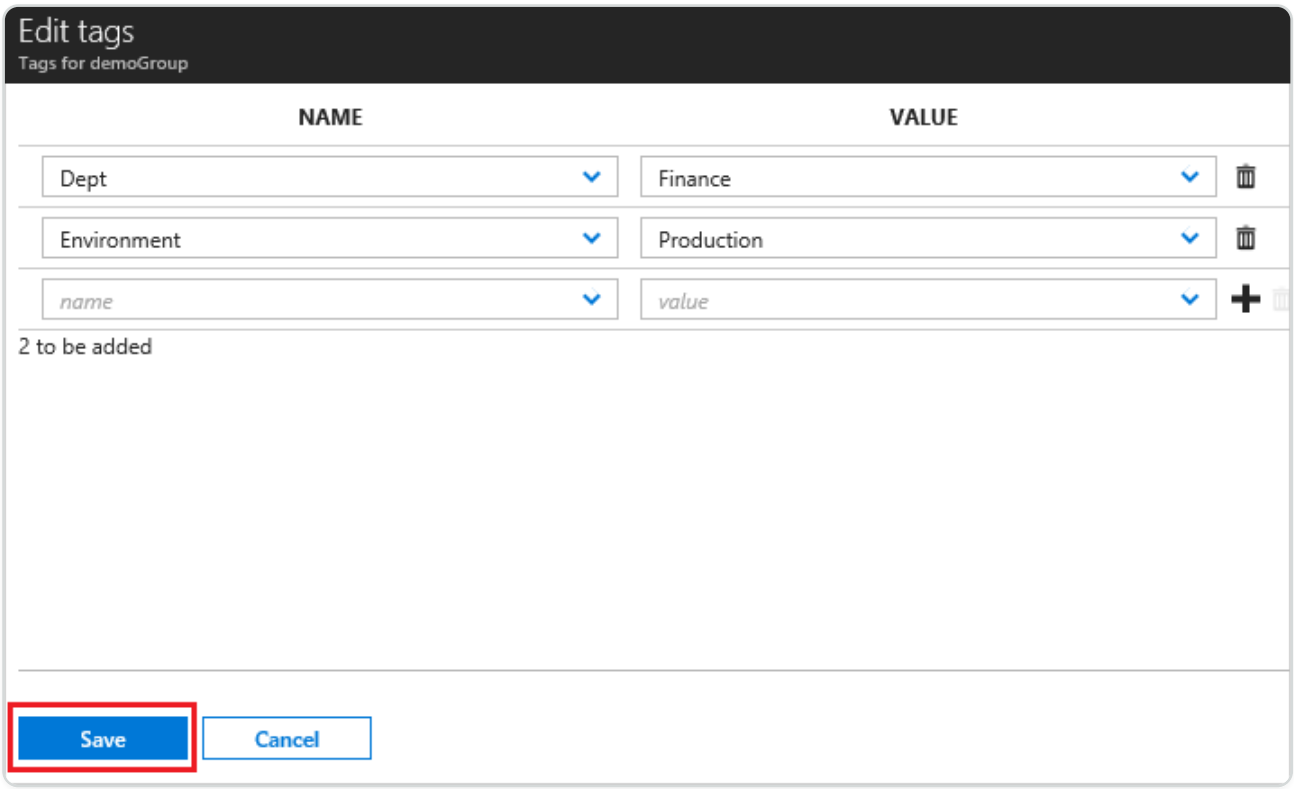
© 1997–2026 Citrix Systems, Inc. All rights reserved.

API，并检索在 VPX GUI 中分配了标签名称和标签值的可用资源。每当添加或删除带有相应标签的 VM 或 NIC 时，ADC 都会检测到相应的更改，并自动从服务组中添加或删除 VM 或 NIC IP 地址。



开始之前

在创建 NetScaler 负载平衡服务组之前，请在 Azure 中为服务器添加标签。您可以将标签分配给虚拟机或 NIC。



有关添加 Azure 标签的更多信息，请参阅 Microsoft 文档 使用标签组织 Azure 资源。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

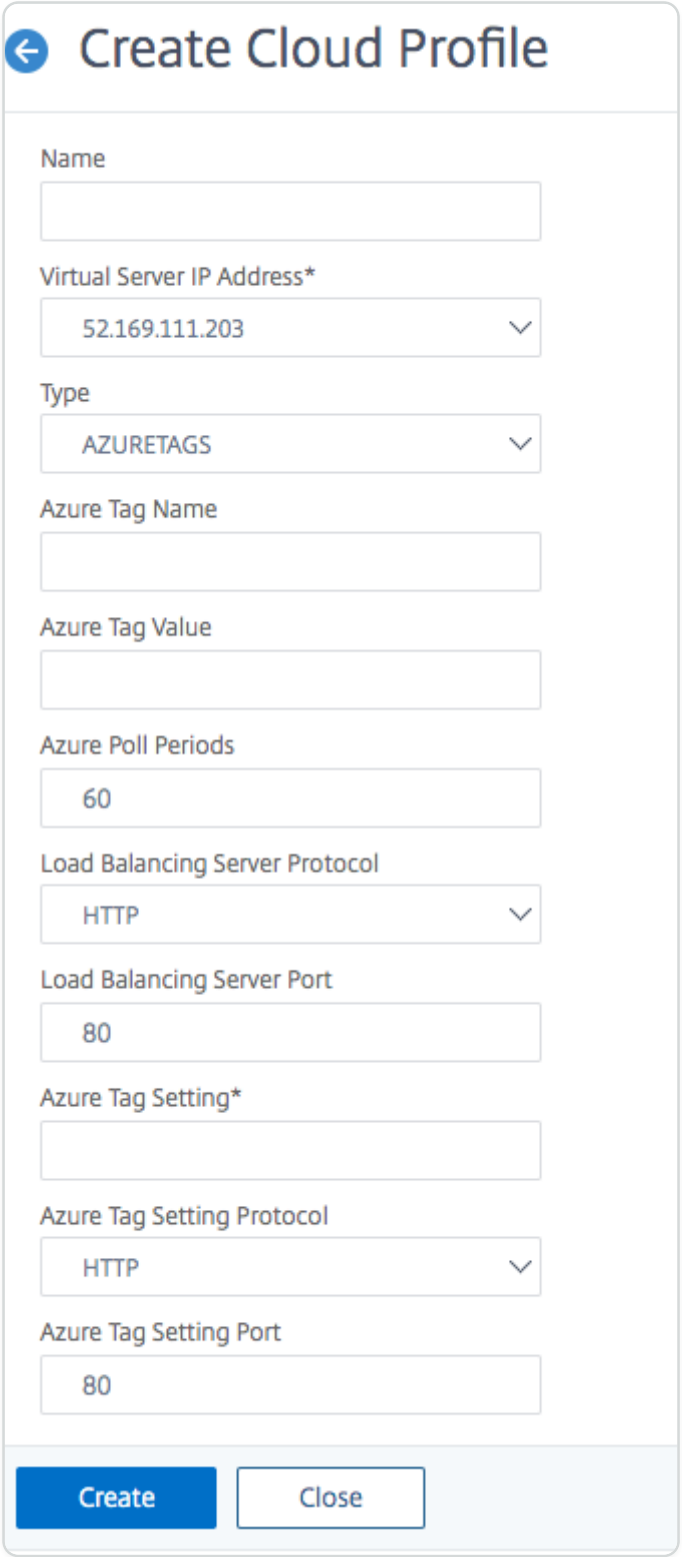
用于添加 Azure 标签设置的 ADC CLI 命令支持仅以数字或字母开头而不是其他键盘字符的标签名称和标签值。

如何通过使用 VPX GUI 添加 Azure 标签设置

您可以通过使用 VPX GUI 将 Azure 标签云配置文件添加到 VPX 实例，以便该实例可以使用指定的标签对后端服务器进行负载平衡。请按照以下步骤操作：

1. 在 VPX GUI 中，转到**配置 > Azure > 云配置文件**。
2. 点击添加以创建云配置文件。云配置文件窗口打开。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. 输入以下字段的值：

   - 名称：为您的配置文件添加名称
   - 虚拟服务器 IP 地址：虚拟服务器 IP 地址将从 VPX 实例可用的空闲 IP 地址自动填充。有关详细信息，请参阅使用 Azure 门户将多个 IP 地址分配给虚拟机。
   - 类型：从菜单中选择 AZURETAGS。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Azure 标签名称：输入您在 Azure 门户中分配给 VM 或 NIC 的名称。
- Azure 标签值：输入您在 Azure 门户中分配给 VM 或 NIC 的值。
- Azure 轮询周期：默认情况下，轮询周期为 60 秒，这是最小值。您可以根据需要进行更改。
- 负载均衡服务器协议：选择负载均衡器侦听的协议。
- 负载均衡服务器端口：选择负载均衡器侦听的端口。
- Azure 标签设置：将为此云配置文件创建的服务组的名称。
- Azure 标签设置协议：选择后端服务器侦听的协议。
- Azure 标签设置端口：选择后端服务器侦听的端口。

2. 点击 **创建**。

为带标签的 VM 或 NIC 创建负载均衡虚拟服务器和服务组。要查看负载均衡虚拟服务器，请从 VPX GUI 导航到 **流量管理 > 负载均衡 > 虚拟服务器**。

如何使用 VPX CLI 添加 Azure 标签设置

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
```

重要提示：

您必须保存所有配置；否则，重新启动实例后配置将丢失。键入 `save config`。

示例 1：以下是为所有带有“myTagName/myTagValue”标签的 Azure VM/NIC 的 HTTP 流量创建云配置文件的示例命令：

```
add cloud profile MyTagCloudProfile -type azuretags -vServerName
MyTagVServer -serviceType HTTP -IPAddress 40.115.116.57 -port 80
-serviceGroupName MyTagsServiceGroup -boundServiceGroupSvcType HTTP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-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 命令打印示例 1 中新添加的云配置文件的信息。

```
show cloudprofile

1)    Name:  MyTagCloudProfile Type:  azuretags         VServerName:
 MyTagVServer ServiceType:  HTTP       IPAddress:  52.178.209.133 Port:
 80                ServiceGroupName:  MyTagsServiceGroup
BoundServiceGroupSvcType:  HTTP

     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：以下命令删除示例 1 中创建的云配置文件。

```
> rm cloudprofile MyTagCloudProfile

  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云配置文件关联的服务组和服务器。当在要删除的云配置文件的轮询周期结束前几秒发出此命令时，会发生这种情况。

解决方案：通过为每个剩余的服务组输入以下 CLI 命令，手动删除剩余的服务组：

```
#> rm servicegroup <serviceGroupName>
```

此外，通过为每个剩余的服务器输入以下 CLI 命令，删除每个剩余的服务器：

```
#> rm server <name>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

问题：如果您使用 CLI 将 Azure 标签设置添加到 VPX 实例，则在热重启后，rain_tags 进程会继续在 HA 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 HA 节点的 CLI 退出到 shell 提示符：

```
#> shell
```

使用以下命令终止 rain_tags 进程：

```
# PID=`ps -aux | grep rain_tags | awk '{print $2}'`; kill -9 $PID
```

问题：后端服务器可能无法访问，并且尽管运行正常，但被 VPX 实例报告为 DOWN。 **解决方案**：确保 VPX 实例可以访问与后端服务器对应的标记 IP 地址。对于标记的 NIC，这是 NIC IP 地址；而对于标记的 VM，这是 VM 的主 IP 地址。如果 VM/NIC 位于不同的 Azure VNet 上，请确保已启用 VNet 对等互连。

在 NetScaler VPX 实例上配置 GSLB

配置了全局服务器负载均衡 (GSLB) 的 NetScaler 设备通过防止 WAN 中的故障点来提供灾难恢复和应用程序的持续可用性。GSLB 可以通过将客户端请求定向到最近或性能最佳的数据中心，或者在发生中断时定向到幸存的数据中心来平衡数据中心之间的负载。

本节介绍如何使用 Windows PowerShell 命令在 Microsoft Azure 环境中两个站点的 VPX 实例上启用 GSLB。

注意：

有关 GSLB 的更多信息，请参阅 全局服务器负载均衡。

您可以通过两个步骤在 Azure 上的 NetScaler VPX 实例上配置 GSLB：

1. 在每个站点上创建具有多个 NIC 和多个 IP 地址的 VPX 实例。
2. 在 VPX 实例上启用 GSLB。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

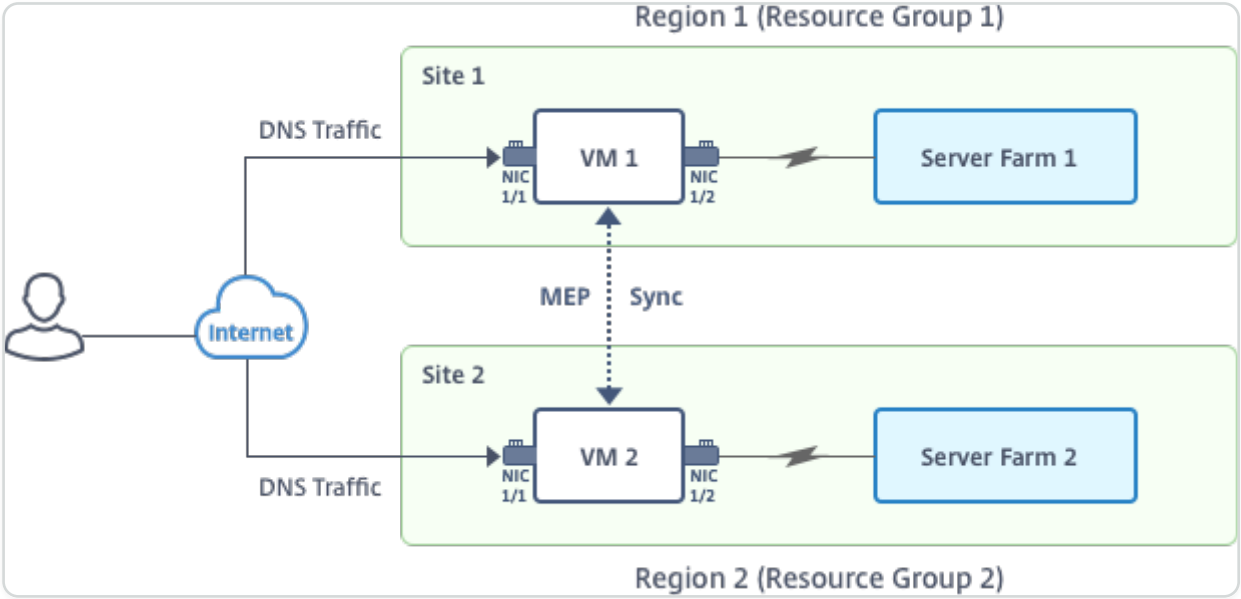
注意：

有关配置多个 NIC 和 IP 地址的更多信息，请参阅：使用 PowerShell 命令为独立模式下的 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。每个站点都有一台配置了多个 NIC、多个 IP 地址和 GSLB 的虚拟机 (VM1 和 VM2)。

图。 跨两个站点（站点 1 和站点 2）实现的 GSLB 设置。



在此场景中，每个虚拟机有三个 NIC - NIC 0/1、1/1 和 1/2。每个 NIC 可以有多个私有和公共 IP 地址。这些 NIC 配置用于以下目的。

- NIC 0/1：用于管理流量
- NIC 1/1：用于客户端流量
- NIC 1/2：用于与后端服务器通信

有关此场景中每个 NIC 上配置的 IP 地址的信息，请参阅 IP 配置详细信息 部分。

参数

以下是本文档中此场景的示例参数设置。

```
$location="West Central US"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$nicNamePrefix="MultiipVPX"

$osDiskSuffix="osdiskdb"

$numberOfVMs=1

$ipAddressPrefix="10.0.0."

$ipAddressPrefix1="10.0.1."

$ipAddressPrefix2="10.0.2."

$pubIPName1="MultiIP-pip1"

$pubIPName2="MultiIP-pip2"

$IpConfigName1="IPConfig1"

$IPConfigName2="IPConfig-2"

$IPConfigName3="IPConfig-3"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$IPConfigName4="IPConfig-4"

$frontendSubnetName="default"

$backendSubnetName1="subnet\_1"

$backendSubnetName2="subnet\_2"

$suffixNumber=10
```

创建 VM

按照步骤 1-10，使用 PowerShell 命令创建具有多个网卡和多个 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. 创建公共 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，重复这些步骤以使用特定于 VM2 的参数创建 VM2。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

创建资源组

```
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}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$backendSubnet2=$vnet.Subnets|?{$_.Name -eq $backendSubnetName2}
```

创建公共 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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“使用 PowerShell 命令创建多 NIC VM”中列出的步骤 1-10，以使用 VM2 特定的参数创建 VM2。

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	私有 IP	公共 IP (PIP)	描述
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。公共 IP 不是强制性的

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NIC	私有 IP	公共 IP (PIP)	描述
1/2	10.0.2.10	-	配置为 SNIP，用于向服务发送监视探测；公共 IP 不是强制性的

表 2. VM2 中使用的 IP 地址

网卡	内部 IP	公共 IP (PIP)	描述
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。公共 IP 不是强制性的
1/2	20.0.2.10	-	配置为 SNIP，用于向服务发送监视探测；公共 IP 不是强制性的

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。

以下是 VM1 上的示例配置。

```
add ns ip 10.0.1.10 255.255.255.0 -mgmtAccess ENABLED

Add nsip 10.0.2.10 255.255.255.0

add service svc1 10.0.1.10 ADNS 53

add lb vserver v1 HTTP 10.0.1.11 80

add service s1 10.0.2.120 http 80

Add service s2 10.0.2.121 http 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Bind lb vs v1 s[1-2]
```

以下是 VM2 上的示例配置。

```
add ns ip 20.0.1.10 255.255.255.0  -mgmtAccess ENABLED

Add nsip 20.0.2.10 255.255.255.0

add service svc1 20.0.1.10 ADNS 53

add lb vserver v1 HTTP 20.0.1.11 80

Add service s1 20.0.2.90 http 80

Add service s2 20.0.2.91 http 80

Bind lb vs v1 s[1-2]
```

配置 GSLB 站点和其他设置

执行以下主题中描述的任务，以配置两个 GSLB 站点和其他必要设置：

全局服务器负载平衡

以下是 VM1 和 VM2 上的 GSLB 示例配置。

```
enable ns feature LB GSLB

add gslb site site1 10.0.1.10 -publicIP PIP2

add gslb site site2 20.0.1.10 -publicIP PIP5

add gslb service site1_gslb_http_svc1 10.0.1.11 HTTP 80 -publicIP PIP3
-publicPort 80 -siteName site1

add gslb service site2_gslb_http_svc1 20.0.1.11 HTTP 80 -publicIP PIP6
-publicPort 80 -siteName site2

add gslb vserver gslb_http_vip1 HTTP

bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

您已在 Azure 上运行的 NetScaler VPX 实例上配置了 GSLB。

灾难恢复

灾难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。数据丢失或数据中心停机至关重要，会破坏业务连续性。

客户当今面临的挑战之一是决定将其灾难恢复 (DR) 站点设置在哪里。无论底层基础设施或网络是否存在故障，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包括：

- 拥有本地数据中心非常昂贵。通过使用云，企业可以腾出时间和资源，而无需扩展自己的系统。
- 许多自动化编排可实现更快的恢复
- 通过提供持续数据保护或持续快照来复制数据，以防范任何中断或攻击。
- 支持客户需要多种不同类型的合规性和安全控制的用例，这些控制已在公共云上提供。这使得他们更容易实现所需的合规性，而不是自行构建。

配置为 GSLB 的 NetScaler 会将流量转发到负载最低或性能最佳的数据中心。这种配置（称为主动-主动设置）不仅可以提高性能，而且在设置中的某个数据中心发生故障时，通过将流量路由到其他数据中心，还可以提供即时灾难恢复。NetScaler 因此为客户节省了宝贵的时间和金钱。

用于灾难恢复的多网卡多 IP（三网卡）部署

如果客户部署到生产环境，并且安全性、冗余、可用性、容量和可扩展性至关重要，他们可能会使用三网卡部署。使用此部署方法，复杂性和管理便捷性对用户而言并非关键问题。

用于灾难恢复的单网卡多 IP（一网卡）部署

如果客户出于以下原因部署到非生产环境，他们可能会使用一网卡部署：

- 设置测试环境，或者在生产部署之前搭建新环境。
- 快速高效地直接部署到云端。
- 同时寻求单个子网配置的简便性。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在主动-备用高可用性设置上配置 GSLB

您可以通过以下三个步骤在 Azure 上的主动-备用 HA 部署中配置全局服务器负载均衡 (GSLB)：

1. 在每个 GSLB 站点上创建 VPX HA 对。有关如何创建 HA 对的信息，请参阅 配置具有多个 IP 地址和 NIC 的高可用性设置。
2. 配置 Azure 负载均衡器 (ALB)，包括前端 IP 地址和规则，以允许 GSLB 和 DNS 流量。

   此步骤包括以下子步骤。有关完成这些子步骤所用的 PowerShell 命令，请参阅本节中的方案。

   a. 为 GSLB 站点创建前端 `IPconfig`。

   b. 创建后端地址池，其中包含 HA 中节点的 NIC 1/1 的 IP 地址。

   c. 为以下各项创建负载均衡规则：

   ```
   TCP/3009 – gslb communication

   TCP/3008 - gslb communication

   UDP/53 - DNS communication
   ```

   d. 将后端地址池与在步骤 c 中创建的 LB 规则关联。

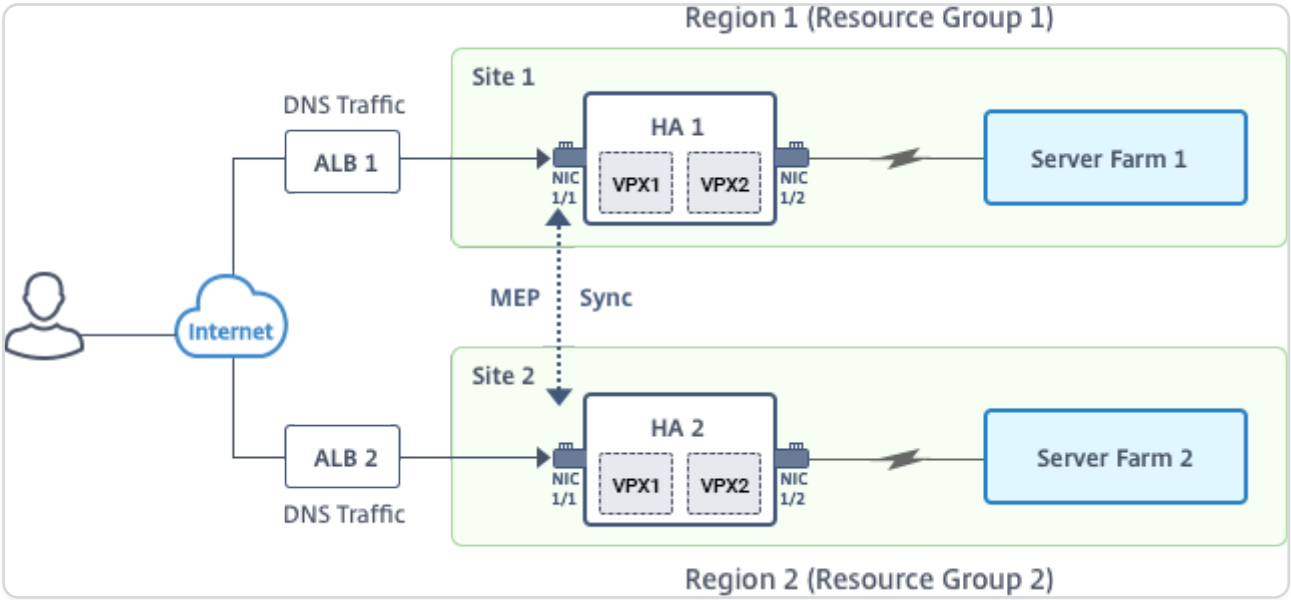
   e. 更新 HA 对中节点的 NIC 1/1 的网络安全组，以允许 TCP 3008、TCP 3009 和 UDP 53 端口的流量。
3. 在每个 HA 对上启用 GSLB。

方案

此方案包括两个站点 - 站点 1 和站点 2。每个站点都配置了一个 HA 对（HA1 和 HA2），具有多个 NIC、多个 IP 地址和 GSLB。

图： Azure 上的主动-备用 HA 部署中的 GSLB

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在此场景中，每个 VM 都有三个 NIC - NIC 0/1、1/1 和 1/2。这些 NIC 配置用于以下目的。

NIC 0/1：用于处理管理流量

NIC 1/1：用于处理客户端流量

NIC 1/2：用于与后端服务器通信

参数设置

以下是 ALB 的示例参数设置。如果需要，您可以使用不同的设置。

```
$locName="South east Asia"


$rgName="MulitIP-MultiNIC-RG"


$pubIPName4="PIPFORGSLB1"


$domName4="vpxgslbdns"


$lbName="MultiIPALB"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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 GSLB 和 DNS 流量

步骤 1. **创建 GSLB 站点 IP 的公共 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. **创建 LB 规则并更新现有 ALB。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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（ALB 1 和 ALB 2）都有两个前端 IP 地址。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（用于 LB 虚拟服务器）
- PIPFORGSLB1 (GSLB IP)

HA 2 具有以下前端 IP 地址：

- FrontEndIPofALB2 (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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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

随着需求的增长，运营本地数据中心为区域客户提供服务的企业希望利用 Azure 云在全球范围内进行扩展和部署。借助网络管理员端的 NetScaler，您可以使用 GSLB StyleBook 配置本地和云中的应用程序。您可以使用 NetScaler ADM 将相同的配置传输到云中。您可以根据与 GSLB 的距离访问本地或云资源。无论您身在何处，这都能让您获得无缝体验。

DBS 概述

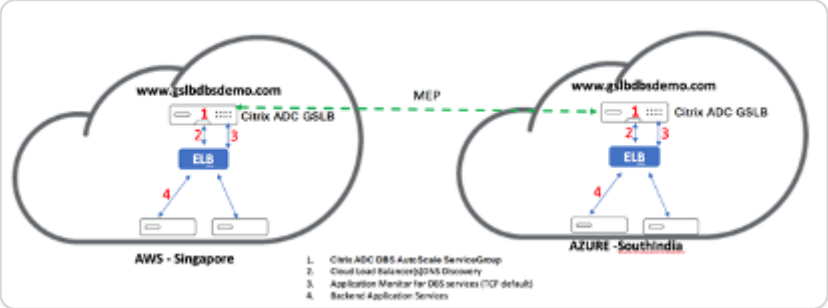
NetScaler GSLB 支持将基于域的服务 (DBS) 用于云负载均衡器。这允许使用云负载均衡器解决方案自动发现动态云服务。此配置允许 NetScaler 在 Active-Active 环境中实施 GSLB DBS。DBS 允许通过 DNS 发现来扩展 Microsoft Azure 环境中的后端资源。本节介绍 Azure 自动缩放环境中 NetScaler 之间的集成。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 Azure 负载均衡器 (ALB) 的基于域名的服务

GSLB DBS 使用用户 ALB 的 FQDN 动态更新 GSLB 服务组，以包含在 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。他们无需在 Azure 中每次创建和删除实例时手动更新 Citrix ADC 即可完成此操作。Citrix ADC 针对 GSLB 服务组的 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。

下图描绘了带有云负载均衡器的 NetScaler GSLB DBS 自动缩放组件：



Azure GSLB 先决条件

NetScaler GSLB 服务组的先决条件包括一个正常运行的 Microsoft Azure 环境，以及配置 Linux Web 服务器、Azure 中的 NetScaler 设备、公共 IP 地址和 Azure 负载均衡器 (ALB) 的知识和能力。

- GSLB DBS 服务集成需要 NetScaler 12.0.57 版本，用于 Microsoft Azure 负载均衡器实例。
- GSLB 服务组实体：NetScaler 12.0.57 版本。
- 引入了 GSLB 服务组，该服务组支持使用 DBS 动态发现进行自动缩放。
- DBS 功能组件（基于域的服务）必须绑定到 GSLB 服务组。

示例：

```
```

 > add server sydney_server LB-Sydney-
xxxxxxxxxx.australiaeast.cloudapp.azure.com

 > add gslb serviceGroup sydney_sg HTTP -autoscale DNS -siteName sydney

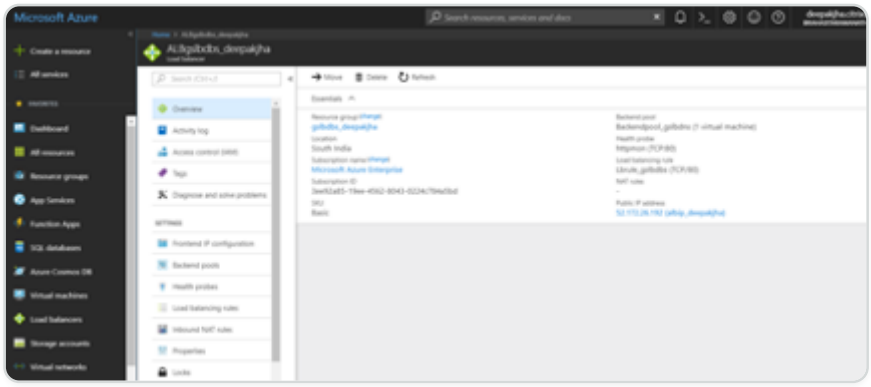
 > bind gslb serviceGroup sydney_sg sydney_server 80

```
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置 Azure 组件

1. 登录到用户 Azure 门户，并从 NetScaler 模板创建新的虚拟机。
2. 创建 Azure 负载均衡器。

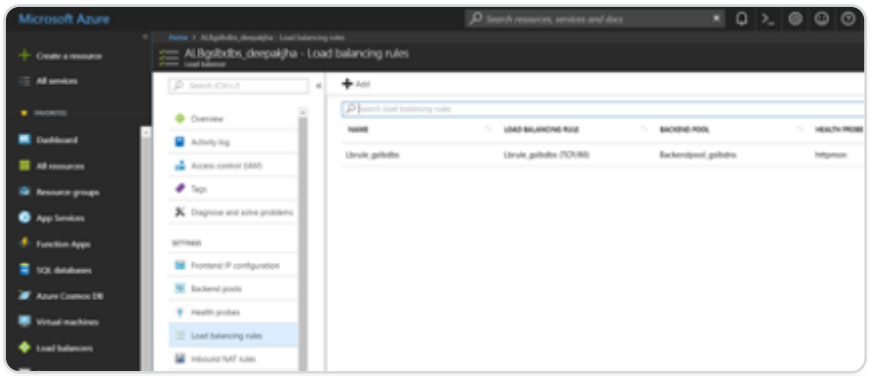


3. 添加已创建的 NetScaler 后端池。

4. 为端口 80 创建运行状况探测。

   使用从负载均衡器创建的前端 IP 创建负载均衡规则。

   - 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
   - 会话持久性：无



© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置 NetScaler GSLB 基于域的服务

以下配置总结了在启用 GSLB 的环境中为自动扩缩 ADC 启用基于域的服务所需的内容。

- 流量管理配置
- GSLB 配置

流量管理配置

注意：

需要使用名称服务器或 DNS 虚拟服务器配置 NetScaler，通过它们解析 DBS 服务组的 ALB 域。有关名称服务器或 DNS 虚拟服务器的更多信息，请参阅：DNS 名称服务器。

1. 导航到 **流量管理 > 负载平衡 > 服务器**。
2. 单击 **添加** 以创建服务器，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，从 Azure 中的第二个资源添加第二个 ALB。

GSLB 配置

1. 单击 **添加** 按钮以配置 GSLB 站点。
2. 指定配置 GSLB 站点的详细信息

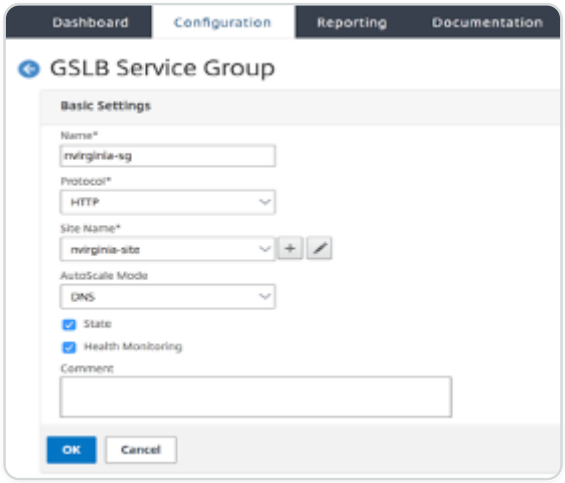
© 1997–2026 Citrix Systems, Inc. All rights reserved.

命名站点。类型根据您配置站点的 NetScaler 是远程还是本地进行配置。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。当使用云服务时，如果特定 IP 地址托管在外部防火墙或 NAT 设备上，则需要公共 IP 地址。将站点配置为父站点，并确保将 **触发监视器** 设置为 **始终**。此外，请务必选中底部的三个复选框，分别用于 **指标交换**、**网络指标交换** 和 **持久会话条目交换**。

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。

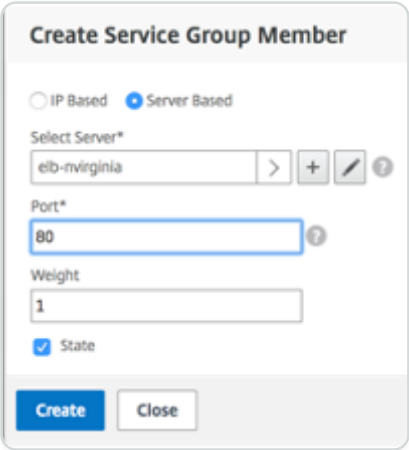
3. 单击 **创建**。
4. 导航到 **流量管理 > GSLB > 服务组**。
5. 单击 **添加** 以添加服务组。
6. 指定详细信息以配置服务组

为服务组命名，使用 HTTP 协议。在 **站点名称** 下，选择您创建的相应站点。确保将自动缩放模式配置为 DNS，并勾选“状态”和“运行状况监视”复选框。单击 **确定** 以创建服务组。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. 单击 **服务组成员** 并选择 **基于服务器**。选择在运行指南开头配置的相应 ALB。配置流量通过端口 80。单击 **创建**。

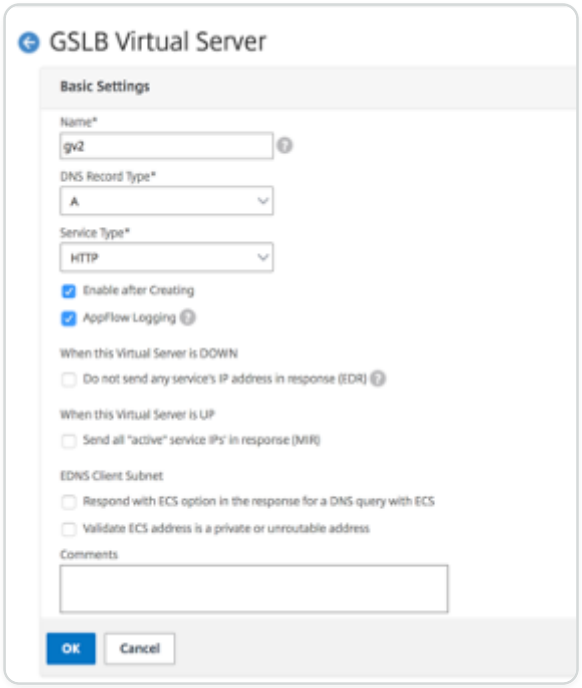


服务组成员绑定将填充从 ALB 接收的 2 个实例。

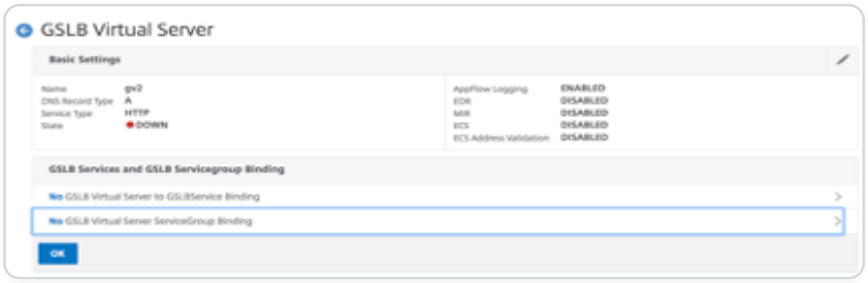
8. 重复步骤 5 和 6，为 Azure 中的第二个资源位置配置服务组。（这可以在同一个 NetScaler GUI 中完成）。
9. 设置 GSLB 虚拟服务器。导航到 **流量管理 > GSLB > 虚拟服务器**。
10. 单击 **添加** 以创建虚拟服务器。
11. 指定详细信息以配置 GSLB 虚拟服务器。

    为服务器命名，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**”以创建 GSLB 虚拟服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



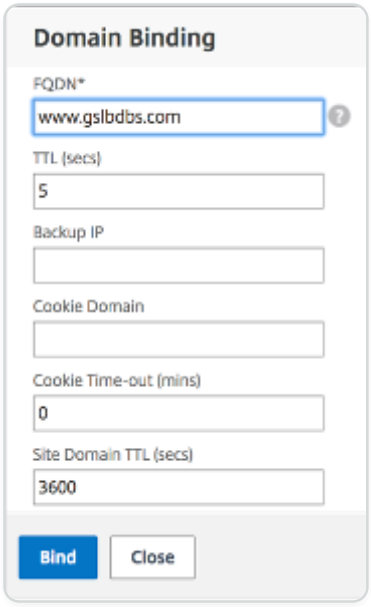
12. 创建 GSLB 虚拟服务器后，单击“**无 GSLB 虚拟服务器服务组绑定**”。



13. 在“**服务组绑定**”下，使用“**选择服务组名称**”选择并添加在前面步骤中创建的服务组。

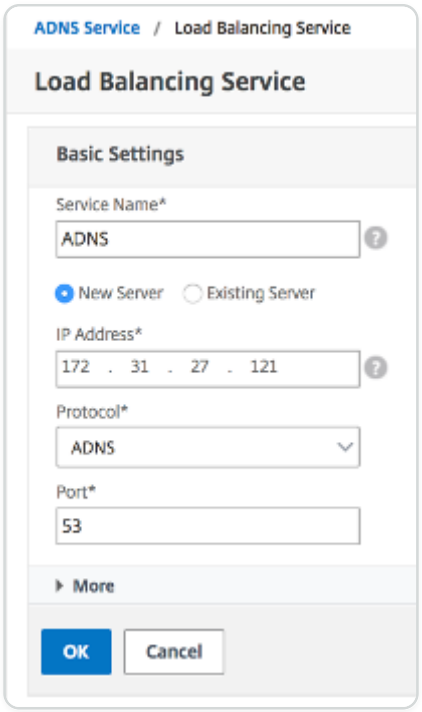
14. 通过单击“**无 GSLB 虚拟服务器域绑定**”配置 GSLB 虚拟服务器域绑定。配置 FQDN 并绑定。其他参数保留默认设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



15. 通过单击“**无服务**”配置 ADNS 服务。
16. 指定详细信息以配置负载平衡服务。

    添加“**服务名称**”，单击“**新建服务器**”，然后输入 ADNS 服务器的“**IP 地址**”。如果用户 ADNS 已配置，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 且流量配置为通过端口 53 流动。



17. 将“**方法**”配置为“**最少连接**”，并将备份方法配置为“**轮询**”。
18. 单击“**完成**”并验证用户 GSLB 虚拟服务器显示为“已启动”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

其他资源

适用于混合云和多云部署的 NetScaler 全局负载平衡

在 Azure Local 上部署 NetScaler VPX 实例

NetScaler VPX™ 支持在 Azure Local（Azure Stack 超融合基础架构 (HCI)）22H2、23H2 和 24H2 版本上部署。您可以在独立的 Azure Local 主机上部署 NetScaler VPX 实例，或在 Azure Local 实例（以前称为 Azure Stack HCI 群集）中将其设置为高可用性 (HA) 对。 Azure Local 是一个混合云平台，允许组织在其自己的数据中心运行 Azure 服务。在 Azure Local 上部署 NetScaler VPX 可在本地提供高级负载平衡、应用程序交付和安全功能，同时确保与 Azure 云服务的无缝集成。此解决方案对于需要低延迟、数据主权或法规遵从性的企业非常有利，因为 NetScaler 可以利用 Azure 生态系统的优势在本地优化和保护应用程序。

在 Azure Local 上部署 NetScaler VPX 实例的先决条件

- 确保您的环境满足以下 NetScaler VPX 版本和 Azure Local 版本要求。
  - **支持的 NetScaler VPX 版本：** 13.1-61.x 及更高版本
  - **支持的 Azure Local 操作系统版本：** 25398.1965、26100.7171 和 20349.3692

    有关 Azure Local 发布版本的更多信息，请参阅 Microsoft 文档。
- 确保您有权访问专用 Azure Local 节点，并且 Windows Admin Center 已安装并正确连接到此节点。
- 从 Citrix 官方网站或您的许可来源下载 NetScaler 虚拟硬盘 (VHD) 映像。确保映像与您的环境兼容。

如何使用 Windows Admin Center 中的 VHD 在 Azure Local 上部署 NetScaler VPX 实例

要使用 Windows Admin Center 中的 VHD 在 Azure Local 上部署 NetScaler VPX 实例，请按照以下步骤操作：

1. 使用 Windows Admin Center 将 NetScaler VHD 文件上传到您的 Azure Stack HCI 节点。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 在 Windows Admin Center 中创建新的虚拟机 (VM)，配置 VM 设置，例如名称、第 1 代、CPU、内存、虚拟交换机，并选择已上传的 VHD。
3. 启动新创建的 NetScaler VM 并监控其启动状态。
4. 使用 Hyper-V 管理器访问 NetScaler 实例控制台，登录并分配 IP 地址。
5. 使用 SSH 远程连接到 NetScaler VPX 实例以进行进一步的设置和管理。
6. 通过检查与 NetScaler 管理界面的连接并完成所需的配置来验证部署。

步骤 1. 使用 Windows Admin Center 将 NetScaler VHD 文件上传到您的 Azure Local 计算机。

1. 打开 Windows Admin Center 并连接到您的 Azure Local 计算机。
2. 导航到 **工具 > 文件和文件共享**。
3. 浏览到所需的卷并导航到您要上传 VHD 文件的特定文件夹。
4. 单击 **上传** 并从您的计算机中选择 VHD 文件。
5. 等待上传过程完成。完成后，验证 VHD 文件是否出现在所选文件夹中。

步骤 2. 创建新的虚拟机并配置 VM 设置。

1. 在 Windows Admin Center 中，转到 **虚拟机**。
2. 单击 **添加**，然后选择 **新建**。
3. 输入 VM 的名称并选择 **第 1 代**。
4. 配置虚拟处理器 (CPU)、内存和虚拟交换机，以满足 NetScaler 要求和您的部署需求。
5. 在 **存储** 设置中，选择 **使用现有虚拟硬盘** 并选择已上传的 VHD 映像。
6. 完成创建虚拟机。

创建虚拟机(/en-us/vpx/media/azure-local-create-new-vm.png)

步骤 3. 启动 NetScaler 虚拟机。

1. 配置完成后，启动您在上一步中创建的 NetScaler 虚拟机。

   启动虚拟机(/en-us/vpx/media/azure-local-start-vm.png)
2. 在 Windows Admin Center 中监控虚拟机状态，确保其成功启动。

   监控虚拟机(/en-us/vpx/media/azure-local-monitor-vm.png)

步骤 4. 使用 Hyper-V 管理器配置网络并设置远程访问。

1. NetScaler 实例启动后，在 Hyper-V 管理器中打开控制台。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置网络(/en-us/vpx/media/azure-local-configure-network.png)

2. 从 Azure Local 节点上的 Hyper-V 控制台登录到 NetScaler。

   Hyper-V 控制台(/en-us/vpx/media/azure-local-assign-ip-address.png)

3. 分配并保存 IP 地址。
4. 使用 SSH 远程连接到 NetScaler 以进行其他设置和管理。

   Azure 本地验证(/en-us/vpx/media/azure-local-validate.png)

步骤 5. 验证 NetScaler VPX 部署。

1. 使用配置的 IP 地址登录 NetScaler GUI 或 CLI，然后继续进行 NetScaler VPX 配置。
2. 验证 NetScaler 配置是否完成，并且 VPX 实例是否按预期运行。

在 Azure 上部署 NetScaler® Web App Firewall

NetScaler Web App Firewall 是一种企业级解决方案，为现代应用程序提供最先进的保护。它可缓解针对面向公众资产（包括网站、Web 应用程序和 API）的威胁。该防火墙包括基于 IP 信誉的过滤、机器人缓解、OWASP 十大应用程序威胁保护、第 7 层 DDoS 保护等功能。此外，还包括强制执行身份验证、强大的 SSL/TLS 密码、TLS 1.3、速率限制和重写策略的选项。结合使用基本和高级 WAF 保护，它为您的应用程序提供全面保护，且易用性无与伦比。几分钟即可启动并运行。此外，通过使用称为动态分析的自动化学习模型，该防火墙为用户节省了宝贵时间。通过自动学习受保护应用程序的工作方式，它甚至在开发人员部署和更改应用程序时也能适应这些应用程序。它有助于符合所有主要法规标准和机构，包括 PCI-DSS、HIPAA 等。借助我们的 CloudFormation 模板，快速启动并运行从未如此简单。通过自动扩展，用户可以放心，即使流量增加，其应用程序也能保持受保护状态。

NetScaler Web App Firewall 可以作为第 3 层网络设备或第 2 层网络桥接安装在客户服务器和客户用户之间，通常位于客户公司的路由器或防火墙之后。有关详细信息，请参阅 NetScaler Web App Firewall 简介。

NetScaler Web App Firewall 部署策略

1. 部署 Web 应用程序防火墙是为了评估哪些应用程序或特定数据需要最大程度的安全保护，哪些应用程序的漏洞较少，以及哪些应用程序可以安全地绕过安全检查。这有助于用户制定最佳配置，并设计适当的策略和绑定点来隔离流量。例如，用户可能希望配置策略以绕过对静态 Web 内容（如图像、MP3 文件和电影）请求的安全检查，并配置另一个策略以对动态内容请求应用高级安全检查。用户可以使用多个策略和配置文件来保护同一应用程序的不同内容。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 为了确定部署基线，请创建一个虚拟服务器并通过它运行测试流量，以了解流经用户系统的流量速率和数量。
3. 部署 Web 应用程序防火墙。使用 NetScaler ADM 和 Web 应用程序防火墙 StyleBook 配置 Web 应用程序防火墙。有关详细信息，请参阅本指南下面的 StyleBook 部分。
4. 实施 NetScaler Web App Firewall 和 OWASP 十大。

Web 应用程序防火墙的三种保护措施对常见的 Web 攻击类型特别有效，因此比其他任何保护措施都更常用。因此，应在初始部署中实施它们。它们是：

- **HTML 跨站点脚本**：检查请求和响应中的脚本，这些脚本试图访问或修改与脚本所在网站不同的网站上的内容。当此检查发现此类脚本时，它会在将请求或响应转发到其目的地之前使脚本无害，或者它会阻止连接。
- **HTML SQL 注入**：检查包含表单字段数据的请求，以查找将 SQL 命令注入 SQL 数据库的尝试。当此检查检测到注入的 SQL 代码时，它会阻止请求，或者在将请求转发到 Web 服务器之前使注入的 SQL 代码无害。

注意：

确保您的 Web 应用程序防火墙已正确配置，以便以下条件适用于您的配置：

```
>-  If users enable the HTML Cross-Site Scripting check or the HTML SQL
Injection check (or both).

>

>-  User protected websites accept file uploads or contain Web forms
that can contain large POST body data.
```

有关配置 Web 应用程序防火墙以处理此情况的更多信息，请参阅配置应用程序防火墙：配置 Web 应用程序防火墙。

- **缓冲区溢出**：检查请求以检测在 Web 服务器上导致缓冲区溢出的尝试。

配置 Web 应用程序防火墙

确保 NetScaler Web App Firewall 已启用并正常运行。我们建议您使用 Web 应用程序防火墙 StyleBook 配置 NetScaler Web App Firewall。大多数用户认为这是配置 Web 应用程序防火墙最简单的方法，并且它旨在防止错误。GUI 和命令行界面都适用于经验丰富的用户，主要用于修改现有配置或使用高级选项。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SQL 注入

NetScaler Web App Firewall HTML SQL 注入检查提供了特殊的防御措施，以防止可能破坏用户应用程序安全的未经授权的 SQL 代码注入。NetScaler Web App Firewall 在三个位置检查请求负载中的注入 SQL 代码：1) POST 正文，2) 标头，和 3) Cookie。有关更多信息，请参阅 HTML SQL 注入检查。

跨站点脚本

HTML 跨站点脚本 (cross-site scripting) 检查会检查用户请求的标头和 POST 正文，以查找可能的跨站点脚本攻击。如果发现跨站点脚本，它会修改（转换）请求以使攻击无害，或者阻止请求。有关更多信息，请参阅 HTML 跨站点脚本检查。

缓冲区溢出检查

缓冲区溢出检查可检测尝试在 Web 服务器上导致缓冲区溢出的行为。如果 Web 应用程序防火墙检测到 URL、Cookie 或标头长度超过配置的长度，它会阻止该请求，因为它可能导致缓冲区溢出。有关更多信息，请参阅 缓冲区溢出检查。

虚拟补丁/签名

签名提供了特定且可配置的规则，以简化保护用户网站免受已知攻击的任务。签名表示一种模式，它是对操作系统、Web 服务器、网站、基于 XML 的 Web 服务或其他资源的已知攻击的组成部分。一套丰富的预配置内置或原生规则提供了一种易于使用的安全解决方案，利用模式匹配的强大功能来检测攻击并防范应用程序漏洞。有关更多信息，请参阅 签名。

NetScaler Web App Firewall 支持签名的 **自动和手动** 更新。 我们还建议为签名启用 **自动更新** 以保持最新。

这些签名文件托管在 AWS 环境中，因此允许网络防火墙出站访问 NetScaler IP 地址以获取最新的签名文件非常重要。在处理实时流量时，更新签名对 NetScaler 没有影响。

应用程序安全分析

应用程序安全仪表板 提供了用户应用程序安全状态的整体视图。例如，它显示了关键安全指标，如安全违规、签名违规和威胁指数。应用程序安全仪表板还显示了发现的 NetScaler 的攻击相关信息，如 SYN 攻击、小窗口攻击和 DNS 洪水攻击。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

要查看应用程序安全仪表板的指标，应在用户希望监控的 NetScaler 实例上启用 AppFlow 安全洞察。

要在应用程序安全仪表板上查看 NetScaler 实例的安全指标：

1. 使用管理员凭据登录到 NetScaler ADM。
2. 导航到**应用程序 > 应用程序安全仪表板**，然后从设备列表中选择实例 IP 地址。

用户可以通过单击图表上绘制的气泡，进一步深入了解应用程序安全调查器中报告的差异。

ADM 上的集中式学习

NetScaler Web App Firewall 可保护用户 Web 应用程序免受 SQL 注入和跨站点脚本 (XSS) 等恶意攻击。为了防止数据泄露并提供正确的安全保护，用户必须监控其流量以发现威胁和有关攻击的实时可操作数据。有时，报告的攻击可能是误报，需要将其作为例外情况提供。

NetScaler ADM 上的集中式学习是一种重复模式过滤器，它使 WAF 能够学习用户 Web 应用程序的行为（正常活动）。根据监控，引擎会为应用于 HTTP 流量的每个安全检查生成建议规则或例外列表。

使用学习引擎部署放宽规则比手动部署必要的放宽规则要容易得多。

要部署学习功能，用户必须首先在用户 NetScaler 上配置 Web 应用程序防火墙配置文件（一组安全设置）。有关详细信息，请参阅创建 Web App Firewall 配置文件。

NetScaler ADM 会为每个安全检查生成例外（放宽）列表。作为管理员，您可以在 NetScaler ADM 中查看例外列表，并决定部署或跳过。

使用 NetScaler ADM 中的 WAF 学习功能，您可以：

- 配置包含以下安全检查的学习配置文件。
  - 缓冲区溢出
  - HTML 跨站点脚本

    注意：

    位置的跨站点脚本限制仅为 FormField。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- HTML SQL 注入

> **注意：**
>
> 对于 HTML SQL 注入检查，用户必须在 NetScaler 中配置 `set -sqlinjectionTransformSpecialChars ON` 和 `set -sqlinjectiontype sqlspclcharorkeywords`。

- 检查 NetScaler ADM 中的放宽规则，并决定采取必要的操作（部署或跳过）。
- 通过电子邮件、Slack 和 ServiceNow 获取通知。
- 使用控制面板查看放宽详细信息。

要在 NetScaler ADM 中使用 WAF 学习功能：

1. 配置学习配置文件：配置学习配置文件
2. 查看放宽规则：查看放宽规则和空闲规则
3. 使用 WAF 学习控制面板：查看 WAF 学习控制面板

StyleBooks

StyleBooks 简化了管理用户应用程序复杂 NetScaler 配置的任务。StyleBook 是用户可用于创建和管理 NetScaler 配置的模板。在此处，用户主要关注用于部署 Web 应用程序防火墙的 StyleBook。有关 StyleBooks 的更多信息，请参阅 StyleBooks。

安全洞察分析

暴露在互联网上的Web和Web服务应用程序越来越容易受到攻击。为了保护应用程序免受攻击，用户需要了解过去、现在和即将发生的威胁的性质和程度，获取关于攻击的实时可操作数据，以及关于对策的建议。Security Insight 提供了一个单一面板解决方案，帮助用户评估用户应用程序的安全状态并采取纠正措施来保护用户应用程序。 有关详细信息，请参阅 Security Insight。

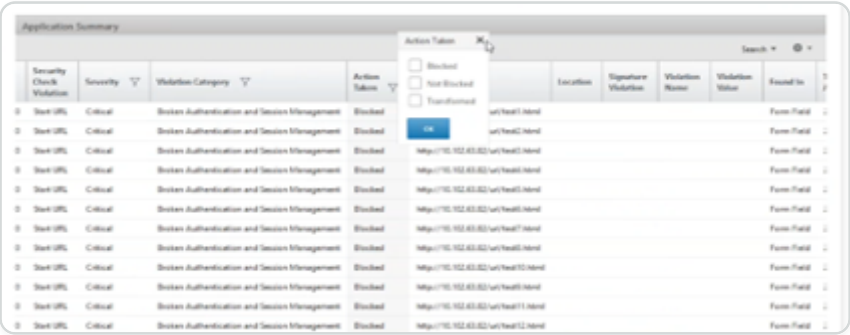
获取有关安全漏洞的详细信息

用户可能希望查看针对应用程序的攻击列表，并深入了解攻击的类型和严重性、ADC 实例采取的操作、请求的资源以及攻击源。

例如，用户可能希望确定有多少针对 Microsoft Lync 的攻击被阻止，请求了哪些资源，以及攻击源的 IP 地址。

在 **Security Insight 仪表板**上，单击 **Lync** > **总违规**。在表中，单击 **已采取的操作** 列标题中的筛选器图标，然后选择 **已阻止**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关请求的资源的信息，请查看 **URL** 列。有关攻击源的信息，请查看 **客户端 IP** 列。

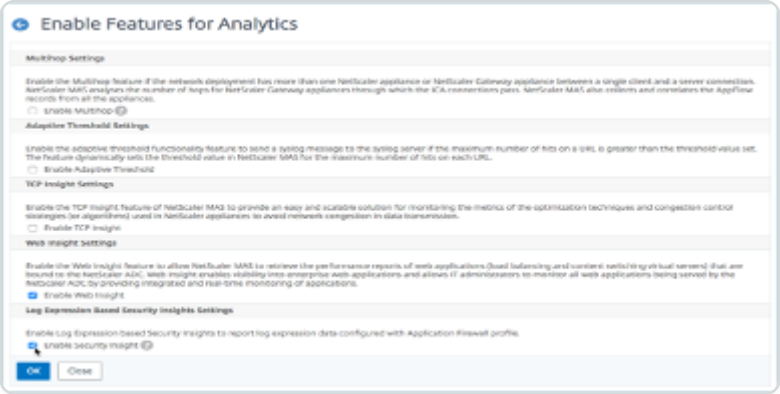
查看日志表达式详细信息

NetScaler 使用通过应用程序防火墙配置文件配置的日志表达式，对用户企业中应用程序上的攻击采取行动。在 **Security Insight** 中，用户可以查看 ADC 实例使用的日志表达式返回的值。这些值包括请求头、请求正文等。除了日志表达式值之外，用户还可以查看 ADC 实例用于对攻击采取行动的应用程序防火墙配置文件中定义的日志表达式名称和注释。

先决条件：

确保用户：

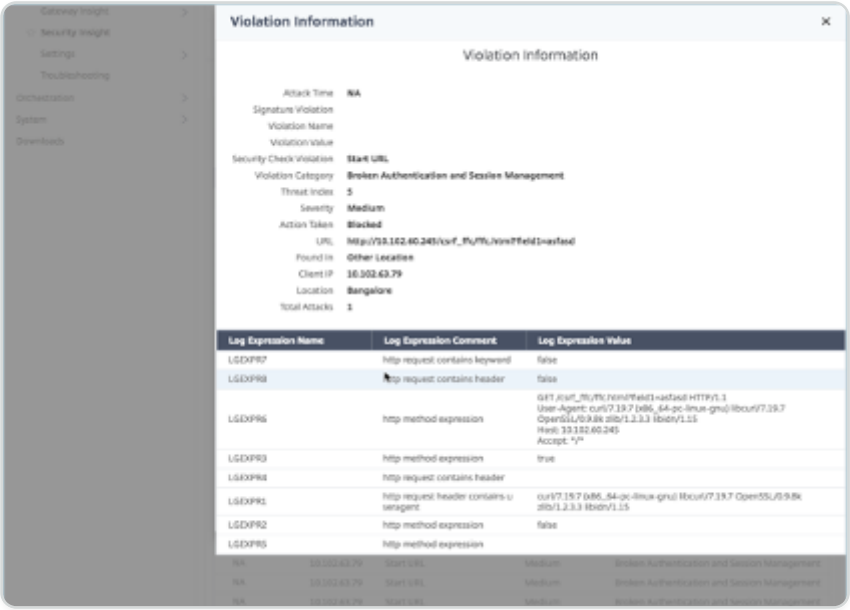
- 在应用程序防火墙配置文件中配置日志表达式。有关详细信息，请参阅应用程序防火墙。
- 在 NetScaler ADM 中启用基于日志表达式的 Security Insights 设置。执行以下操作：
  - 导航到 **分析** > **设置**，然后单击 **启用分析功能**。
  - 在“启用分析功能”页面中，在“**基于日志表达式的安全洞察设置**”部分下选择“**启用安全洞察**”，然后单击“**确定**”。



例如，您可能希望查看 ADC 实例针对用户企业中 Microsoft Lync 攻击所采取的操作返回的日志表达式值。

在“**安全洞察仪表板**”上，导航到“**Lync**”>“**总违规**”。在“应用程序摘要”表中，单击 URL 以在“**违规信息**”页面中查看违规的完整详细信息，包括日志表达式名称、注释以及 ADC 实例针对该操作返回的值。

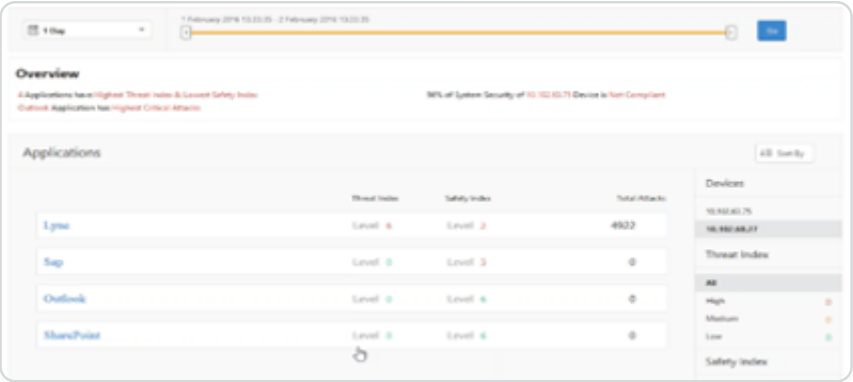
© 1997–2026 Citrix Systems, Inc. All rights reserved.



在部署配置之前确定安全指数。安全漏洞通常在用户将安全配置部署到 ADC 实例后发生，但用户可能希望在部署之前评估安全配置的有效性。

例如，用户可能希望评估 IP 地址为 10.102.60.27 的 ADC 实例上 SAP 应用程序配置的安全指数。

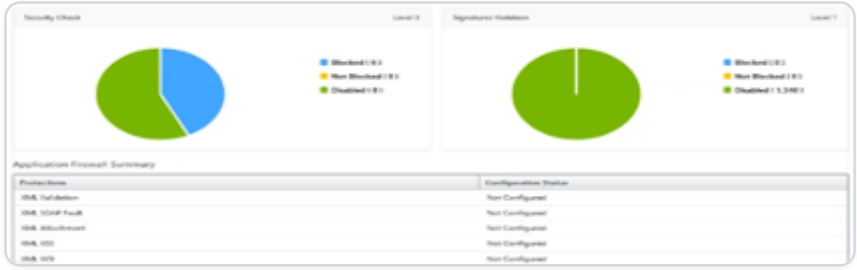
在“**安全洞察仪表板**”的“**设备**”下，单击用户配置的 ADC 实例的 IP 地址。用户可以看到威胁指数和攻击总数均为 0。威胁指数直接反映了应用程序上攻击的数量和类型。零攻击表示应用程序未受到任何威胁。



单击“**Sap**”>“**安全指数**”>“**SAP_Profile**”，并评估显示的安全指数信息。

在应用程序防火墙摘要中，用户可以查看不同保护设置的配置状态。如果某个设置配置为日志记录或未配置，则应用程序将被分配较低的安全指数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



安全违规

暴露在互联网上的 Web 应用程序已变得极易受到攻击。NetScaler ADM 使您能够可视化可操作的违规详细信息，以保护应用程序免受攻击。

查看应用程序安全违规详情

暴露在互联网上的 Web 应用程序已显著更容易受到攻击。NetScaler ADM 允许用户可视化可操作的违规详情，以保护应用程序免受攻击。导航到“**安全**”>“**安全违规**”，以获取一个单一窗格解决方案，用于：

- 根据类别（例如 **Network**、**Bot** 和 **WAF**）访问应用程序安全违规
- 采取纠正措施以保护应用程序

要在 NetScaler ADM 中查看安全违规，请确保：

- 用户拥有 NetScaler 的高级许可证（用于 WAF 和 BOT 违规）。
- 用户已在负载平衡或内容切换虚拟服务器上申请了许可证（用于 WAF 和 BOT）。有关详细信息，请参阅管理虚拟服务器上的许可。
- 用户可以启用更多设置。有关详细信息，请参阅 NetScaler 产品文档中“设置”部分提供的过程：设置。

违规类别

NetScaler ADM 允许用户查看所有违规中可用的违规：

设置

对于违规，请确保已启用“**指标收集器**”。默认情况下，NetScaler 上已启用“**指标收集器**”。有关详细信息，请参阅配置智能应用程序分析。

启用高级安全分析

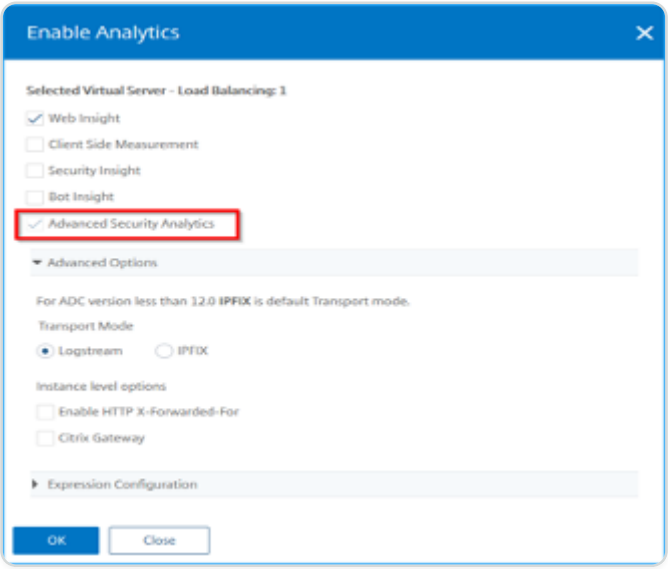
- 导航到“**网络**”>“**实例**”>“**NetScaler**”，然后选择实例类型。例如，MPX。
- 选择 NetScaler 实例，然后从“**选择操作**”列表中选择“**配置分析**”。
- 选择虚拟服务器，然后单击 **启用分析**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在 **启用分析** 窗口中：
  - 选择 **Web Insight**。用户选择 Web Insight 后，只读的 **高级安全分析** 选项将自动启用。

> **注意：**
>
> **高级安全分析** 选项仅适用于高级许可的 ADC 实例。

  - 选择 **Logstream** 作为传输模式
  - 表达式默认为 true
  - 单击 **确定**



启用 Web 事务设置

- 导航到 **分析** > **设置**。

将显示 **设置** 页面。

- 单击 **启用分析功能**。
- 在 **Web 事务设置** 下，选择 **全部**。

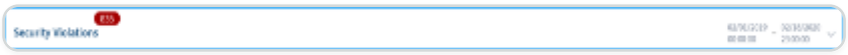
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 点击 **确定**。

安全违规仪表板

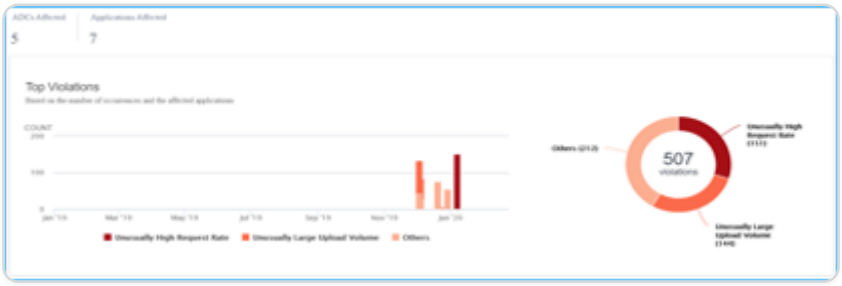
在安全违规仪表板中，用户可以查看：

- 所有 NetScaler 和应用程序中发生的违规总数。总违规数根据所选时间段显示。



- 每个类别下的违规总数。

- 受影响的 ADC 总数、受影响的应用程序总数以及根据总发生次数和受影响应用程序得出的主要违规。



有关违规详情的更多信息，请参阅 所有违规。

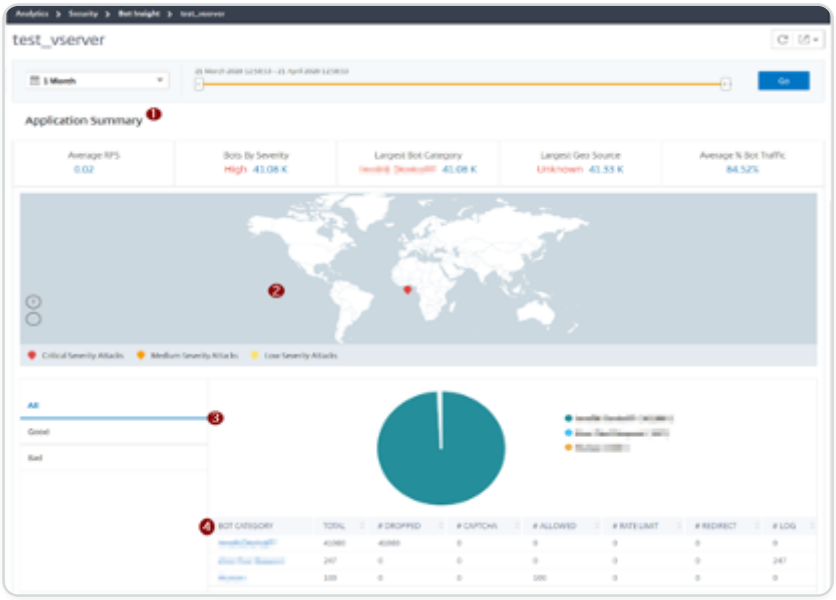
Bot 洞察

在 NetScaler 中配置 BOT 洞察。有关更多信息，请参阅 Bot。

查看 Bot

单击虚拟服务器以查看 **应用程序摘要**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. 提供应用程序摘要详细信息，例如：

   - **平均 RPS** – 表示虚拟服务器上每秒接收的平均僵尸程序事务请求 (RPS)。
   - **按严重性分类的僵尸程序** – 表示根据严重性发生最高僵尸程序事务。严重性分为**关键**、**高**、**中**和**低**。

   例如，如果虚拟服务器有 11770 个高严重性僵尸程序和 1550 个关键严重性僵尸程序，则 NetScaler ADM 会在**按严重性分类的僵尸程序**下显示**关键 1.55 K**。

   - **最大僵尸程序类别** – 表示根据僵尸程序类别发生最高僵尸程序攻击。

   例如，如果虚拟服务器有 8000 个阻止列表僵尸程序、5000 个允许列表僵尸程序和 10000 个超出速率限制的僵尸程序，则 NetScaler ADM 会在**最大僵尸程序类别**下显示**超出速率限制 10 K**。

   - **最大地理源** – 表示根据区域发生最高僵尸程序攻击。

   例如，如果虚拟服务器在圣克拉拉有 5000 次僵尸程序攻击，在伦敦有 7000 次僵尸程序攻击，在班加罗尔有 9000 次僵尸程序攻击，则 NetScaler ADM 会在**最大地理源**下显示**班加罗尔 9 K**。

   - **平均僵尸程序流量百分比** – 表示人机比。

2. 在地图视图中显示基于位置的僵尸程序攻击严重性
3. 显示僵尸程序攻击的类型（良好、恶意和所有）
4. 显示总僵尸程序攻击以及相应的配置操作。例如，如果您已配置：

   - IP 地址范围 (192.140.14.9 到 192.140.14.254) 作为阻止列表僵尸程序，并选择“丢弃”作为这些 IP 地址范围的操作
   - IP 范围 (192.140.15.4 到 192.140.15.254) 作为阻止列表僵尸程序，并选择创建日志消息作为这些 IP 范围的操作

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在此场景中，NetScaler ADM 显示：

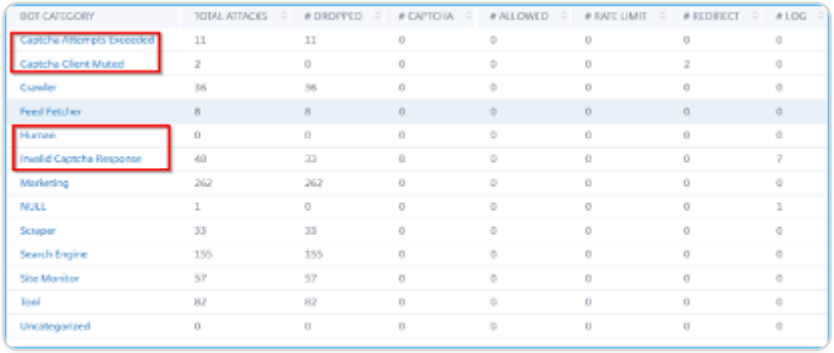
- 已列入阻止列表的机器人总数
- 处于 **已丢弃** 状态的机器人总数
- 处于日志状态的机器人总数

查看 CAPTCHA 机器人

在网页中，CAPTCHA 旨在识别传入流量是来自人类还是自动化机器人。要在 NetScaler ADM 中查看 CAPTCHA 活动，用户必须在 NetScaler ADM 实例中将 CAPTCHA 配置为 IP 信誉和设备指纹检测技术的机器人操作。有关详细信息，请参阅：配置机器人管理。

以下是 NetScaler ADM 在 Bot insight 中显示的 CAPTCHA 活动：

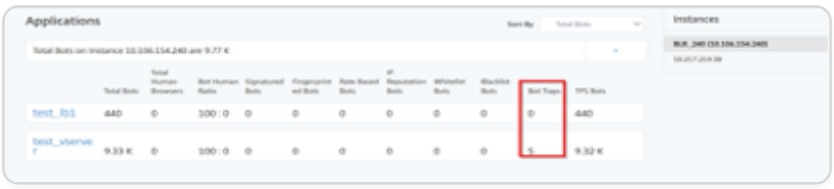
- **CAPTCHA 尝试次数超出限制** – 表示登录失败后进行的 CAPTCHA 尝试的最大次数
- **CAPTCHA 客户端已静音** – 表示因这些请求之前在 CAPTCHA 质询中被检测为恶意机器人而被丢弃或重定向的客户端请求数量
- **人类** – 表示人类用户执行的 CAPTCHA 条目
- **无效的 CAPTCHA 响应** – 表示当 NetScaler 发送 CAPTCHA 质询时，从机器人或人类接收到的不正确 CAPTCHA 响应的数量



BOT CATEGORY	TOTAL ATTACKS	# DROPPED	# CAPTCHA	# ALLOWED	# RATE LIMIT	# REDIRECT	# LOG
Captcha Attempts Exceeded	11	11	0	0	0	0	0
Captcha Client Muted	2	0	0	0	0	2	0
Crawler	36	36	0	0	0	0	0
Feed Fetcher	8	8	0	0	0	0	0
Human	0	0	0	0	0	0	0
Invalid Captcha Response	40	33	0	0	0	0	7
Marketing	262	262	0	0	0	0	0
NULL	1	0	0	0	0	0	1
Scraper	33	33	0	0	0	0	0
Search Engine	155	155	0	0	0	0	0
Site Monitor	57	57	0	0	0	0	0
Tool	82	82	0	0	0	0	0
Uncategorized	0	0	0	0	0	0	0

查看机器人陷阱

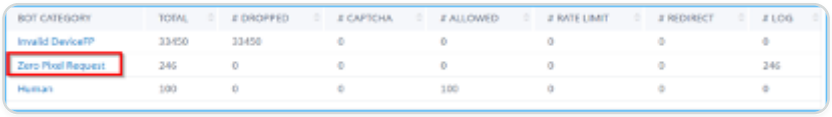
要在 NetScaler ADM 中查看机器人陷阱，您必须在 NetScaler 中配置机器人陷阱。有关详细信息，请参阅：配置机器人管理。



为了识别机器人陷阱，网页中会启用一个脚本，该脚本对人类隐藏，但对机器人不隐藏。当机器人访问此脚本时，NetScaler ADM 会识别并报告机器人陷阱。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

点击虚拟服务器并选择 **Zero Pixel Request**

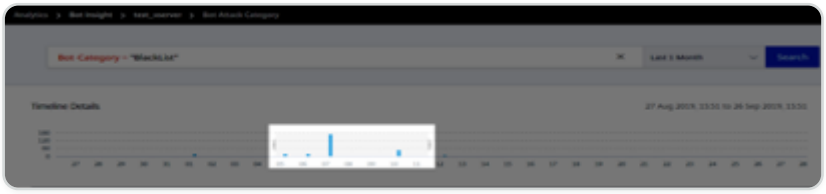


查看机器人详细信息

有关更多详细信息，请点击 **Bot Category** 下的机器人攻击类型。

将显示所选验证码类别的攻击时间以及机器人攻击总数等详细信息。

用户还可以拖动条形图以选择要显示机器人攻击的特定时间范围。



要获取机器人攻击的更多信息，请点击展开。

- **实例 IP** – 指示 NetScaler 实例 IP 地址。
- **机器人总数** – 指示在该特定时间发生的机器人攻击总数。
- **HTTP 请求 URL** – 指示为验证码报告配置的 URL。
- **国家/地区代码** – 指示发生机器人攻击的国家/地区。
- **区域** – 指示发生机器人攻击的区域。
- **配置文件名称** – 指示用户在配置期间提供的配置文件名称。

高级搜索

用户还可以使用搜索文本框和时间范围列表，根据用户要求查看机器人详细信息。当用户单击搜索框时，搜索框会提供以下搜索建议列表。

- **实例 IP** – NetScaler 实例 IP 地址。
- **客户端 IP** – 客户端 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **机器人类型** – 机器人类型，例如好或坏。
- **严重性** – 机器人攻击的严重性。
- **已采取的操作** – 机器人攻击后采取的操作，例如丢弃、不采取任何操作、重定向。
- **机器人类别** – 机器人攻击的类别，例如阻止列表、允许列表、指纹。用户可以根据类别为其关联机器人操作。
- **机器人检测** – 用户在 NetScaler 上配置的机器人检测类型（阻止列表、允许列表等）。
- **位置** – 发生机器人攻击的区域/国家/地区
- **请求 URL** – 可能存在机器人攻击的 URL

用户还可以在用户搜索查询中使用运算符来缩小用户搜索的范围。例如，如果用户想要查看所有恶意机器人：

- 单击搜索框并选择 **机器人类型**
- 再次单击搜索框并选择运算符 **=**
- 单击搜索框，然后选择**不良**
- 单击**搜索**以显示结果

异常高的请求速率

用户可以控制应用程序的入站和出站流量。僵尸程序攻击可能会导致异常高的请求速率。例如，如果用户将应用程序配置为允许每分钟 100 个请求，但观察到 350 个请求，则这可能是一次僵尸程序攻击。

使用**异常高的请求速率**指示器，用户可以分析应用程序收到的异常请求速率。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在**事件详细信息**下，用户可以查看：

- 受影响的应用程序。如果两个或更多应用程序受到违规影响，用户还可以从列表中选择应用程序。
- 指示所有违规的图表
- 违规发生时间
- 违规的检测消息，指示收到的总请求数以及超出预期请求的过多请求的百分比
- 应用程序接受的预期请求速率范围

僵尸程序检测

NetScaler 僵尸程序管理系统使用各种技术来检测入站僵尸程序流量。这些技术用作检测规则，以检测僵尸程序类型。

使用 NetScaler GUI 配置 Bot 管理

用户可以通过首先在设备上启用该功能来配置 NetScaler Bot 管理。有关更多信息，请参阅 Bot 检测。

IP 信誉

IP 信誉是一种识别发送不需要请求的 IP 地址的工具。使用 IP 信誉列表，您可以拒绝来自信誉不佳的 IP 地址的请求。

使用 NetScaler GUI 配置 IP 信誉

此配置是 Bot IP 信誉功能的先决条件。有关更多信息，请参阅 IP 信誉。

Bot 签名自动更新

Bot 静态签名技术使用包含良好 Bot 和不良 Bot 列表的签名查找表。有关更多信息，请参阅 签名自动更新。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Web App Firewall 和 OWASP 十大安全风险 – 2021

开放式 Web 应用程序安全项目 (OWASP) 发布了 2021 年 OWASP 十大 Web 应用程序安全风险。此列表记录了最常见的 Web 应用程序漏洞，是评估 Web 安全性的一个很好的起点。本节解释了如何配置 NetScaler Web App Firewall 以缓解这些缺陷。WAF 作为集成模块在 NetScaler（高级版）和全系列设备中提供。

完整的 OWASP 十大安全风险文档可在 OWASP Top Ten 处获取。

OWASP 十大安全风险 2021	NETSCALER WEB 应用防火墙 功能
A1:2021 访问控制失效	AAA、NetScaler AAA 模块中的授权安全功能、表单保护、Cookie 篡改保护、StartURL 和 ClosureURL
A2:2021 - 加密故障	信用卡保护、安全商务、Cookie 代理和 Cookie 加密
A3:2021- 注入	注入攻击防护（SQL 或任何其他自定义注入，例如 OS 命令注入、XPath 注入和 LDAP 注入）、自动更新签名功能
A5:2021 安全配置错误	此保护包括 WSI 检查、XML 消息验证和 XML SOAP 故障过滤检查
A6:2021 - 漏洞和过时组件	漏洞扫描报告、应用程序防火墙模板和自定义签名
A7:2021 - 身份识别和身份验证失败	AAA、Cookie 篡改保护、Cookie 代理、Cookie 加密、CSRF 标记、使用 SSL
A8:2021 – 软件和数据完整性故障	XML 安全检查、GWT 内容类型、自定义签名、JSON 和 XML 的 XPath
A9:2021 – 安全日志记录和监控故障	用户可配置的自定义日志记录、NetScaler 管理和分析系统

A1:2021 访问控制失效

认证用户被允许执行的操作的限制通常未得到正确执行。攻击者可以利用这些缺陷来访问未经授权的功能和数据，例如访问其他用户的帐户、查看敏感文件、修改其他用户的数据、更改访问权限。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Web 应用防火墙 保护

- 支持所有应用程序流量的身份验证、授权和审计的 AAA 功能允许站点管理员使用 ADC 设备管理访问控制。
- ADC 设备 AAA 模块中的授权安全功能使设备能够验证每个用户应被允许访问受保护服务器上的哪些内容。
- 表单字段一致性：如果对象引用作为隐藏字段存储在表单中，则可以使用表单字段一致性来验证这些字段在后续请求中未被篡改。
- Cookie 代理和 Cookie 一致性：存储在 Cookie 值中的对象引用可以通过这些保护进行验证。
- 启动 URL 检查与 URL 闭包：允许用户访问预定义的 URL 允许列表。URL 闭包会构建用户会话期间在有效响应中看到的所有 URL 列表，并在该会话期间自动允许访问这些 URL。

A2:2021 - 加密故障

许多 Web 应用程序和 API 未能正确保护敏感数据，例如财务、医疗保健和 PII。攻击者可能会窃取或修改这些保护不力的数据，以进行信用卡欺诈、身份盗窃或其他犯罪。敏感数据在没有额外保护（例如静态或传输中的加密）的情况下可能会受到损害，并且在与浏览器交换时需要采取特殊预防措施。

NetScaler Web 应用防火墙防护

- Web Application Firewall 保护应用程序免受敏感数据（如信用卡详细信息）泄露。
- 敏感数据可以在安全商务保护中配置为安全对象，以避免暴露。
- Cookie 中的任何敏感数据都可以通过 Cookie 代理和 Cookie 加密进行保护。

A3:2021- 注入

注入缺陷，例如 SQL、NoSQL、OS 和 LDAP 注入，发生在将不受信任的数据作为命令或查询的一部分发送到解释器时。攻击者的恶意数据可以欺骗解释器运行意外命令或在未经适当授权的情况下访问数据。

每当应用程序在没有适当验证或转义的情况下在新网页中包含不受信任的数据，或者使用可以创建 HTML 或 JavaScript 的浏览器 API 更新现有网页中的用户提供数据时，就会发生 XSS 漏洞。XSS 允许攻击者在受害者的浏览器中运行脚本，这可能劫持用户会话、篡改网站或将用户重定向到恶意站点。

NetScaler Web 应用防火墙 保护

- SQL 注入防护功能可防止常见的注入攻击。可以上传自定义注入模式，以防止任何类型的注入攻击，包括 XPath 和 LDAP。这适用于 HTML 和 XML 有效负载。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 自动更新签名功能使注入签名保持最新。
- 字段格式保护功能允许管理员将任何用户参数限制为正则表达式。例如，您可以强制邮政编码字段只包含整数，甚至是 5 位整数。
- 表单字段一致性根据用户会话表单签名验证每个提交的用户表单，以确保所有表单元素的有效性。
- 缓冲区溢出检查可确保 URL、标头和 Cookie 在正确的限制范围内，从而阻止任何注入大型脚本或代码的尝试。
- XSS 保护可防止常见的 XSS 攻击。可以上传自定义 XSS 模式以修改允许的标签和属性的默认列表。ADC WAF 使用允许的 HTML 属性和标签的白名单来检测 XSS 攻击。这适用于 HTML 和 XML 有效负载。
- ADC WAF 阻止 OWASP XSS 过滤器评估备忘单中列出的所有攻击。
- 字段格式检查可防止攻击者发送不适当的 Web 表单数据，这可能是一种潜在的 XSS 攻击。
- 表单字段一致性。

A5:2021 - 安全配置错误

安全配置错误是最常见的问题。这通常是由于不安全的默认配置、不完整或临时配置、开放的云存储、配置错误的 HTTP 标头以及包含敏感信息的详细错误消息造成的。所有操作系统、框架、库和应用程序不仅必须安全配置，而且必须及时修补和升级。

许多旧的或配置不当的 XML 处理器会评估 XML 文档中的外部实体引用。外部实体可用于使用文件 URI 处理程序、内部文件共享、内部端口扫描、远程代码执行和拒绝服务攻击来泄露内部文件。

NetScaler Web 应用防火墙 保护

- 应用程序防火墙生成的 PCI-DSS 报告记录了防火墙设备上的安全设置。
- 扫描工具的报告将转换为 ADC WAF 签名，以处理安全配置错误。
- NetScaler Web App Firewall Web Application Firewall 支持 Cenzic、IBM AppScan（企业版和标准版）、Qualys、TrendMicro、WhiteHat 和自定义漏洞扫描报告。
- 除了检测和阻止可用于攻击基于 XML 的应用程序（即跨站点脚本、命令注入等）的常见应用程序威胁之外。
- NetScaler Web App Firewall Web Application Firewall 包含一套丰富的 XML 特定安全保护。其中包括用于彻底验证 SOAP 消息和 XML 有效负载的架构验证，以及强大的 XML 附件检查，以阻止包含恶意可执行文件或病毒的附件。
- 自动流量检查方法可阻止针对获取访问权限的 URL 和表单上的 XPath 注入攻击。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Web App Firewall Web Application Firewall 还可以阻止各种 DoS 攻击，包括外部实体引用、递归扩展、过度嵌套以及包含长属性或多个属性和元素的恶意消息。

A6:2021 - 易受攻击和过时的组件

组件（例如库、框架和其他软件模块）以与应用程序相同的权限运行。如果易受攻击的组件被利用，此类攻击可能导致严重的数据丢失或服务器接管。使用已知漏洞组件的应用程序和 API 可能会破坏应用程序防御并导致各种攻击和影响。

NetScaler Web 应用防火墙防护

- 我们建议保持第三方组件最新。
- 转换为 ADC 签名的漏洞扫描报告可用于虚拟修补这些组件。
- 可以使用适用于这些易受攻击组件的应用程序防火墙模板。
- 可以将自定义签名与防火墙绑定以保护这些组件。

A7:2021–身份验证失效

应用程序中与身份验证和会话管理相关的功能常常实现不正确，这使得攻击者能够窃取密码、密钥或会话令牌，或者利用其他实现缺陷来暂时或永久地冒充其他用户的身份。

NetScaler Web App Firewall 保护措施

- NetScaler AAA 模块执行用户身份验证，并为后端应用程序提供单点登录功能。它已集成到 NetScaler AppExpert 策略引擎中，以允许基于用户和组信息制定自定义策略。
- 利用 SSL 卸载和 URL 转换功能，防火墙还可以帮助站点使用安全的传输层协议，以防止通过网络嗅探窃取会话令牌。
- 可以采用 Cookie 代理和 Cookie 加密来完全缓解 Cookie 窃取。

A8:2021 - 软件和数据完整性故障

不安全的序列化常常导致远程代码执行。即使序列化缺陷不会导致远程代码执行，它们也可以用于执行攻击，包括重放攻击、注入攻击和权限提升攻击。

NetScaler Web App Firewall 保护措施

- 使用自定义签名的 JSON 有效负载检查。
- XML 安全：防止 XML 拒绝服务 (xDoS)、XML SQL 和 Xpath 注入以及跨站点脚本、格式检查、WS-I 基本配置文件合规性、XML 附件检查。
- 可以使用字段格式检查、Cookie 一致性和字段一致性。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A9:2021 - 安全日志记录和监控故障

不足的日志记录和监控，加上与事件响应的缺失或无效集成，使得攻击者能够进一步攻击系统、维持持久性、转向更多系统，以及篡改、提取或销毁数据。大多数泄露研究表明，检测到泄露的时间超过 200 天，通常是由外部方而非内部流程或监控检测到的。

NetScaler Web App Firewall 保护措施

- 当为安全检查或签名启用日志操作时，生成的日志消息会提供有关应用程序防火墙在保护您的网站和应用程序时观察到的请求和响应的信息。
- 应用程序防火墙提供了使用内置 ADC 数据库的便利，用于识别恶意请求源 IP 地址对应的位置。
- 默认格式 (PI) 表达式提供了灵活性，可以自定义日志中包含的信息，并可选择将特定数据添加到应用程序防火墙生成的日志消息中进行捕获。
- 应用程序防火墙支持 CEF 日志。

参考

- HTML SQL 注入检查
- XML SQL 注入检查
- 使用命令行配置 HTML 跨站点脚本检查
- XML 跨站点脚本检查
- 使用命令行配置缓冲区溢出安全检查
- 添加或删除签名对象
- 配置或修改签名对象
- 更新签名对象
- Snort 规则集成
- Bot 检测
- 在 Microsoft Azure 上部署 NetScaler VPX 实例

为 NetScaler Gateway 设备配置地址池内网 IP

在某些情况下，使用 NetScaler Gateway 插件连接的用户需要为 NetScaler Gateway 设备提供唯一的 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唯一的 IP 地址别名。您可以使用内网 IP (IIP) 地址配置地址池。

您可以通过以下两个步骤在 Azure 上部署的 NetScaler Gateway 设备上配置地址池：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在 Azure 中注册地址池中使用的私有 IP 地址
- 在 NetScaler Gateway 设备中配置地址池

在 Azure 门户中注册私有 IP 地址

在 Azure 中，您可以部署具有多个 IP 地址的 NetScaler VPX 实例。您可以通过两种方式向 VPX 实例添加 IP 地址：

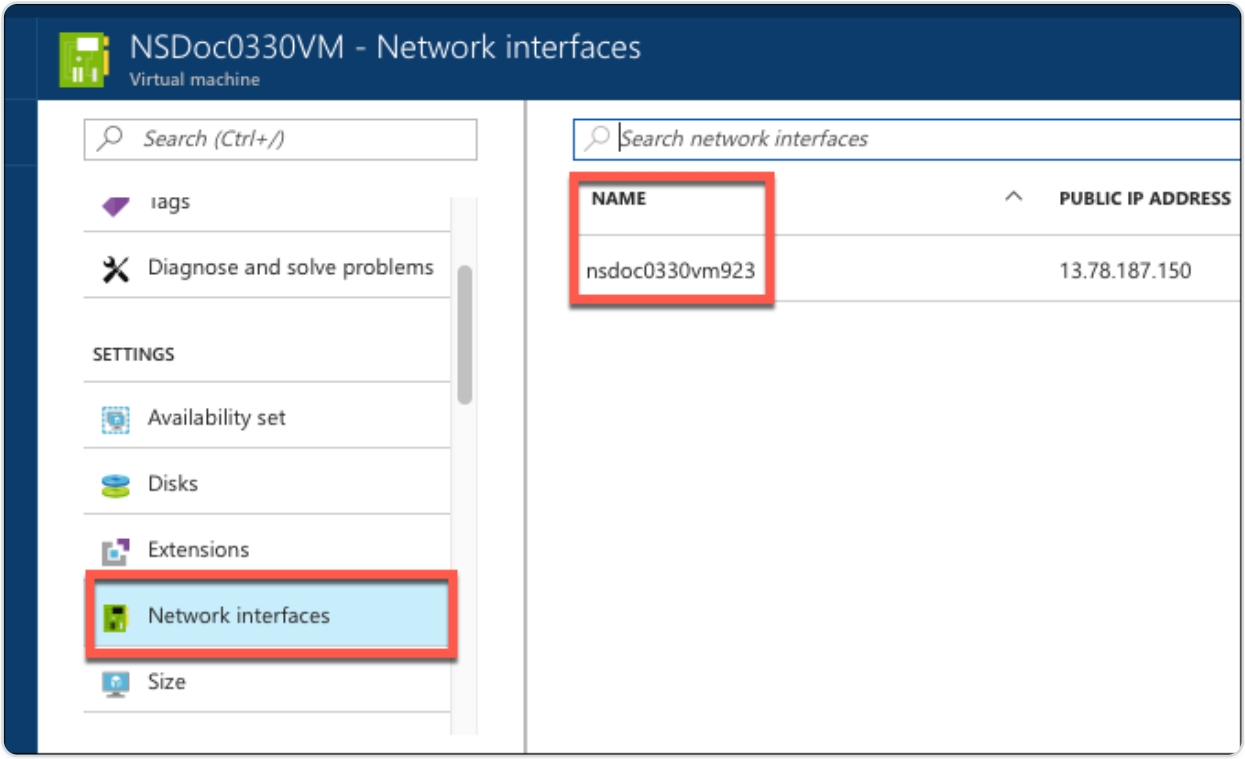
a. 预置 VPX 实例时

有关在预置 VPX 实例时如何添加多个 IP 地址的更多信息，请参阅 为 NetScaler 独立实例配置多个 IP 地址。要在使用 PowerShell 命令预置 VPX 实例时添加 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。

b. 预置 VPX 实例后

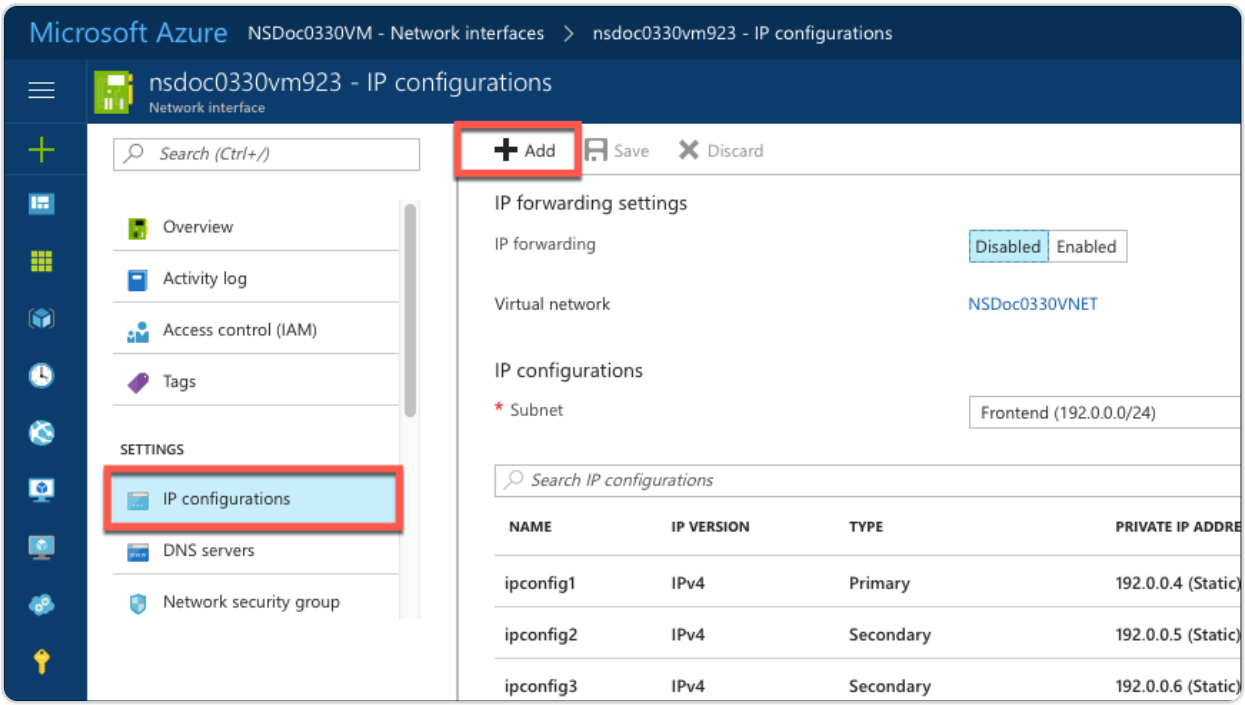
预置 VPX 实例后，请按照以下步骤在 Azure 门户中注册私有 IP 地址，您将在 NetScaler Gateway 设备中将其配置为地址池。

1. 在 Azure Resource Manager (ARM) 中，转到已创建的 NetScaler VPX 实例 > **网络接口**。选择绑定到您要注册的 IIP 所属子网的网络接口。

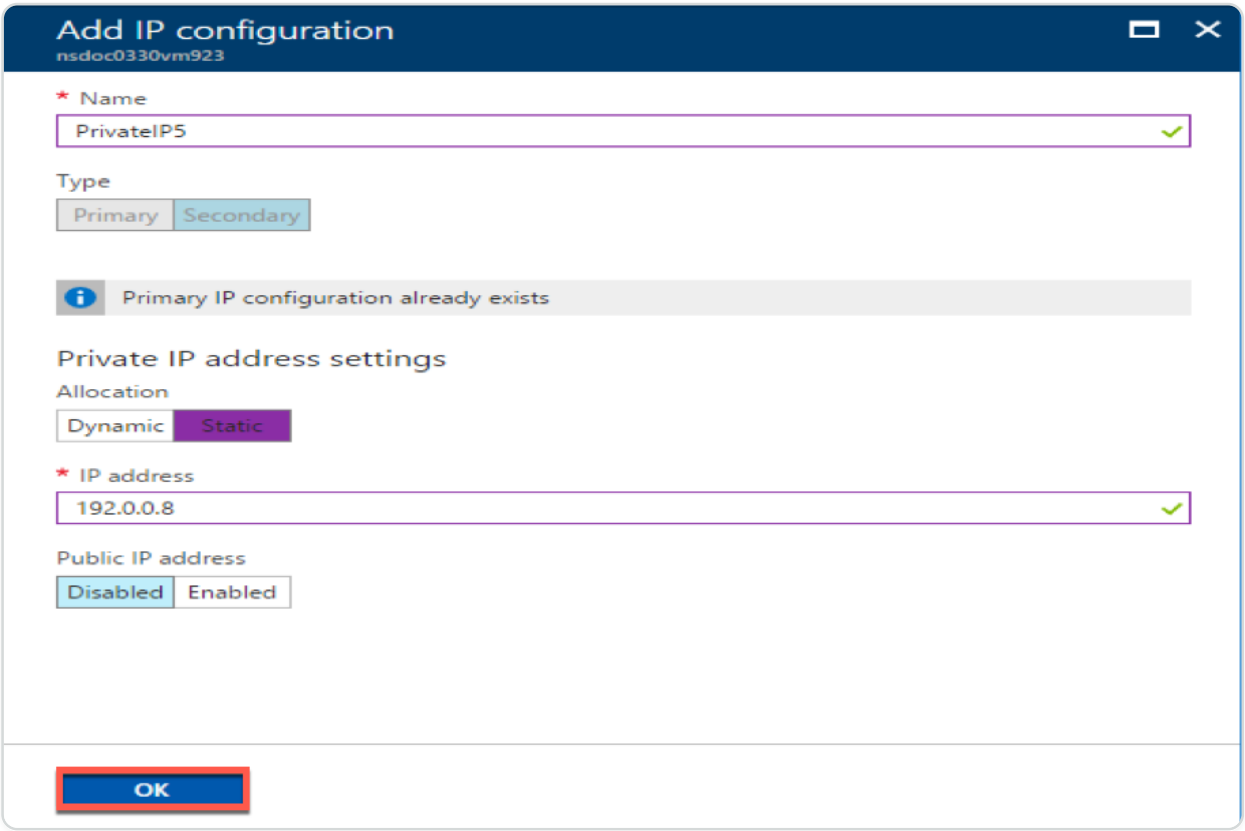


2. 单击 **IP 配置**，然后单击 **添加**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 提供所需详细信息，如下例所示，然后单击 **OK**。



在 NetScaler Gateway 设备中配置地址池

有关如何在 NetScaler Gateway 上配置地址池的更多信息，请参阅 配置地址池。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

限制：

您无法将一系列 IIP 地址绑定到用户。地址池中使用的每个 IIP 地址都必须注册。

使用 PowerShell 命令为 NetScaler VPX 独立实例配置多个 IP 地址

在 Azure 环境中，可以部署具有多个 NIC 的 NetScaler VPX 虚拟设备。每个 NIC 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。您可以将相同的脚本用于多 NIC 和多 IP 部署。

注意：

在本文档中，IP-Config 指的是与单个 NIC 关联的一对 IP 地址（公共 IP 和私有 IP）。有关更多信息，请参阅 (/zh-cn/vpx/13-1/deploy-vpx-on-azure/azure-terminology.html) 部分中的 。

用例

在此用例中，单个 NIC 连接到虚拟网络 (VNET)。此 NIC 关联了三个 IP 配置，如以下表格所示。

IP 配置	关联对象
IP 配置-1	静态公共 IP 地址；静态私有 IP 地址
IP 配置-2	静态公共 IP 地址；静态私有地址
IP 配置-3	静态私有 IP 地址

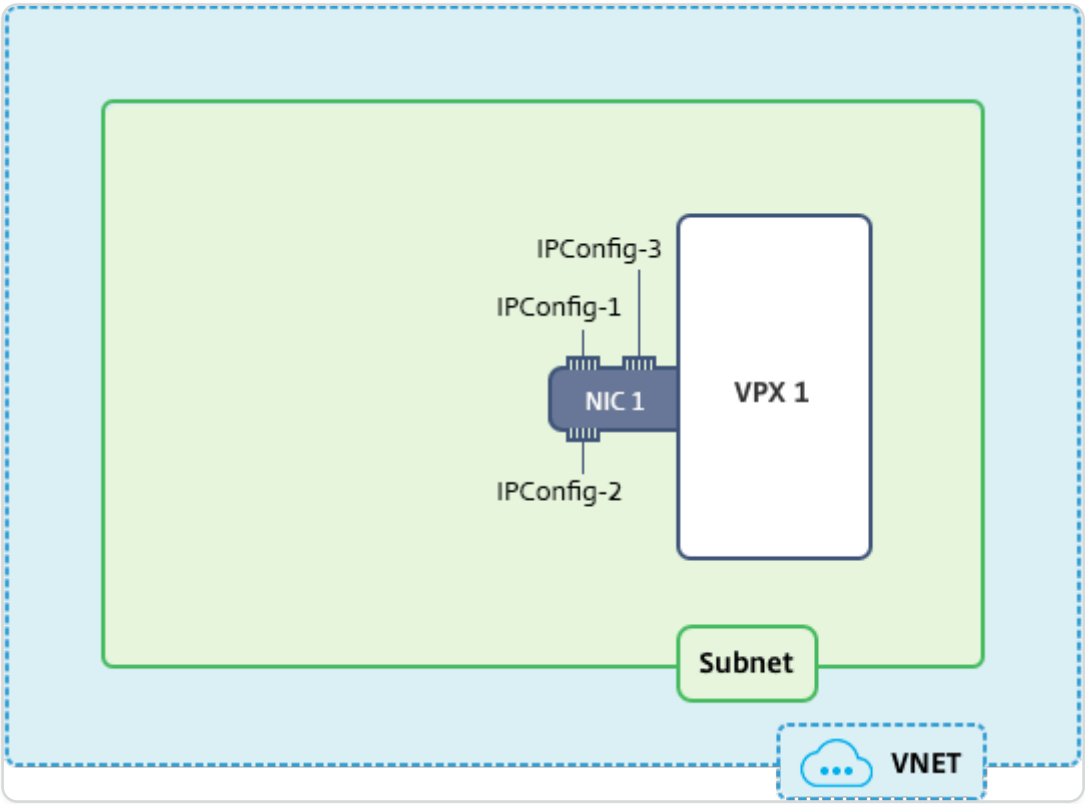
注意：

IPConfig-3 未与任何公共 IP 地址关联。

图：拓扑

以下是用例的视觉表示。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

在多网卡、多 IP 的 Azure NetScaler VPX 部署中，与主（第一个）网卡的主（第一个）`IPConfig` 关联的私有 IP 地址会自动添加为设备的管理 NSIP 地址。与 `IPConfigs` 关联的其余私有 IP 地址必须根据您的要求，使用 `add ns ip` 命令在 VPX 实例中添加为 VIP 或 SNIP。

以下是在独立模式下为 NetScaler VPX 虚拟设备配置多个 IP 地址所需的步骤摘要：

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. 创建公共 IP 地址
7. 分配 IP 配置
8. 创建网卡
9. 创建 NetScaler VPX 实例
10. 检查 NIC 配置

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. 检查 VPX 侧配置

脚本

参数

以下是本文档中用例的示例参数设置。

```
$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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$vmSize="Standard\_DS4\_V2" (This parameter creates a VM with up to four
NICs.)
```

注意：

VPX 实例的最低要求是 2 个 vCPU 和 2 GB RAM。

```
$publisher="Citrix"

$offer="netscalervpx110-6531" (You can use different offers.)

$sku="netscalerbyol" (According to your offer, the SKU can be different.)

$version="latest"

$pubIPName1="PIP1"

$pubIPName2="PIP2"

$domName1="multiipvpx1"

$domName2="multiipvpx2"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$vmNamePrefix="VPXMultiIP"

$osDiskSuffix="osmultiipalbdiskdb1"

**Network Security Group (NSG)-related information**:

$nsgName="NSG-MultiIP"

$rule1Name="Inbound-HTTP"

$rule2Name="Inbound-HTTPS"

$rule3Name="Inbound-SSH"

$IpConfigName1="IPConfig1"

$IPConfigName2="IPConfig-2"

$IPConfigName3="IPConfig-3"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。您必须为任何提供流量的端口向网络安全组添加规则。

   ```
   $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
   ```

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`$vnet=New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName $rgName -Location $locName -AddressPrefix $vNetAddressRange -Subnet $frontendSubnet`

3. 检索子网。

`$subnetName="frontEndSubnet"` `$subnet1=$vnet.Subnets|?{$_.Name -eq $subnetName}`

6. 创建公共 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：

使用前检查域名可用性。

IP 地址的分配方法可以是动态的或静态的。

7. 分配 IP 配置

在此用例中，分配 IP 地址之前请考虑以下几点：

- 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：

当您为 NIC 分配多个 IP 配置时，其中一个配置必须指定为主配置。

```
$IPAddress1="11.6.1.27"

$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1
-Subnet $subnet1 -PrivateIpAddress $IPAddress1 -PublicIpAddress $pip1 –
Primary

$IPAddress2="11.6.1.28"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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
```

使用符合子网要求的有效 IP 地址并检查其可用性。

8. 创建 NIC

`$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。

   `$cred=Get-Credential -Message "Type the name and password for VPX login."` `$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName $vmName -Credential $cred` `$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher -Offer $offer -Skus $sku -Version $version`

4. 添加网卡。

   `$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -Primary`

   注意：

   在多网卡 VPX 部署中，一个网卡必须是主网卡。因此，在将该网卡添加到 VPX 实例时，必须附加“-Primary”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 指定操作系统磁盘并创建虚拟机。

   `$osDiskName=$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

VPX 实例启动后，您可以使用以下命令检查分配给 VPX 网卡 `IPConfigs` 的 IP 地址。

```
$nic.IPConfig
```

11. 检查 VPX 端配置

当 NetScaler VPX 实例启动时，与主网卡的主 `IPconfig` 关联的私有 IP 地址将作为 NSIP 地址添加。其余私有 IP 地址必须根据您的要求添加为 VIP 或 SNIP 地址。使用以下命令。

```
add nsip <Private IPAddress><netmask> -type VIP/SNIP
```

您现在已为独立模式下的 NetScaler VPX 实例配置了多个 IP 地址。

用于 Azure 部署的其他 PowerShell 脚本

本节提供 PowerShell cmdlet 命令，您可以使用它们在 Azure PowerShell 中执行以下配置：

- 预配 NetScaler VPX 独立实例
- 在具有 Azure 外部负载均衡器的高可用性设置中预配 NetScaler VPX 对
- 在具有 Azure 内部负载均衡器的高可用性设置中预配 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-备用高可用性设置上配置 GSLB
- 使用 PowerShell 命令为独立模式下的 NetScaler VPX 实例配置多个 IP 地址

预配 NetScaler VPX 独立实例

1. **创建资源组**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

资源组可以包含解决方案的所有资源，也可以只包含您希望作为组进行管理的资源。此处指定的位置是该资源组中资源的默认位置。请确保所有创建负载均衡器的命令都使用相同的资源组。

`$rgName="<resource group name>"` `$locName="<location name, such as West US>` `New-AzureRmResourceGroup -Name $rgName -Location $locName`

例如：

```
$rgName = "ARM-VPX"

$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一个仅包含小写字母和数字的唯一名称。

`$saName="<storage account name>"` `$saType="<storage account type>"`，指定以下其中一项：`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**

可用性集有助于在停机期间（例如在维护期间）保持虚拟机可用。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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. **创建虚拟网络**

   如果之前未创建子网，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-AzureRmVirtualNetworkSubnetConfig -Name backendSubnet -AddressPrefix $BackendAddressPrefix` `New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -Subnet $frontendSubnet, $backendSubnet`

   例如：

   ```
   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
   frontendSubnet -AddressPrefix $FrontendAddressPrefix



   $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
   backendSubnet -AddressPrefix $BackendAddressPrefix



   New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName
   -Location $locName -AddressPrefix $vnetAddressPrefix -Subnet
   $frontendSubnet,$backendSubnet
   ```

5. **创建 NIC**

   创建 NIC 并将 NIC 与 NetScaler VPX 实例关联。在上述过程中创建的前端子网索引为 0，后端子网索引为 1。现在通过以下三种方式之一创建 NIC：

   a) *具有公共 IP 地址的 NIC*

   `$nicName="<name of the NIC of the VM>"`

   `$pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName $rgName -Location $locName -AllocationMethod Dynamic`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`$nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -PublicIpAddressId $pip.Id`

b) *具有公共 IP 和 DNS 标签的 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`

在分配 $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) *具有动态公共地址和静态私有 IP 地址的 NIC*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

确保您添加到 VM 的私有（静态）IP 地址必须与指定子网的范围相同。

```
$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 映像**

```
$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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`$pubName="citrix"`

以下命令用于显示 Citrix® 的所有产品/服务：

```
Get-AzureRMVMImageOffer -Location $locName -Publisher $pubName | Select
Offer



$offerName="netscalervpx110-6531"
```

以下命令用于了解发布者针对特定产品/服务名称提供的 SKU：

`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：

```
$diskName="dynamic"



$pubName="citrix"



$offerName="netscalervpx110-6531"



$skuName="netscalerbyol"



$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -Name
$saName
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$osDiskUri=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds/" +
$diskName  + ".vhd"



$vm=Set-AzureRmVMOSDisk -VM $vm -Name $diskName -VhdUri $osDiskUri
-CreateOption fromImage
```

当您从市场中的映像创建 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`

在具有 Azure 外部负载均衡器的高可用性设置中预配 NetScaler VPX 对

使用您的 Azure 用户凭据登录到 AzureRmAccount。

1. **创建资源组**

   这里指定的位置是该资源组中资源的默认位置。确保所有用于创建负载均衡器的命令都使用相同的资源组。

   `$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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **创建存储帐户**

   为您的存储帐户选择一个仅包含小写字母和数字的唯一名称。

   `$saName="<storage account name>"`

   `$saType="<storage account type>"`，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**

   如果之前未创建子网，则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"
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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。

将前端和后端子网分配给您在此步骤中早些时候创建的虚拟网络。

如果前端子网是数组 VNet 的第一个元素，则 subnetId 必须是 $vnet.Subnets\[0\].Id。

如果前端子网是数组中的第二个元素，则 subnetId 必须是 $vnet.Subnets\[1\].Id，依此类推。

5. **配置前端 IP 地址并创建后端地址池**

   为传入的负载均衡器网络流量配置前端 IP 地址，并创建后端地址池以接收负载均衡流量。

```
$pubName="PublicIp1"


$publicIP1 = New-AzureRmPublicIpAddress -Name $pubName
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-ResourceGroupName $rgName -Location $locName -AllocationMethod Static
-DomainNameLabel nsvpx
```

注意：

检查 DomainNameLabel 值的可用性。

```
$FIPName = "ELBFIP"



$frontendIP1 = New-AzureRmLoadBalancerFrontendIpConfig -Name $FIPName
-PublicIpAddress $publicIP1



$BEPool = "LB-backend-Pool"



$beaddresspool1= New-AzureRmLoadBalancerBackendAddressPoolConfig -Name
$BEPool
```

6. **创建运行状况探测**

   创建端口为 9000、间隔为 5 秒的 TCP 运行状况探测。

```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name HealthProbe
-Protocol Tcp -Port 9000 -IntervalInSeconds 5 -ProbeCount 2
```

7. **创建负载均衡规则**

   为您正在进行负载均衡的每个服务创建一个 LB 规则。

   例如：

   您可以使用以下示例对 HTTP 服务进行负载均衡。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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**

   为不进行负载均衡的服务创建 NAT 规则。

   例如，当为 NetScaler VPX 实例创建 SSH 访问时。

   注意：

   两个 NAT 规则的协议-前端端口-后端端口三元组不能相同。

```
$inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -Name
SSH1     -FrontendIpConfiguration $frontendIP1 -Protocol TCP
-FrontendPort 22 -BackendPort 22



$inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -Name
SSH2 -FrontendIpConfiguration $frontendIP1 -Protocol TCP -FrontendPort
10022 -BackendPort 22
```

9. **创建负载均衡器实体**

   创建负载均衡器，并将所有对象（NAT 规则、负载均衡器规则、探测配置）添加在一起。

```
$lbName="ELB"



$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name
$lbName -Location $locName -InboundNatRule $inboundNATRule1,
$inboundNATRule2 -FrontendIpConfiguration $frontendIP1
-LoadBalancingRule $lbrule1 -BackendAddressPool $beAddressPool1 -Probe
$healthProbe
```

10. **创建 NIC**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

创建两个 NIC，并将每个 NIC 与每个 VPX 实例关联

a) NIC1 与 VPX1

例如：

```
$nicName="NIC1"


$lbName="ELB"


$bePoolIndex=0


\* Rule indexes starts from 0.


$natRuleIndex=0


$subnetIndex=0


\* Frontend subnet index


$lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName


$nic1=New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
$rgName -Location $locName -Subnet $vnet.Subnets\[$subnetIndex\]
-LoadBalancerBackendAddressPool $lb.BackendAddressPools\[$bePoolIndex\]
-LoadBalancerInboundNatRule $lb.InboundNatRules\[$natRuleIndex\]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b) NIC2 与 VPX2

例如：

```
$nicName="NIC2"


$lbName="ELB"


$bePoolIndex=0


$natRuleIndex=1


\* Second Inbound NAT (SSH) rule we need to use


`$subnetIndex=0


\* Frontend subnet index


$lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName


$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**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

创建两个 NetScaler VPX 实例，作为同一资源组和可用性集的一部分，并将其附加到外部负载均衡器。

a) NetScaler VPX 实例 1

例如：

```
$vmName="VPX1"


$vmSize="Standard\_A3"


$pubName="citrix"


$offerName="netscalervpx110-6531"


$skuName="netscalerbyol"


$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName


$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize
-AvailabilitySetId $avset.Id


$cred=Get-Credential -Message "Type Credentials which will be used to
login to VPX instance"


$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName $vmName
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-Credential $cred -Verbose



$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -Offer
$offerName -Skus $skuName -Version "latest"



$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $nic1.Id



$diskName="dynamic"



$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -Name
$saName



$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/" +
$diskName  + ".vhd"



$vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri $osDiskUri1
-CreateOption fromImage



Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
-Name $skuName



New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM $vm1
```

b) NetScaler VPX 实例 2

例如：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$vmName="VPX2"


$vmSize="Standard\_A3"


$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName


$vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize
-AvailabilitySetId $avset.Id


$cred=Get-Credential -Message " Type Credentials which will be used to
login to VPX instance "


$vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName $vmName
-Credential $cred -Verbose


$vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -Offer
$offerName -Skus $skuName -Version "latest"


$vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id


$diskName="dynamic"


$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -Name
$saName
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$osDiskUri1=$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**

    当两个 NetScaler VPX 实例都启动后，使用 SSH 协议连接到这两个 NetScaler VPX 实例以配置虚拟机。

    a) 主动-主动：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。

在具有 Azure 内部负载均衡器的高可用性设置中预配 NetScaler VPX 对

使用您的 Azure 用户凭据登录到 AzureRmAccount。

1. **创建资源组**

   此处指定的位置是该资源组中资源的默认位置。请确保所有创建负载均衡器的命令都使用相同的资源组。

   `$rgName="\<resource group name\>"`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`$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一个仅包含小写字母和数字的唯一名称。

   `$saName="<storage account name>"`

   `$saType="<storage account type>"`，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**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**

   如果之前未创建子网，则添加至少包含一个子网的新虚拟网络。

```
$vnetName = "LBVnet"



$vnetAddressPrefix="10.0.0.0/16"



$FrontendAddressPrefix="10.0.1.0/24"



$BackendAddressPrefix="10.0.2.0/24"



$vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
$rgName -Location $locName -AddressPrefix $vnetAddressPrefix -Subnet
$frontendSubnet,$backendSubnet\`



$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
frontendSubnet -AddressPrefix $FrontendAddressPrefix



$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
backendSubnet -AddressPrefix $BackendAddressPrefix
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

根据您的要求选择 AddressPrefix 参数值。

将前端和后端子网分配给您在此步骤中早些时候创建的虚拟网络。

如果前端子网是数组 VNet 的第一个元素，则 subnetId 必须是 $vnet.Subnets\[0\].Id。

如果前端子网是数组中的第二个元素，则 subnetId 必须是 $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**

为您不进行负载均衡的服务创建 NAT 规则。

```
$inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -Name
"Inboundnatrule1" -FrontendIpConfiguration $frontendIP -Protocol TCP
-FrontendPort 3441 -BackendPort 3389



$inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -Name
"RDP2" -FrontendIpConfiguration $frontendIP -Protocol TCP -FrontendPort
3442 -BackendPort 3389
```

根据您的要求使用前端和后端端口。

7. **创建运行状况探测**

创建一个 TCP 运行状况探测，端口为 9000，间隔为 5 秒。

```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name "HealthProbe"
 " -Protocol tcp -Port 9000 -IntervalInSeconds 5 -ProbeCount 2
```

8. **创建负载均衡规则**

为您正在进行负载均衡的每个服务创建一条 LB 规则。

例如：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以使用以下示例对 HTTP 服务进行负载均衡。

```
$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和后端端口。

9. **创建负载均衡器实体**

   创建负载均衡器，将所有对象（NAT 规则、负载均衡器规则、探测配置）添加在一起。

```
$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 与每个 NetScaler VPX 实例关联。

```
$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。私有 IP 必须与所添加子网位于同一子网中。

```
$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\[1\].
```

    此 NIC 用于 NetScaler VPX 2。参数 `Private IPAddress` 可以根据您的要求使用任何私有 IP。

11. **创建 NetScaler VPX 实例**

    创建两个属于同一资源组和可用性集的 VPX 实例，并将其附加到内部负载均衡器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a) NetScaler VPX 实例 1

例如：

```
$vmName="VPX1"


$vmSize="Standard\_A3"


$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName


$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize
-AvailabilitySetId $avset.Id


$cred=Get-Credential -Message "Type Credentials which will be used to
login to VPX instance"


$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName $vmName
-Credential $cred -Verbose


$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -Offer
$offerName -Skus $skuName -Version "latest"


$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $backendnic1.Id


$diskName="dynamic"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -Name
$saName


$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/" +
$diskName  + ".vhd"


$vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri $osDiskUri1
-CreateOption fromImage


Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
-Name $skuName


New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM $vm1
```

b) NetScaler VPX 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM $vm2
```

12. **配置虚拟机**

    当两个 NetScaler VPX 实例启动时，使用 SSH 协议连接到这两个 NetScaler VPX 实例以配置虚拟机。

    a) 主动-主动: 在两个 NetScaler VPX 实例的命令行上运行相同的配置命令。

    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。

Azure 常见问题

- **从 Azure Marketplace 安装的 NetScaler VPX 实例的升级过程与本地升级过程不同吗？**

  不。您可以使用标准的 NetScaler VPX 升级过程，将 Microsoft Azure 云中的 NetScaler VPX 实例升级到 NetScaler VPX 11.1 或更高版本。您可以使用 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，请转到 **NetScaler 下载** > **NetScaler 固件**。

- **如何纠正在 Azure 上托管的 NetScaler VPX 实例上观察到的 MAC 移动和接口静默？**

  在 Azure 多 NIC 环境中，默认情况下，所有数据接口都可能显示 MAC 移动和接口静默。为避免 Azure 环境中的 MAC 移动和接口静默，Citrix 建议您为 NetScaler VPX 实例的每个数据接口（不带标签）创建一个 VLAN，并绑定 Azure 中 NIC 的主 IP。

  有关详细信息，请参阅 CTX224626 文章。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 Google Cloud Platform 上部署 NetScaler VPX 实例

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您的业务需求。您可以在 GCP 中将 VPX 实例部署为独立实例。支持单 NIC 和多 NIC 配置。

支持的功能

GCP 上支持所有 Premium、Advanced 和 Standard 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 实例必须至少具有 2 个 vCPU 和 4 GB RAM。

注意事项

在开始部署之前，请考虑以下 GCP 特定的注意事项。

- 创建实例后，您无法添加或删除任何网络接口。
- 对于多 NIC 部署，请为每个 NIC 创建单独的 VPC 网络。一个 NIC 只能与一个网络关联。
- 对于单 NIC 实例，GCP 控制台默认创建一个网络。
- 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：部署多网卡、多 IP 的独立 VPX 实例

此场景说明了如何在 GCP 中部署 NetScaler VPX 独立实例。在此场景中，您将创建一个具有多个网卡的独立 VPX 实例。该实例与后端服务器（服务器场）通信。

GCP 部署场景(/en-us/vpx/media/deploy-vpx-gcp-scenario.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

创建三个网卡用于以下目的。

网卡	用途	关联到 VPC 网络
网卡 0	用于处理管理流量 (NetScaler IP)	管理网络
网卡 1	用于处理客户端流量 (VIP)	客户端网络
网卡 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：

- VPX 实例和后端服务器。
- 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. 为端口 22、80 和 443 创建防火墙规则
3. 创建一个具有三个 NIC 的实例

注意：

在您创建 VPC 网络的同一区域中创建实例。

步骤 1. 创建 VPC 网络。

创建三个 VPC 网络，分别与管理 NIC、客户端 NIC 和服务器 NIC 相关联。要创建 VPC 网络，请登录 **Google console > Networking > VPC network > Create VPC Network**。填写屏幕截图中所示的必填字段，然后单击 **Create**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

netscaler-vpx-platform-eng

Create a VPC network

Name

vpxmgmt

Description (Optional)

management vpc

Subnets

Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. Learn more

Subnet creation mode

Custom | Automatic

New subnet

Name

vpxmgmtsubnet

Add a description

Region

asia-east1

IP address range

192.168.30.0/24

Create secondary IP range

Private Google access

- (•) On
- ( ) Off

Flow logs

同样，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. 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。有关防火墙规则的更多信息，请参阅防火墙规则概述。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

netscaler-vpx-platform-eng

Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Name

vpxmgmtingressrule

Description (Optional)

management traffic ingress rules

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. Learn more

- On
- Off

Network

vpxmgmt

Priority

Priority can be 0 - 65535 Check priority of other firewall rules

1000

Direction of traffic

- Ingress
- Egress

Action on match

- Allow
- Deny

Targets

All instances in the network

Source filter

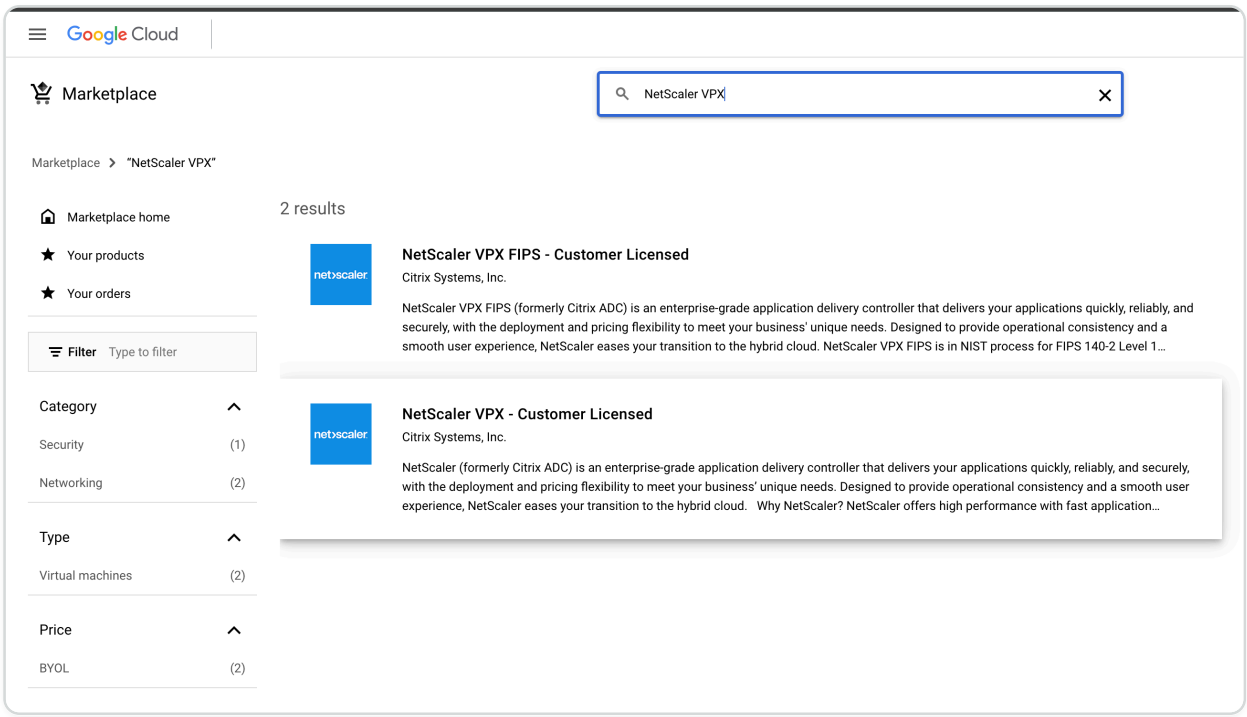
IP ranges

Source IP ranges

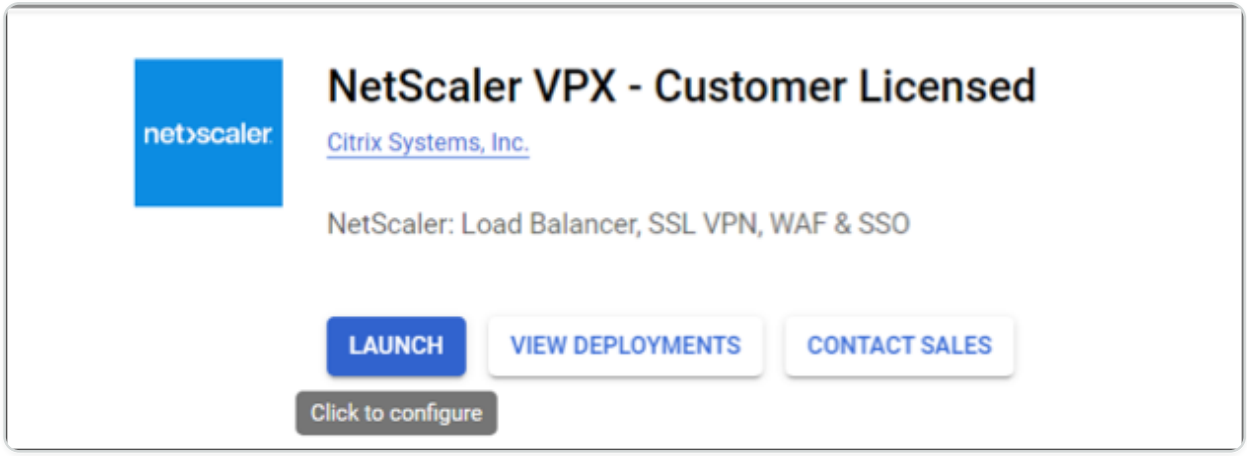
0.0.0.0/0

步骤 3. 创建 VPX 实例。

1. 登录到 GCP 控制台。
2. 导航到GCP Marketplace。
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。

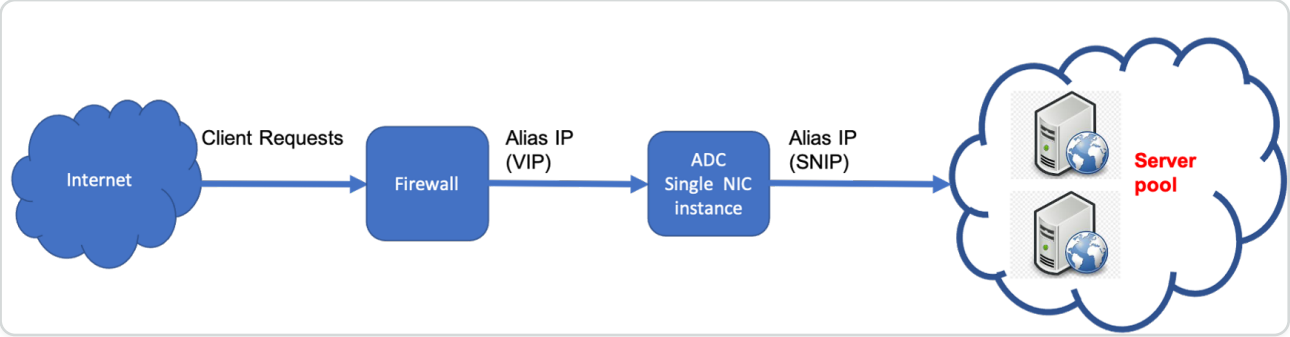
6. 部署的实例显示在**Compute Engine > VM 实例**下。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 GCP SSH 或串行控制台配置和管理 VPX 实例。

场景：部署单 NIC 独立 VPX 实例

此场景说明了如何在 GCP 中部署具有单个 NIC 的 NetScaler VPX 独立实例。使用别名 IP 地址来实现此部署。



创建单个 NIC (NIC0) 用于以下目的：

- 在管理网络中处理管理流量 (NetScaler IP)。
- 在客户端网络中处理客户端流量 (VIP)。
- 在后端服务器网络中与后端服务器 (SNIP) 通信。

设置以下各项之间所需的通信路由：

- 实例和后端服务器。
- 实例和公共互联网上的外部主机。

部署步骤摘要

1. 为 NIC0 创建 VPC 网络。
2. 创建用于端口 22、80 和 443 的防火墙规则。
3. 创建具有单个 NIC 的实例。
4. 将别名 IP 地址添加到 VPX。
5. 在 VPX 上添加 VIP 和 SNIP。
6. 添加负载均衡虚拟服务器。
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均衡虚拟服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

在您已创建 VPC 网络的同一区域中创建实例。

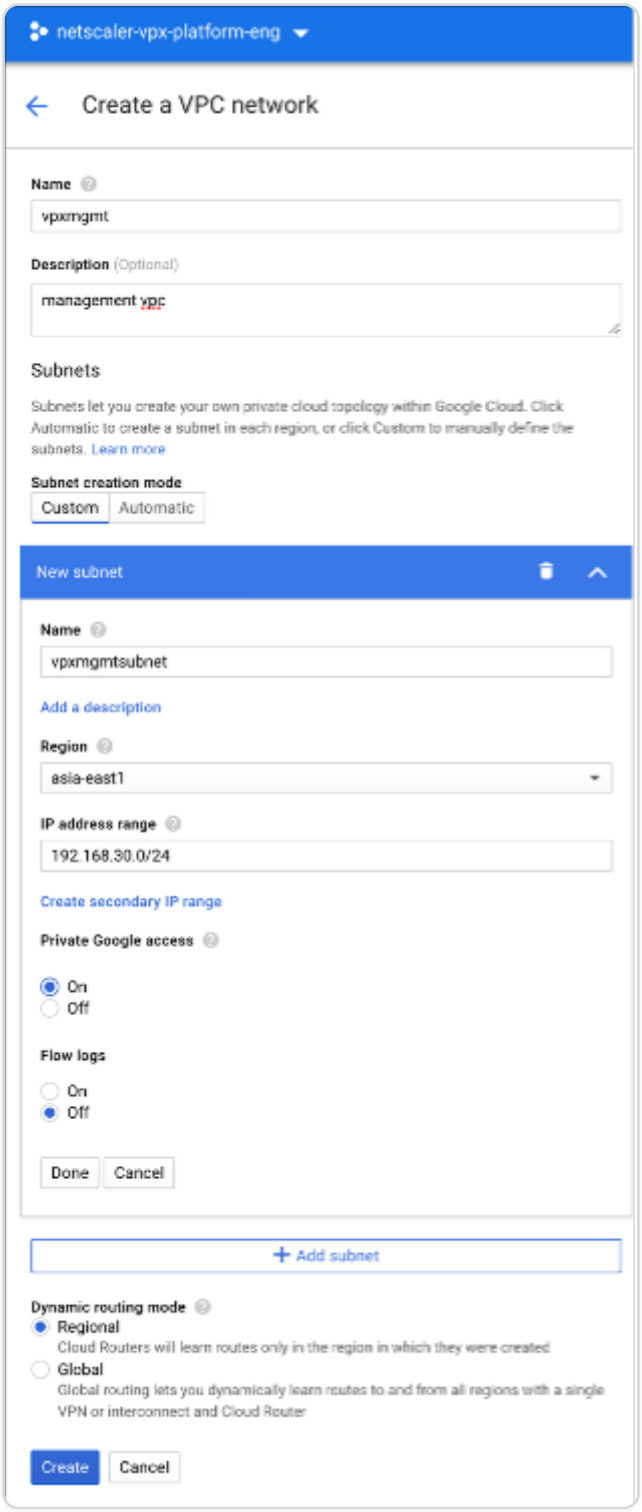
步骤 1. 创建一个 VPC 网络。

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. 登录到 **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**。

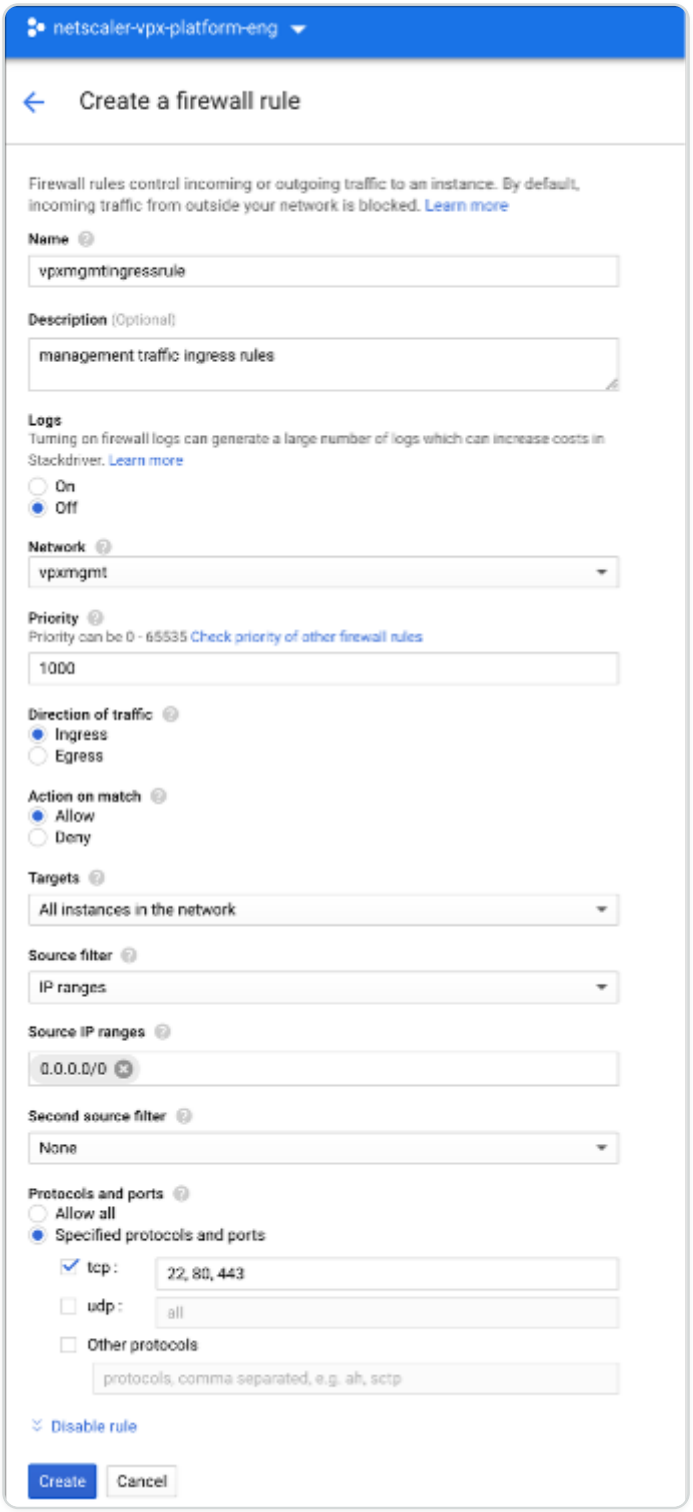
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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。有关防火墙规则的更多信息，请参阅 Firewall Rules Overview。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

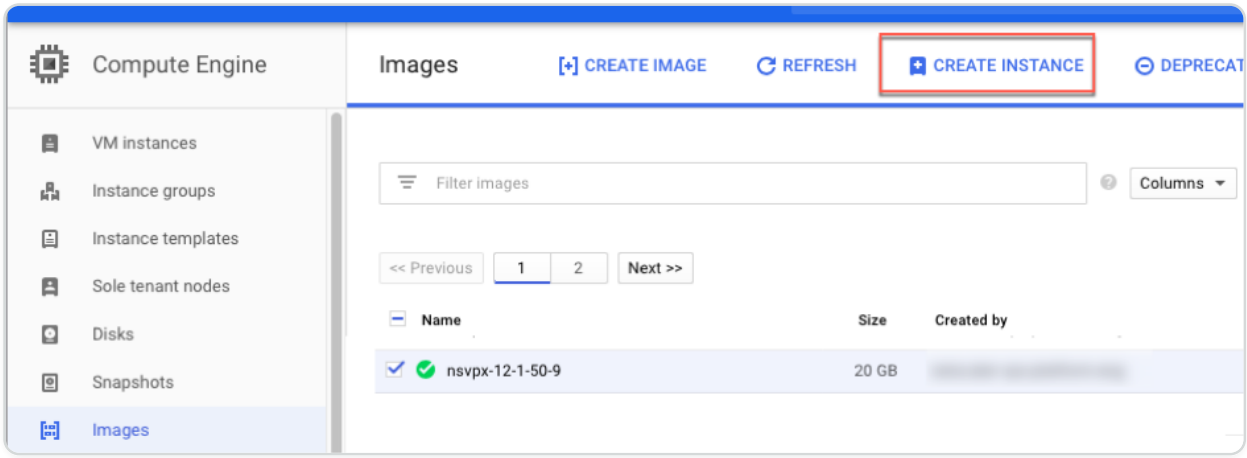


步骤 3. 创建具有单个 NIC 的实例。

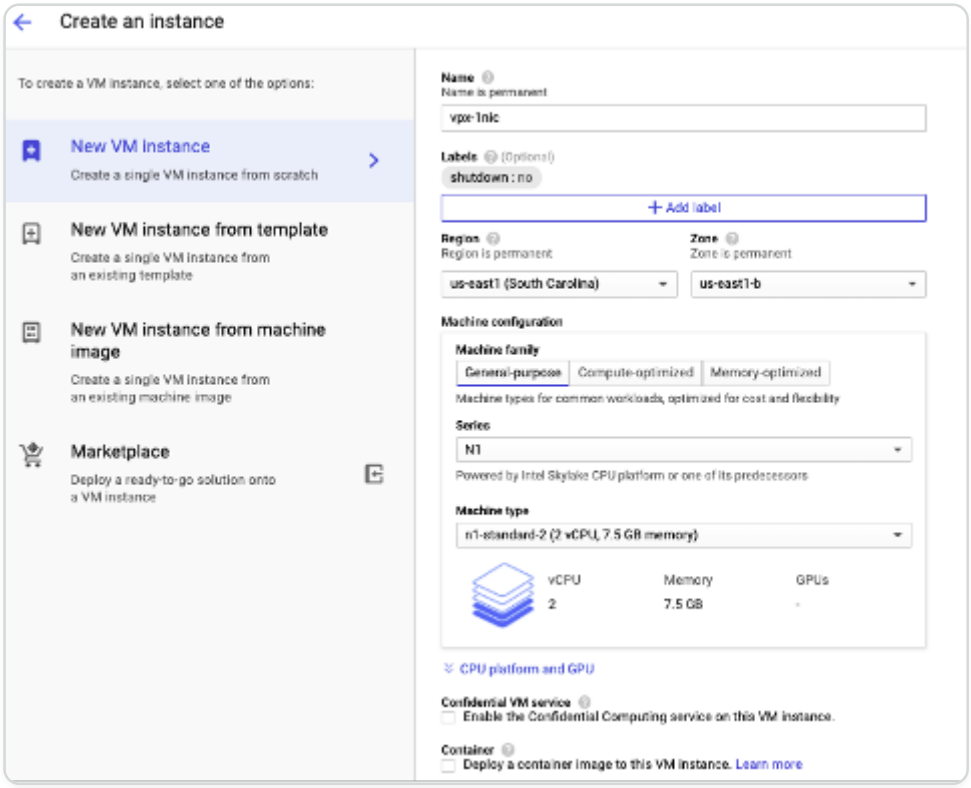
要创建具有单个 NIC 的实例，请执行以下步骤：

1. 登录到 **GCP 控制台**。
2. 在 **Compute** 下，将鼠标悬停在 **Compute Engine** 上，然后选择 **Images**。
3. 选择映像，然后单击 **Create Instance**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 选择具有两个 vCPU 的实例类型（ADC 的最低要求）。



5. 在 **Management, security, disks, networking** 窗口中，单击 **Networking** 选项卡。
6. 在 **Network interfaces** 下，单击 **Edit** 图标以编辑默认 NIC。
7. 在 **Network interfaces** 窗口中，在 **Network** 下，选择您创建的 VPC 网络。
8. 您可以创建静态外部 IP 地址。在 **External IP addresses** 下，单击 **Create IP address**。
9. 在 **Reserve a static address** 窗口中，添加名称和描述，然后单击 **Reserve**。
10. 单击 **Create** 以创建 VPX 实例。 新实例将显示在 VM 实例下。

步骤 4. 将别名 IP 地址添加到 VPX 实例。

为 VPX 实例分配两个别名 IP 地址，用作 VIP 和 SNIP 地址。

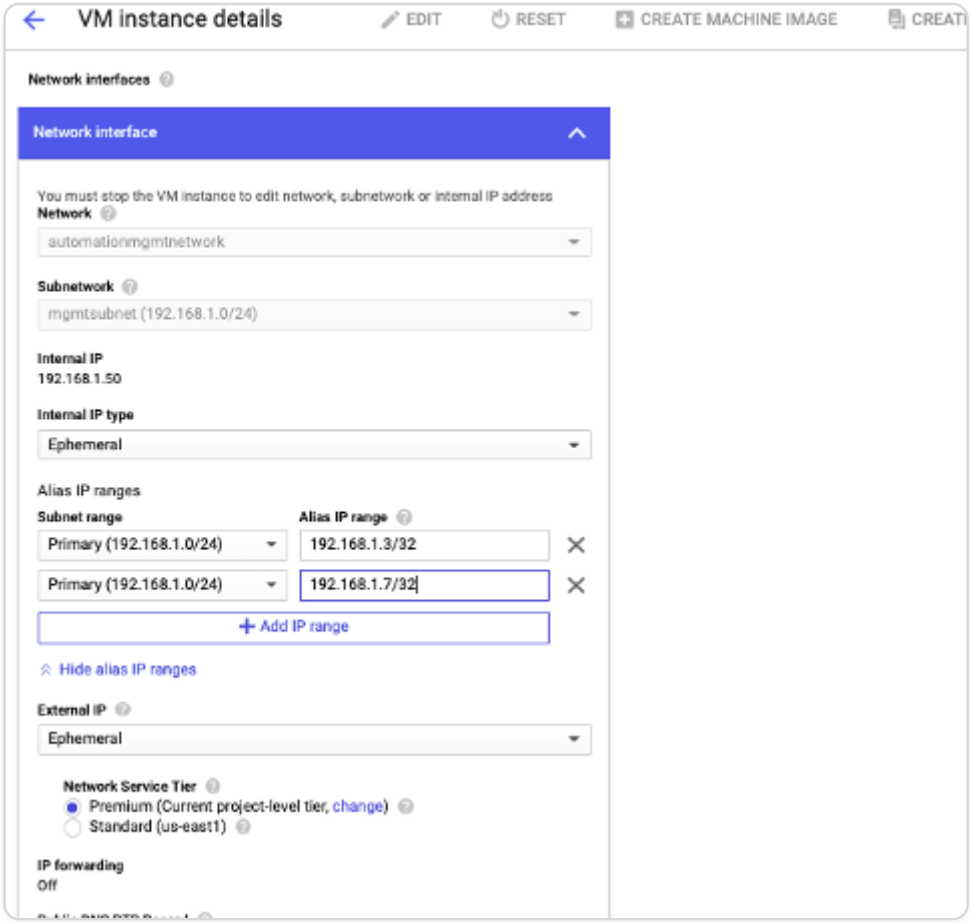
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

请勿使用 VPX 实例的主内部 IP 地址来配置 VIP 或 SNIP。

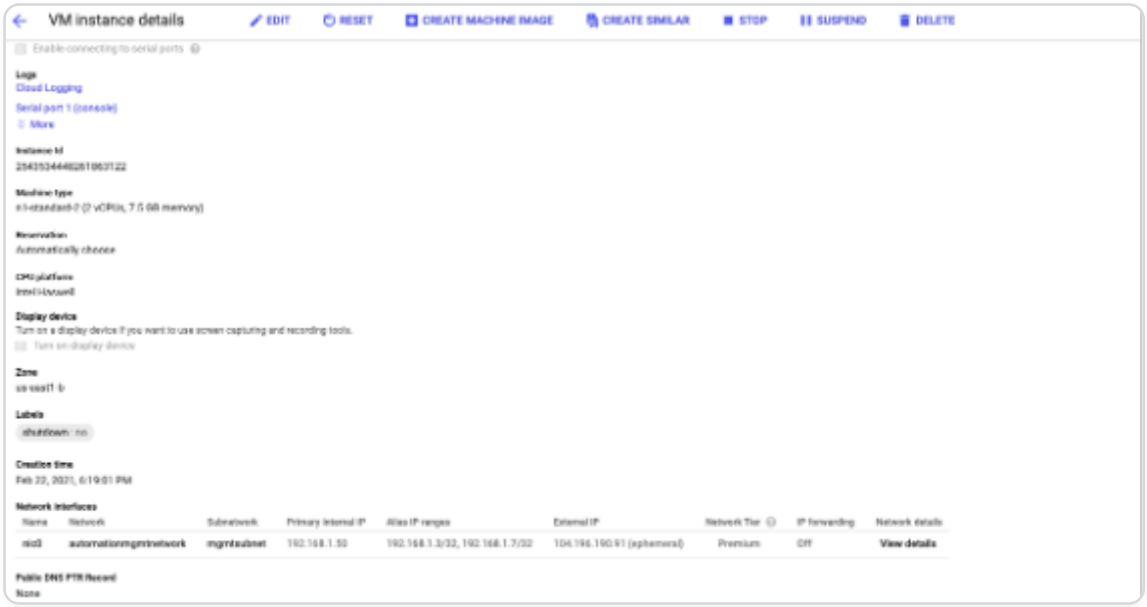
要创建别名 IP 地址，请执行以下步骤：

1. 导航到 VM 实例并单击“**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“**VM 实例详细信息**”页面中验证别名 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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**”。

   添加 IPv4 地址(/en-us/vpx/media/adc-add-ipv4-address.png)

2. 创建客户端别名 IP (VIP) 地址：

   - 输入为 VM 实例中的 VPC 子网配置的客户端别名 IP 地址和子网掩码。
   - 在“**IP 类型**”字段中，从下拉菜单中选择“**虚拟 IP**”。
   - 单击“**创建**”。

3. 创建服务器别名 IP (SNIP) 地址：

   - 输入为 VM 实例中的 VPC 子网配置的服务器别名 IP 地址和子网掩码。
   - 在“**IP 类型**”字段中，从下拉菜单中选择“**子网 IP**”。
   - 单击“**创建**”。

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）和端口的所需值。
3. 单击“**确定**”以创建负载平衡虚拟服务器。

创建负载平衡虚拟服务器(/en-us/vpx/media/create-lb-vserver-adc.png)

步骤 7. 在 VPX 实例上添加服务或服务组。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 在 NetScaler GUI 中，导航到 **配置 > 流量管理 > 负载均衡 > 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 **OK**。

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. 在 GUI 中，导航到 **配置 > 流量管理 > 负载均衡 > 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 **Edit**。
3. 在“**服务和服务器组**”窗口中，单击“**无负载均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 **Bind**。

在 GCP 上部署 VPX 实例后需要注意的事项

- 使用用户名 `nsroot` 和实例 ID 作为密码登录 VPX。在提示符处，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`，而不是常用的 `show techsupport`。
- 从 GCP 控制台删除 NetScaler VM 后，也要删除关联的 NetScaler 内部目标实例。为此，请转到 gcloud CLI 并键入以下命令：

```
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 实例需要有效的许可证。适用于在 GCP 上运行的 NetScaler VPX 实例的许可选项如下：

自带许可证 (BYOL)：要使用 BYOL 选项，请按照以下步骤操作：

- 使用 NetScaler® 网站上的许可门户生成有效许可证。
- 将生成的许可证上传到实例。
- **NetScaler VPX 签入和签出许可证**：此许可模型允许您从可用许可证池中签出许可证，并在不再需要时将其签回。有关更多信息和详细说明，请参阅 NetScaler VPX 签入和签出许可证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

GCP 上的 NetScaler VPX 实例不再支持基于订阅的许可。

GCP 上支持的 NetScaler VPX 产品

下表列出了 GCP 上支持的 NetScaler VPX 产品。

支持的 VPX 产品
NetScaler VPX - 客户许可
NetScaler VPX FIPS - 客户许可

支持的 GCP 机器类型系列

机器类型系列	最低机器类型
通用机器	e2-medium, e2-standard-2, e2-highmem-2, n1-standard-2, n1-highmem-2, n2-standard-2, n2-highmem-2, n2d-standard-2, n2d-highmem-2
计算优化型机器	c2-standard-4, c2d-standard-2, c2d-highmem-2

用于部署 NetScaler VPX 实例的 GDM 模板

您可以使用 NetScaler VPX Google Deployment Manager (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 Marketplace 映像

您可以使用 GDM 模板中的映像来启动 NetScaler 设备。

下表列出了 GCP Marketplace 上可用的映像。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

版本	映像名称	映像位置
13.1	citrix-adc-vpx-精简版-13-1-53-17	projects/citrix-master-project/global/images/citrix-adc-vpx-express-13-1-53-17
13.1	citrix-adc-vpx-200-企业版-13-1-53-17	projects/citrix-master-project/global/images/citrix-adc-vpx-200-enterprise-13-1-53-17
13.1	citrix-adc-vpx-1000-白金版-13-1-53-17	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-platinum-13-1-53-17
13.1	citrix-adc-vpx-5000-白金版-13-1-53-17	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-platinum-13-1-53-17
13.1	citrix-adc-vpx-自带许可-13-1-53-17	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-13-1-53-17

资源

- 创建具有多个网络接口的实例
- 创建并启动虚拟机实例

相关信息

- 在 Google Cloud Platform 上部署 VPX 高可用性对

在 Google Cloud Platform 上部署 VPX 高可用性对

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，另一个配置为辅助节点时，主节点接受连接并管理服务器。辅助节点监控主节点。如果由于任何原因主节点无法接受连接，则辅助节点将接管。

有关 HA 的更多信息，请参阅 高可用性。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

节点必须位于同一区域；但是，它们可以位于同一可用区或不同的可用区。有关更多信息，请参阅区域和可用区。

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® 建议为标准 VPX 实例配置三个网络接口。

您可以通过以下方法部署 VPX 高可用性对：

- 使用外部静态 IP 地址
- 使用私有 IP 地址
- 使用带私有 IP 地址的单网卡虚拟机

用于在 GCP 上部署 VPX 高可用性对的 GDM 模板

您可以使用 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 VPX 高可用性对的转发规则支持

您可以使用转发规则在 GCP 上部署 VPX 高可用性对。

有关转发规则的更多信息，请参阅转发规则概述。

先决条件

- 转发规则必须与 VPX 实例位于同一区域。
- 目标实例必须与 VPX 实例位于同一可用区。
- 主节点和辅助节点的目标实例数量必须匹配。

示例：

您在 `us-east1` 区域有一个高可用性对，其中主 VPX 位于 `us-east1-b` 可用区，辅助 VPX 位于 `us-east1-c` 可用区。为主 VPX 配置了一个转发规则，其目标实例位于 `us-east1-b` 可用区。为辅助 VPX 在 `us-east1-c` 可用区配置一个目标实例，以便在故障转移时更新转发规则。

限制

VPX 高可用性部署仅支持后端配置了目标实例的转发规则。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 Google Cloud Platform 上部署具有外部静态 IP 地址的 VPX 高可用性对

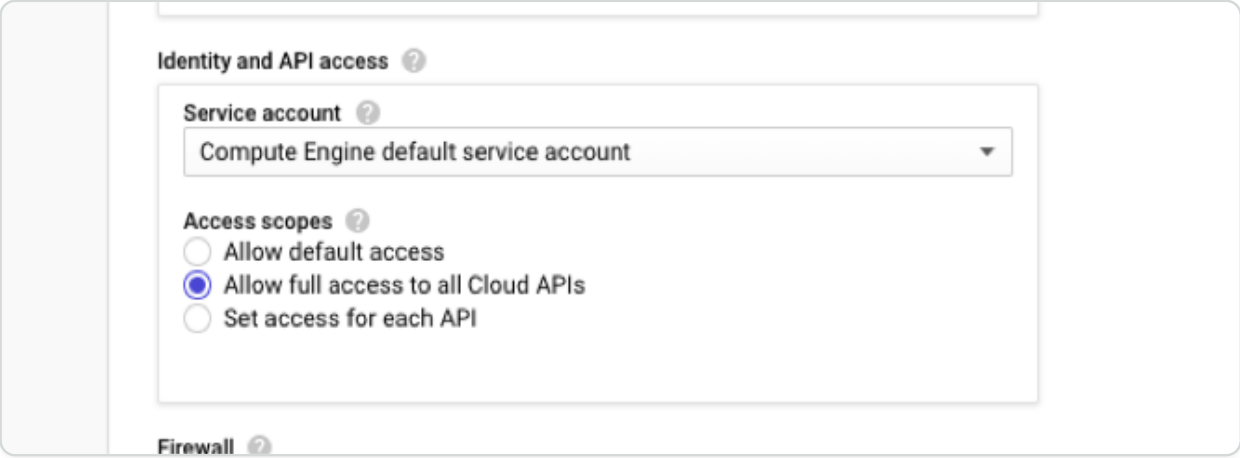
您可以在 GCP 上使用外部静态 IP 地址部署 VPX 高可用性对。主节点的客户端 IP 地址必须绑定到外部静态 IP 地址。发生故障转移时，外部静态 IP 地址将移动到辅助节点，以便流量恢复。

静态外部 IP 地址是为您的项目保留的外部 IP 地址，直到您决定释放它。如果您使用 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它。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

- 阅读在 Google Cloud Platform 上部署 NetScaler VPX 实例 中提及的限制、硬件要求和注意事项。此信息也适用于 HA 部署。
- 为您的 GCP 项目启用 **Cloud Resource Manager API**。
- 在创建实例时允许完全访问所有 Cloud API。



- 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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"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",

]
```

- 如果您在管理接口以外的接口上配置了别名 IP 地址，请确保您的 GCP 服务帐户具有以下附加 IAM 权限：

```
"compute.instances.updateNetworkInterface"
```

- 如果您在主节点上配置了 GCP 转发规则，请阅读GCP 上 VPX 高可用性对的转发规则支持 中提及的限制和要求，以便在故障转移时将其更新到新的主节点。

如何在 Google Cloud Platform 上部署 VPX HA 对

以下是 HA 部署步骤的摘要：

1. 在同一区域创建 VPC 网络。例如，亚洲东部。
2. 在同一区域创建两个 VPX 实例（主节点和辅助节点）。它们可以在同一区域或不同区域。例如，亚洲东部-1a 和亚洲东部-Ib。
3. 通过使用 NetScaler GUI 或 ADC CLI 命令，在两个实例上配置 HA 设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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，分别用于关联管理 NIC、客户端 NIC 和服务器 NIC。

要创建 VPC 网络，请执行以下步骤：

1. 登录 **Google 控制台 > 网络 > VPC 网络 > 创建 VPC 网络**。
2. 填写必填字段，然后单击“**创建**”。

有关详细信息，请参阅 在 Google Cloud Platform 上部署 NetScaler VPX 实例 中的“**创建 VPC 网络**”部分。

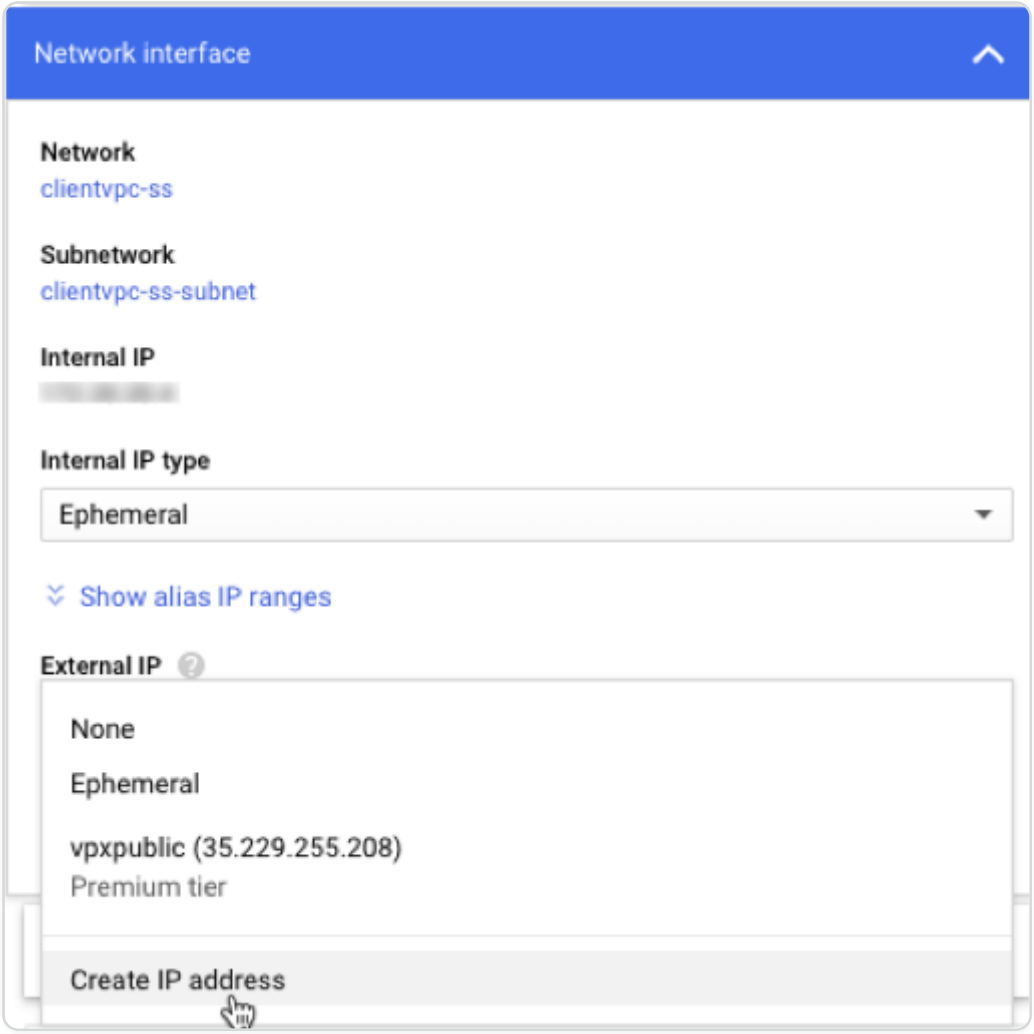
步骤 2. 创建两个 VPX 实例

按照 场景：部署多 NIC、多 IP 独立 VPX 实例 中给出的步骤创建两个 VPX 实例。

重要提示：

将静态外部 IP 地址分配给主节点的客户端 IP 地址 (VIP)。您可以使用现有的保留 IP 地址或创建一个新的。要创建静态外部 IP 地址，请导航到“**网络接口 > 外部 IP**”，然后单击“**创建 IP 地址**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



故障转移后，当旧主节点成为新辅助节点时，静态外部 IP 地址将从旧主节点移动并附加到新主节点。有关详细信息，请参阅 Google Cloud 文档 保留静态外部 IP 地址。

配置 VPX 实例后，您可以配置 VIP 和 SNIP 地址。有关详细信息，请参阅 配置 NetScaler 拥有的 IP 地址。

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 for CLI 配置 HA。

使用 GUI 配置 HA

步骤 1。在两个实例上以 INC 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` 和 GCP 控制台中的节点实例 ID 作为密码登录实例。
2. 导航到 **配置 > 系统 > 高可用性 > 节点**，然后单击 **添加**。
3. 在**远程节点 IP 地址**字段中，输入辅助节点的管理 NIC 的私有 IP 地址。
4. 选中**在自节点上启用 INC（独立网络配置）模式**复选框。

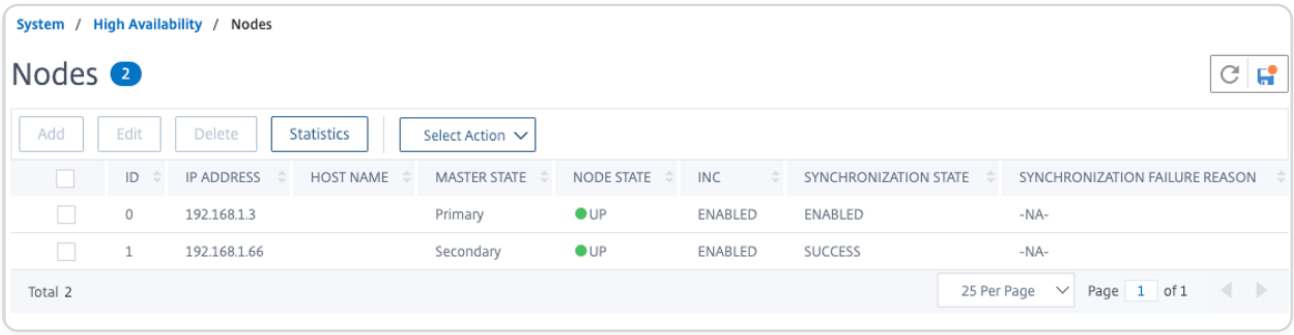
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 单击**创建**。

在**辅助节点**上，执行以下步骤：

1. 使用用户名 `nsroot` 和 GCP 控制台中的节点实例 ID 作为密码登录实例。
2. 导航到 **配置 > 系统 > 高可用性 > 节点**，然后单击 **添加**。
3. 在**远程节点 IP 地址**字段中，输入主节点的管理 NIC 的私有 IP 地址。
4. 选中**在自节点上启用 INC（独立网络配置）模式**复选框。
5. 单击**创建**。

在您继续之前，请确保辅助节点的同步状态在“**节点**”页面中显示为 **SUCCESS**。



注意：

现在，辅助节点具有与主节点相同的登录凭据。

步骤 2。在两个节点上添加虚拟 IP 地址和子网 IP 地址。

在“**主节点**”上，执行以下步骤：

1. 导航到“**系统 > 网络 > IP > IPv4**”，然后单击“**添加**”。
2. 通过执行以下步骤添加主 VIP 地址：
   a. 输入主实例面向客户端接口的内部 IP 地址以及在 VM 实例中为客户端子网配置的子网掩码。
   b. 在“**IP 类型**”字段中，从下拉菜单中选择“**虚拟 IP**”。
   c. 单击“**创建**”。
3. 通过执行以下步骤添加主 SNIP 地址：
   a. 输入主实例面向服务器接口的内部 IP 地址以及在主实例中为服务器子网配置的子网掩码。
   b. 在“**IP 类型**”字段中，从下拉菜单中选择“**子网 IP**”。
   c. 单击“**创建**”。

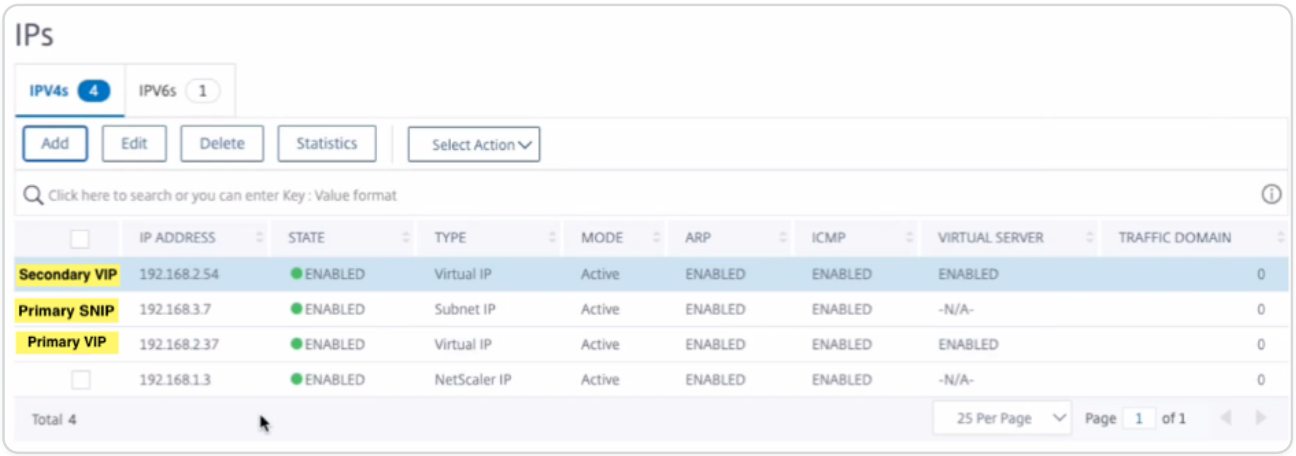
© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 通过以下步骤添加辅助 VIP 地址：

   a. 输入辅助实例面向客户端接口的内部 IP 地址以及在 VM 实例中为客户端子网配置的子网掩码。

   b. 在 **IP 类型**字段中，从下拉菜单中选择 **Virtual IP**。

   c. 单击 **Create**。



在**辅助节点**上，执行以下步骤：

1. 导航到 **System > Network > IPs > IPv4s**，然后单击 **Add**。
2. 通过以下步骤添加辅助 VIP 地址：

   a. 输入辅助实例面向客户端接口的内部 IP 地址以及在 VM 实例中为客户端子网配置的子网掩码。

   b. 在 **IP 类型**字段中，从下拉菜单中选择 **Virtual IP**。

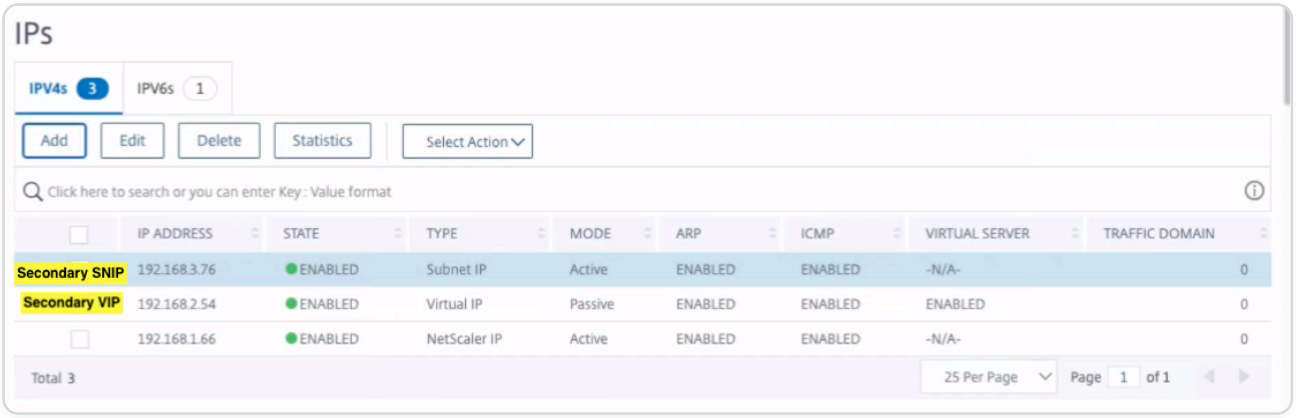
3. 通过以下步骤添加辅助 SNIP 地址：

   a. 输入辅助实例面向服务器接口的内部 IP 地址以及在辅助实例中为服务器子网配置的子网掩码。

   b. 在 **IP 类型**字段中，从下拉菜单中选择 **Subnet IP**。

   c. 单击 **Create**。

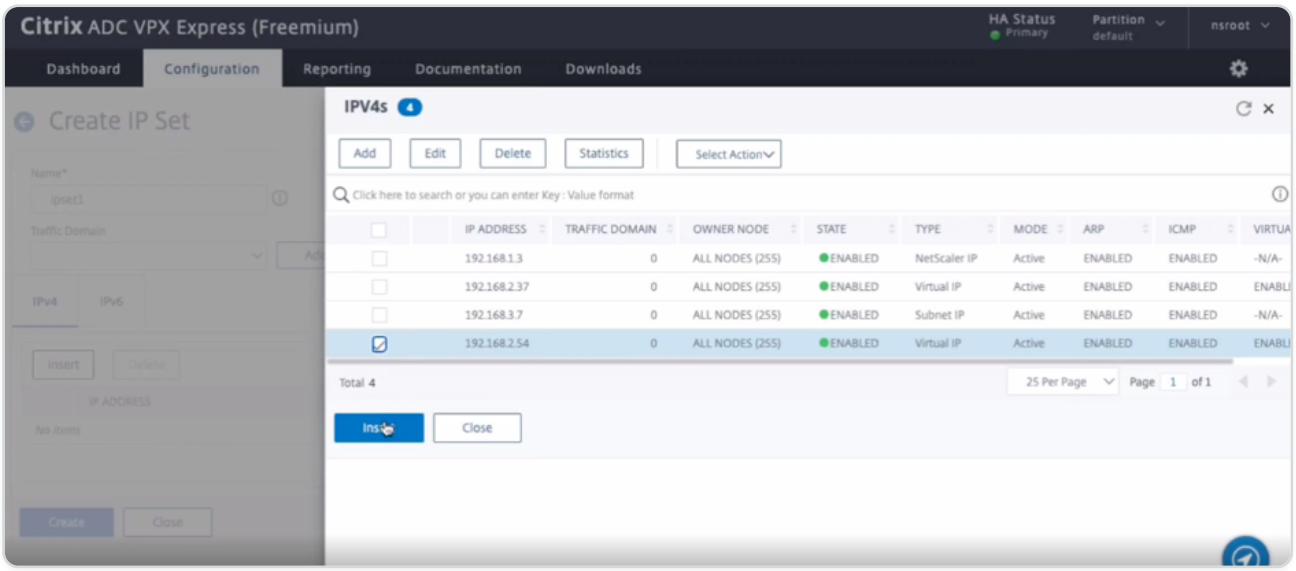
© 1997–2026 Citrix Systems, Inc. All rights reserved.



步骤 3。添加 IP 集并将 IP 集绑定到两个实例上的辅助 VIP。

在**主节点**上，执行以下步骤：

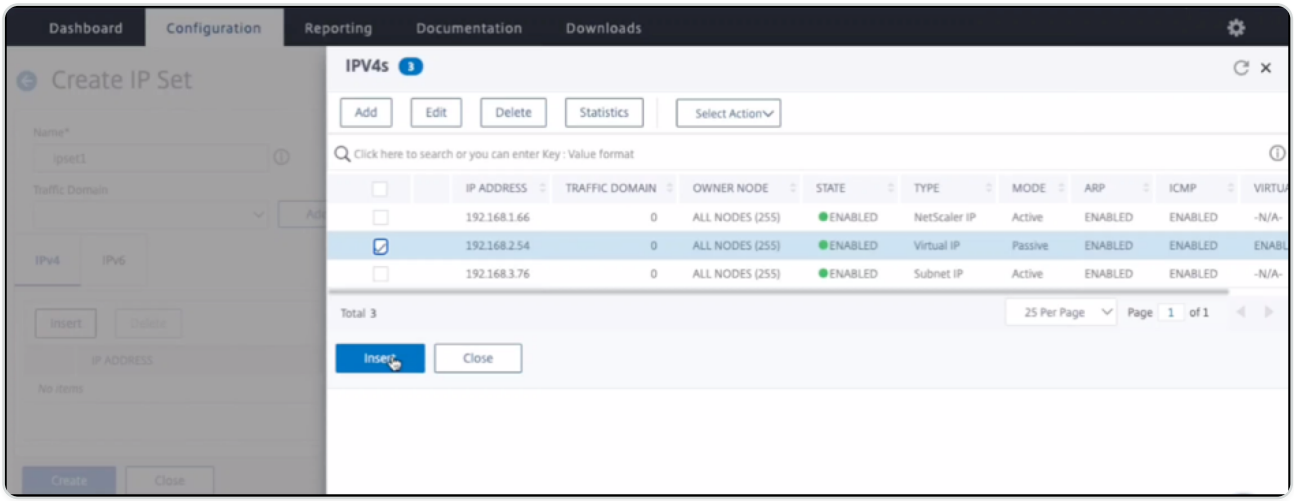
1. 导航到 **系统 > 网络 > IP 集 > 添加**。
2. 添加 IP 集名称，然后单击**插入**。
3. 在 **IPV4s** 页面上，选择虚拟 IP（辅助 VIP），然后单击**插入**。
4. 单击**创建**以创建 IP 集。



在**辅助节点**上，执行以下步骤：

1. 导航到 **系统 > 网络 > IP 集 > 添加**。
2. 添加 IP 集名称，然后单击**插入**。
3. 在 **IPV4s** 页面上，选择虚拟 IP（辅助 VIP），然后单击**插入**。
4. 单击**创建**以创建 IP 集。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

IP 集名称在两个实例上必须相同。

步骤 4。在主实例上添加负载均衡虚拟服务器。

1. 导航到 **配置 > 流量管理 > 负载均衡 > 虚拟服务器 > 添加**。
2. 为名称、协议、IP 地址类型 (IP 地址)、IP 地址 (主 VIP) 和端口添加所需值。

   主实例上的负载均衡虚拟服务器(/en-us/vpx/media/primary-lb-vserver.png)
3. 单击 **更多**。导航到 **IP 范围 IP 集设置**，从下拉菜单中选择 **IPset**，并提供在 **步骤 3** 中创建的 IPset。
4. 单击 **确定** 以创建负载均衡虚拟服务器。

步骤 5。在主节点上添加服务或服务组。

1. 导航到 **配置 > 流量管理 > 负载均衡 > 服务 > 添加**。
2. 为服务名称、IP 地址、协议和端口添加所需值，然后单击 **确定**。

步骤 6。将服务或服务组绑定到主节点上的负载均衡虚拟服务器。

1. 导航到 **配置 > 流量管理 > 负载均衡 > 虚拟服务器**。
2. 选择在 **步骤 4** 中配置的负载均衡虚拟服务器，然后单击 **编辑**。
3. 在 **服务和服务组** 选项卡中，单击 **无负载均衡虚拟服务器服务绑定**。
4. 选择在 **步骤 5** 中配置的服务，然后单击 **绑定**。

保存配置。强制故障转移后，辅助节点将成为新的主节点。旧主 VIP 的外部静态 IP 将移动到新辅助 VIP。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 CLI 配置高可用性

步骤 1。在两个实例中以 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` 指的是辅助节点管理 NIC 的内部 IP 地址。

`prim_ip` 指的是主节点管理 NIC 的内部 IP 地址。

步骤 2。在两个节点上添加虚拟 IP 和子网 IP。

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` 指的是主实例面向客户端的接口的内部 IP 地址。

`secondary_vip` 指的是辅助实例面向客户端的接口的内部 IP 地址。

`primary_snip` 指的是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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add ns ip <secondary_snip> <subnet> -type SNIP
```

`secondary_vip` 指的是辅助实例面向客户端的接口的内部 IP 地址。

`secondary_snip` 指的是辅助实例面向服务器的接口的内部 IP 地址。

步骤 3。在两个实例上添加 IP 集并将 IP 集绑定到辅助 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：

IP 集名称在两个实例上必须相同。

步骤 4。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>
```

步骤 5。在主实例上添加一个服务或服务组。

键入以下命令：

```
add service <service_name> <service_ip_address> <protocol> <port>
```

步骤 6。将服务/服务组绑定到主实例上的负载均衡虚拟服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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，重启实例后配置将丢失。

步骤 7。验证配置。

确保附加到主客户端 NIC 的外部 IP 地址在故障转移时移动到辅助 NIC。

1. 向外部 IP 地址发出 cURL 请求，并确保其可访问。
2. 在主实例上，执行故障转移：

   从 GUI，导航到 **配置 > 系统 > 高可用性 > 操作 > 强制故障转移**。

   从 CLI，键入以下命令：

   ```
   force ha failover -f
   ```

   在 GCP 控制台中，转到辅助实例。外部 IP 地址在故障转移后必须已移动到辅助实例的客户端 NIC。
3. 向外部 IP 发出 cURL 请求，并确保其再次可达。

在 Google Cloud Platform 上部署具有私有 IP 地址的单 NIC VPX 高可用性对

您可以在 GCP 上使用私有 IP 地址部署单 NIC VPX 高可用性对。客户端 IP (VIP) 地址必须在主节点上配置为别名 IP 地址。发生故障转移时，客户端 IP 地址会移动到辅助节点，以便流量恢复。每个节点的子网 IP (SNIP) 地址也必须配置为别名 IP 范围。

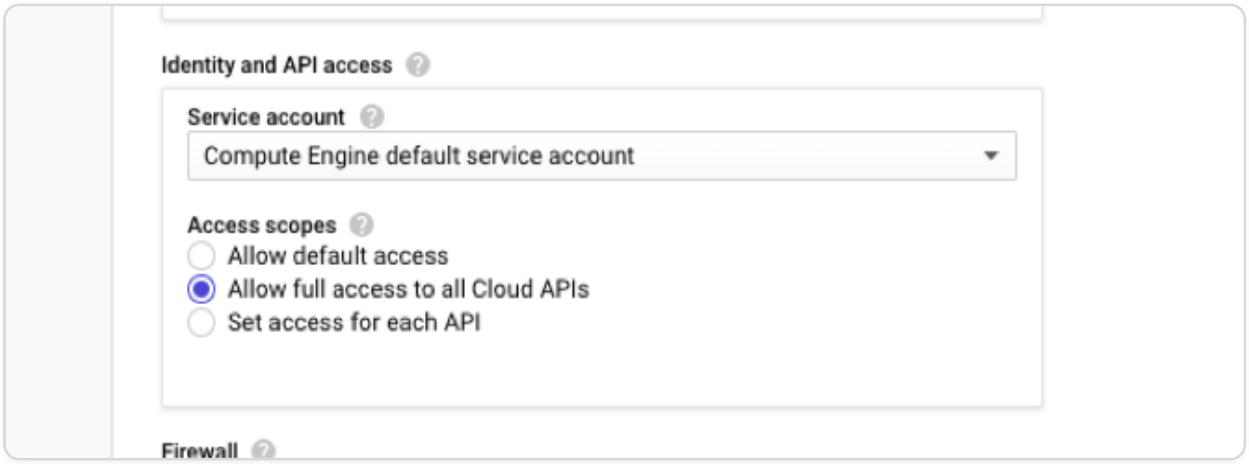
有关高可用性的更多信息，请参阅高可用性。

开始之前

- 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**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在创建实例时，允许完全访问所有 Cloud API。

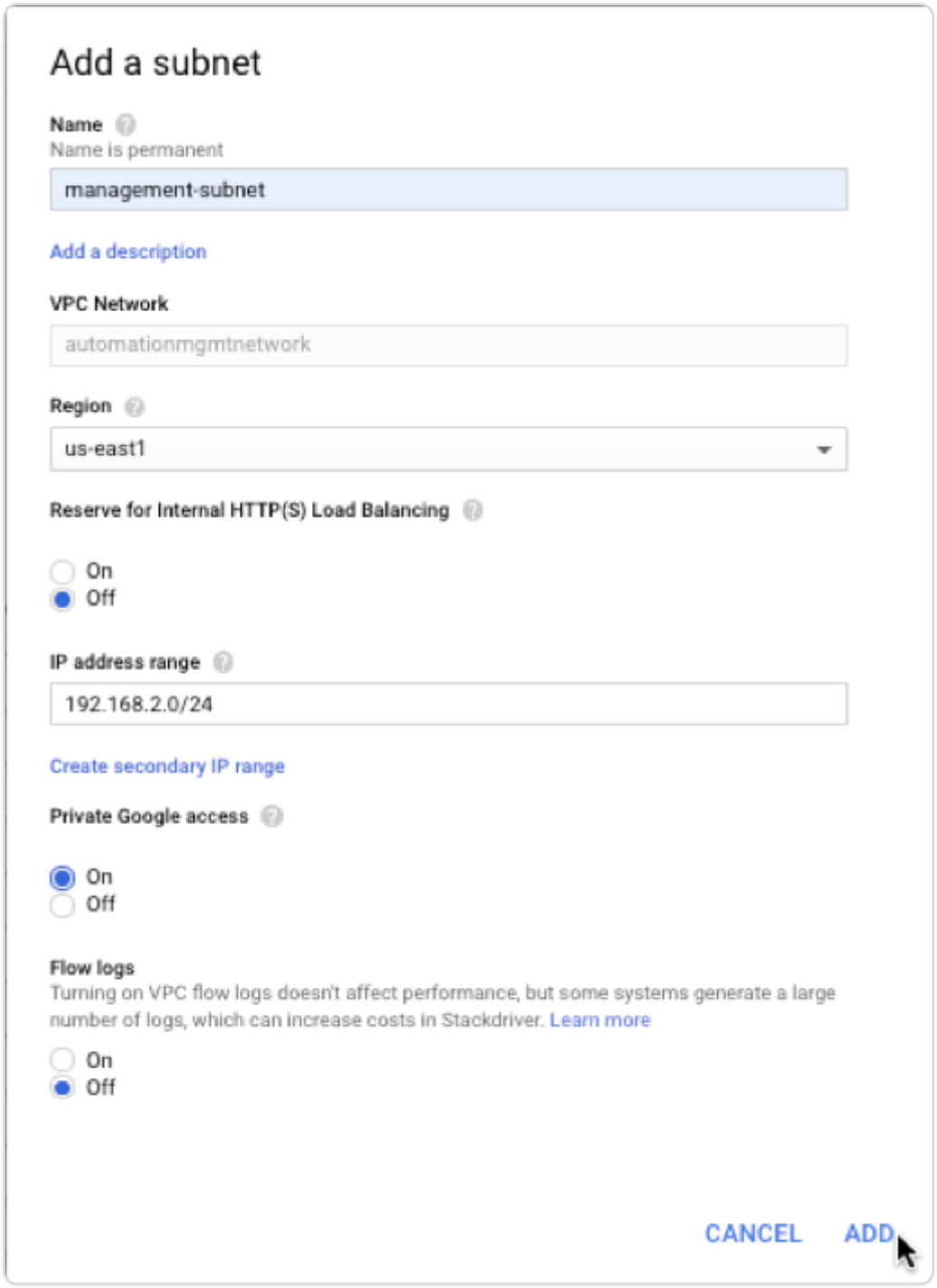


- 确保您的 GCP 服务帐户具有以下 IAM 权限：

```
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 VM 没有互联网访问权限，您必须在 VPC 子网上启用 **Private Google Access**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 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其更新到新的主节点。

如何在 Google Cloud Platform 上部署 VPX 高可用性对

以下是使用单 NIC 部署 HA 对的步骤摘要：

1. 创建一个 VPC 网络。
2. 在同一区域中创建两个 VPX 实例（主节点和辅助节点）。它们可以位于同一区域或不同区域。例如，亚洲东部-1a 和亚洲东部-Ib。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 使用 NetScaler GUI 或 ADC CLI 命令在这两个实例上配置 HA 设置。

步骤 1. 创建 VPC 网络

要创建 VPC 网络，请执行以下步骤：

1. 登录到 **Google 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**。

有关更多信息，请参阅 Deploy a NetScaler VPX instance on Google Cloud Platform 中的 **Create VPC Networks** 部分。

步骤 2. 创建两个 VPX 实例

按照 Scenario: Deploy a single-NIC, standalone VPX instance 中给出的步骤 1 到步骤 3 创建两个 VPX 实例。

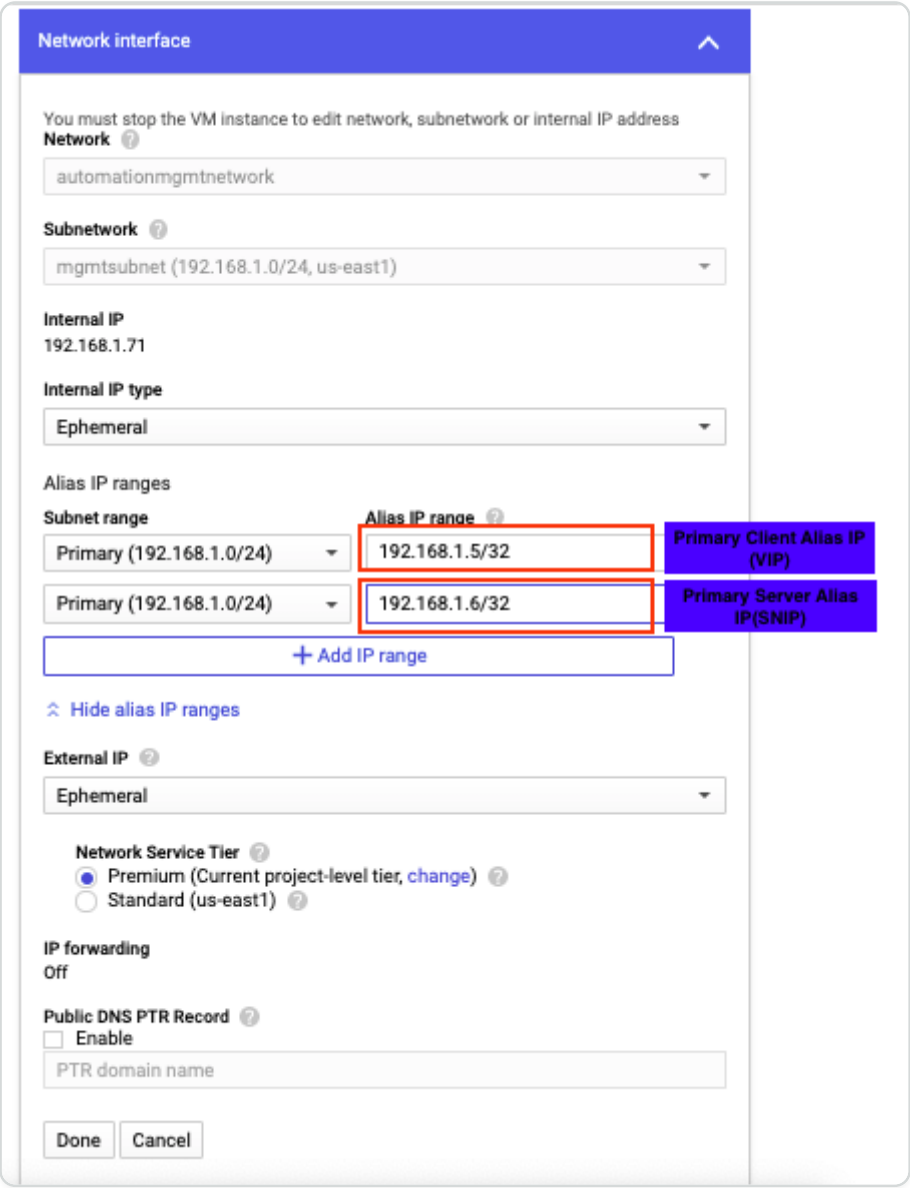
重要提示：

仅将客户端别名 IP 地址分配给主节点，并将服务器别名 IP 地址分配给主节点和辅助节点。请勿使用 VPX 实例的内部 IP 地址配置 VIP 或 SNIP。

要在主节点上创建客户端和服务器别名 IP 地址，请执行以下步骤：

1. 导航到 VM 实例，然后单击 **Edit**。
2. 在 **Network Interface** 窗口中，编辑客户端 (NIC0) 接口。
3. 在 **Alias IP range** 字段中，输入客户端别名 IP 地址。
4. 单击 **Add IP Range**，然后输入服务器别名 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 实例并点击 **编辑**。
2. 在 **网络接口** 窗口中，编辑客户端 (NIC0) 接口。
3. 在 **别名 IP 范围** 字段中，输入服务器别名 IP 地址。

单 NIC 辅助 SNIP(/en-us/vpx/media/gcp-single-nic-secondary-snip.png)

故障转移后，当旧主节点成为新辅助节点时，客户端别名 IP 地址将从旧主节点移至新主节点并附加到新主节点。

配置 VPX 实例后，您可以配置虚拟 (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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

步骤 1。在两个节点上以 INC Enabled 模式设置高可用性。

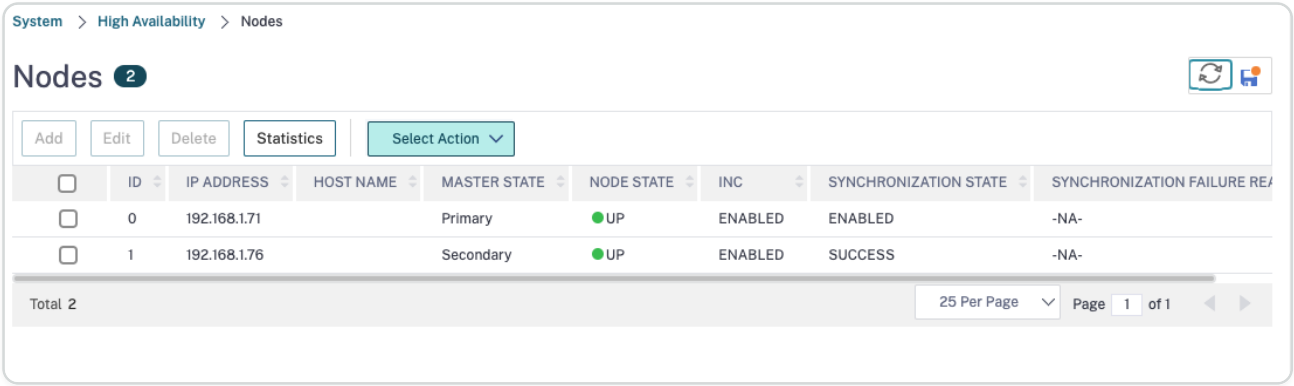
在**主节点**上，执行以下步骤：

1. 使用用户名 `nsroot` 和 GCP 控制台中的节点实例 ID 作为密码登录实例。
2. 导航到 **配置 > 系统 > 高可用性 > 节点**，然后点击 **添加**。
3. 在 **Remote Node IP address** 字段中，输入辅助节点的管理 NIC 的私有 IP 地址。
4. 选中 **在自节点上启用 INC（独立网络配置）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` 登录实例，并使用 GCP 控制台中的节点实例 ID 作为密码。
2. 导航到 **配置 > 系统 > 高可用性 > 节点**，然后单击 **添加**。
3. 在 **远程节点 IP 地址** 字段中，输入主节点管理 NIC 的私有 IP 地址。
4. 选中 **在自节点上启用 INC（独立网络配置）模式** 复选框。
5. 单击 **创建**。

在继续之前，请确保辅助节点的同步状态在 **节点** 页面中显示为 **成功**。



注意：

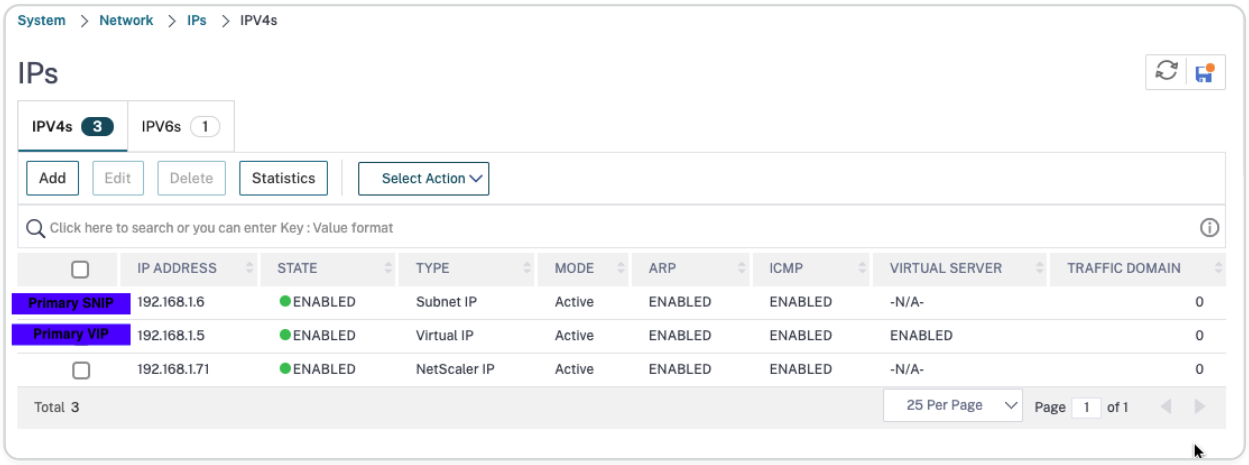
辅助节点与主节点同步后，辅助节点将具有与主节点相同的登录凭据。

步骤 2。在两个节点上添加虚拟 IP 地址和子网 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在主节点上，执行以下步骤：

1. 导航到 **系统 > 网络 > IP > IPv4**，然后单击 **添加**。
2. 要创建客户端别名 IP (VIP) 地址：
   a. 输入为主 VM 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 类型**”字段中，从下拉菜单中选择“**虚拟 IP**”。
   c. 单击“**创建**”。
3. 要创建服务器别名 IP (SNIP) 地址：
   a. 输入为主 VM 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 类型**”字段中，从下拉菜单中选择“**子网 IP**”。
   c. 单击“**创建**”。



在辅助节点上，执行以下步骤：

1. 导航到“**系统 > 网络 > IP > IPv4**”，然后单击“**添加**”。
2. 要创建客户端别名 IP (VIP) 地址：
   a. 输入为主 VM 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 类型**”字段中，从下拉菜单中选择“**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 VM 实例的 VPC 子网配置的服务器别名 IP 地址和子网掩码。
   b. 在 **IP 类型**字段中，从下拉菜单中选择**子网 IP**。
   c. 单击**创建**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

创建辅助客户端和服务器 IP 地址(/en-us/vpx/media/gcp-single-nic-create-ipv4-address-secondary.png)

步骤 3。在主节点上添加负载平衡虚拟服务器。

1. 导航到**配置 > 流量管理 > 负载平衡 > 虚拟服务器 > 添加**。
2. 添加名称、协议、IP 地址类型（IP 地址）、IP 地址（主客户端别名 IP 地址）和端口的所需值，然后单击**确定**。

   LB 虚拟服务器客户端别名(/en-us/vpx/media/gcp-single-nic-lb-vserver-client-alias.png)

步骤 4。在主节点上添加服务或服务组。

1. 导航到**配置 > 流量管理 > 负载平衡 > 服务 > 添加**。
2. 添加服务名称、IP 地址、协议和端口的所需值，然后单击**确定**。

步骤 5。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**配置 > 流量管理 > 负载平衡 > 虚拟服务器**。
2. 选择在**步骤 3**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**”选项卡中，单击“**无负载平衡虚拟服务器服务绑定**”。
4. 选择在“**步骤 4**”中配置的服务，然后单击“**绑定**”。

“**步骤 6**。” 保存配置。

强制故障转移后，辅助节点成为新的主节点。旧主节点上的客户端别名 IP (VIP) 将移动到新主节点。

使用 CLI 配置高可用性

“**步骤 1**。” 使用 NetScaler CLI 在两个实例中以“**INC Enabled**”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` 指的是辅助节点的管理 NIC 的内部 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`prim_ip` 指的是主节点的管理 NIC 的内部 IP 地址。

“**步骤 2**。” 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：

”。

输入在 VM 实例中为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 VM 实例中的客户端子网配置的别名 IP 地址和子网掩码。

```
add ns ip <secondary_server_alias_ip> <subnet> -type SNIP
```

注意：

输入为 VM 实例中的服务器子网配置的别名 IP 地址和子网掩码。

步骤 3。在主节点上添加虚拟服务器。

键入以下命令：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add <server_type> vserver <vserver_name> <protocol>
<primary_client_alias_ip> <port>
```

步骤 4。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>
```

步骤 5。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，重新启动实例后，配置将丢失。

在 Google Cloud Platform 上部署具有私有 IP 地址的 VPX 高可用性对

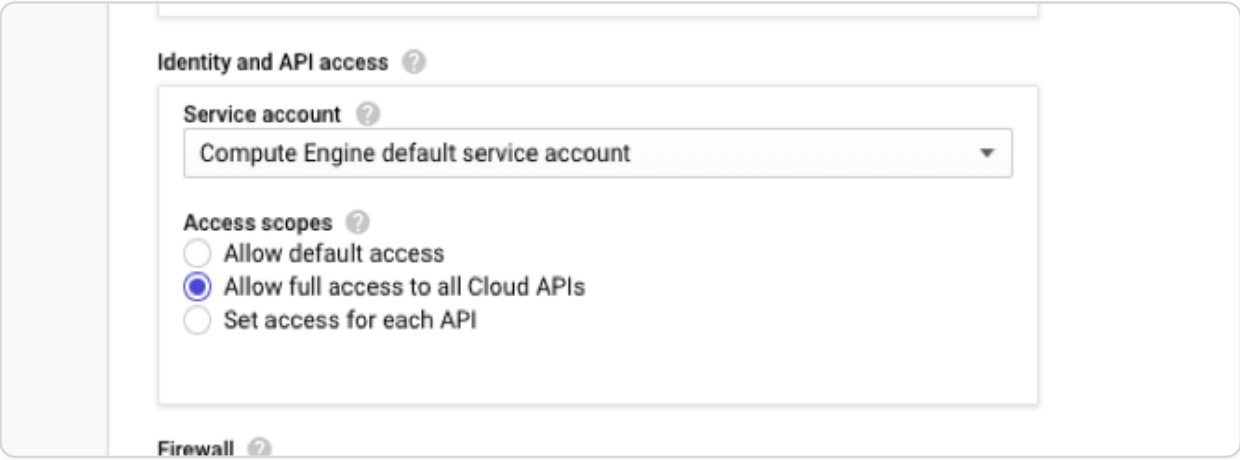
您可以在 GCP 上使用私有 IP 地址部署 VPX 高可用性对。客户端 IP (VIP) 必须在主节点上配置为别名 IP 地址。发生故障转移时，客户端 IP 地址会移动到辅助节点，以便流量恢复。

有关高可用性的更多信息，请参阅 高可用性。

开始之前

- 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，允许完全访问所有 Cloud API。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 确保您的 GCP 服务帐户具有以下 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",

]
```

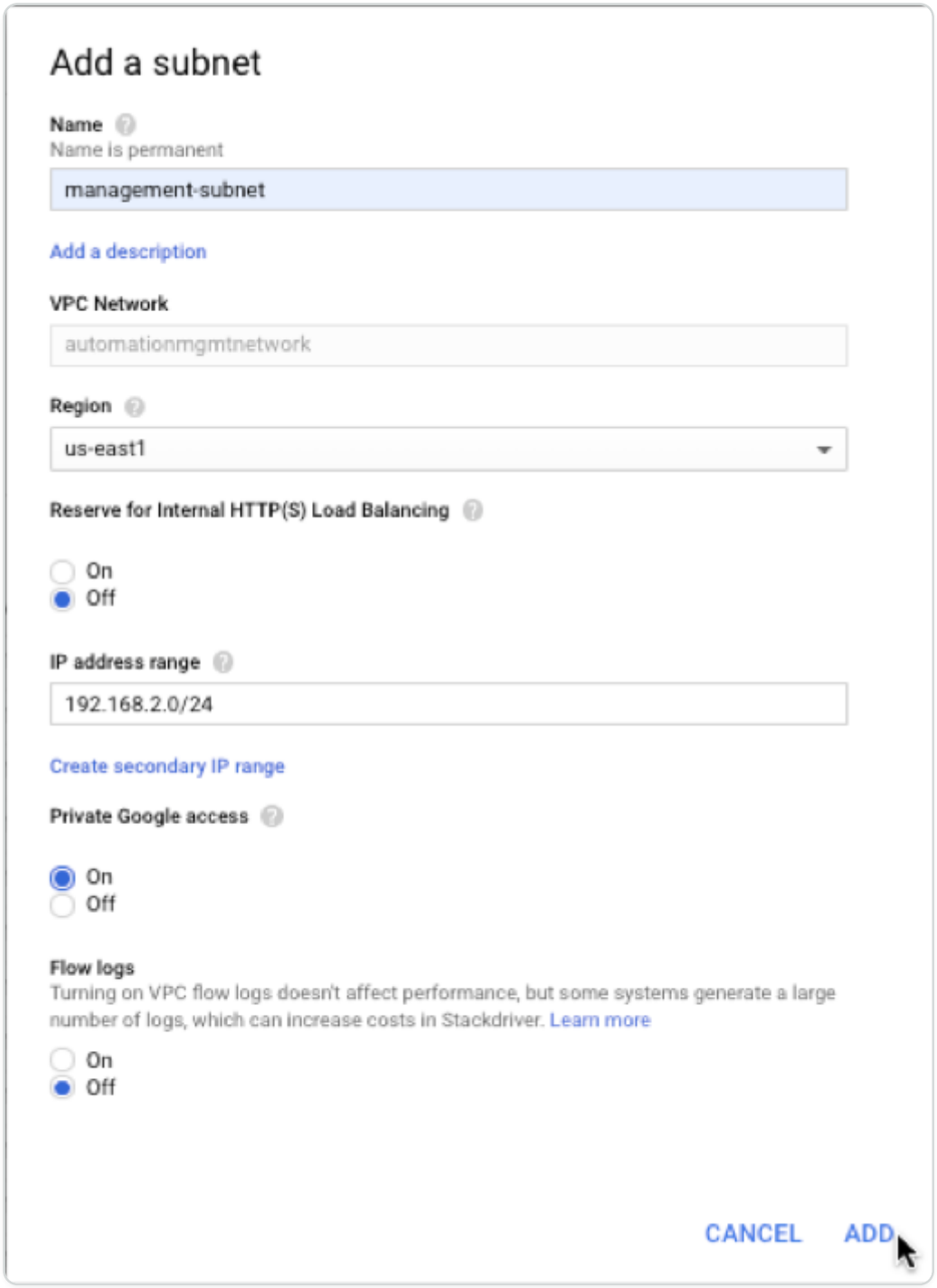
- 如果您在管理接口以外的接口上配置了外部 IP 地址，请确保您的 GCP 服务帐户具有以下附加 IAM 权限：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
REQUIRED_INSTANCE_IAM_PERMS = [

"compute.addresses.use"

"compute.instances.addAccessConfig",

"compute.instances.deleteAccessConfig",

"compute.networks.useExternalIp",

"compute.subnetworks.useExternalIp",

]
```

- 如果您的 VM 没有互联网访问权限，则必须在管理子网上启用 **Private Google Access**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 如果您在主节点上配置了 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其更新到新的主节点。

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. 在同一区域创建 VPC 网络。例如，亚洲东部。
2. 在同一区域创建两个 VPX 实例（主节点和辅助节点）。它们可以位于同一区域或不同区域。例如，亚洲东部-1a 和亚洲东部-Ib。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. 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，分别用于关联管理 NIC、客户端 NIC 和服务器 NIC。

要创建 VPC 网络，请执行以下步骤：

1. 登录 **Google 控制台 > 网络 > VPC 网络 > 创建 VPC 网络**。
2. 填写必填字段，然后单击 **创建**。

有关详细信息，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. 创建两个 VPX 实例

按照 场景：部署多 NIC、多 IP 独立 VPX 实例 中给出的步骤创建两个 VPX 实例。

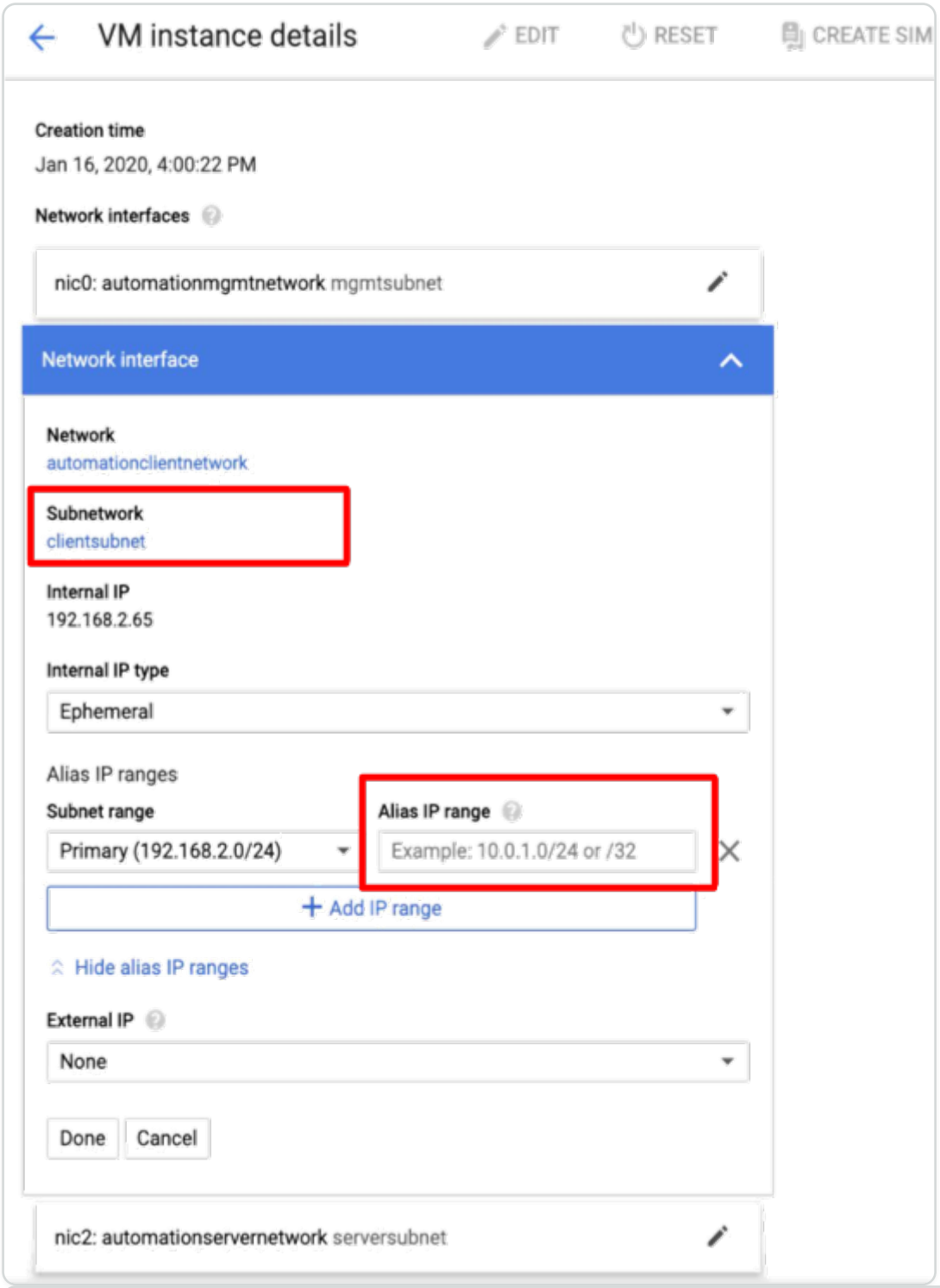
重要：

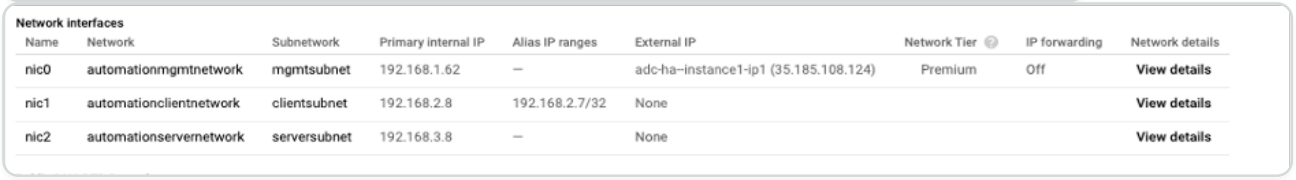
将客户端别名 IP 地址分配给主节点。请勿使用 VPX 实例的内部 IP 地址配置 VIP。

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“**网络接口**”窗口中，编辑客户端接口。
3. 在“**别名 IP 范围**”字段中，输入客户端别名 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.





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

故障转移后，当旧的主节点成为新的辅助节点时，别名 IP 地址会从旧的主节点移动并附加到新的主节点。

配置 VPX 实例后，您可以配置虚拟 IP (VIP) 和子网 IP (SNIP) 地址。有关详细信息，请参阅配置 NetScaler 拥有的 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

步骤 1. 在两个节点上以 INC 启用模式设置高可用性。

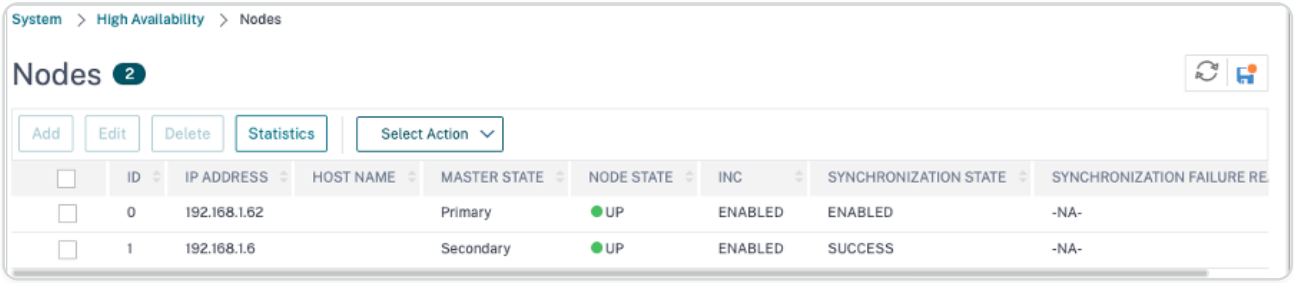
在**主节点**上，执行以下步骤：

1. 使用用户名 `nsroot` 并使用 GCP 控制台中的节点实例 ID 作为密码登录实例。
2. 导航到**配置 > 系统 > 高可用性 > 节点**，然后单击**添加**。
3. 在**远程节点 IP 地址**字段中，输入辅助节点的管理 NIC 的私有 IP 地址。
4. 选中**在自节点上启用 INC（独立网络配置）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` 登录实例，并使用 GCP 控制台中的节点实例 ID 作为密码。
2. 导航到 **配置 > 系统 > 高可用性 > 节点**，然后单击 **添加**。
3. 在 **Remote Node IP address** 字段中，输入主节点管理 NIC 的私有 IP 地址。
4. 选中 **在自节点上启用 INC（独立网络配置）模式** 复选框。
5. 单击 **Create**。

在继续之前，请确保辅助节点的同步状态在 **Nodes** 页面中显示为 **SUCCESS**。



注意：

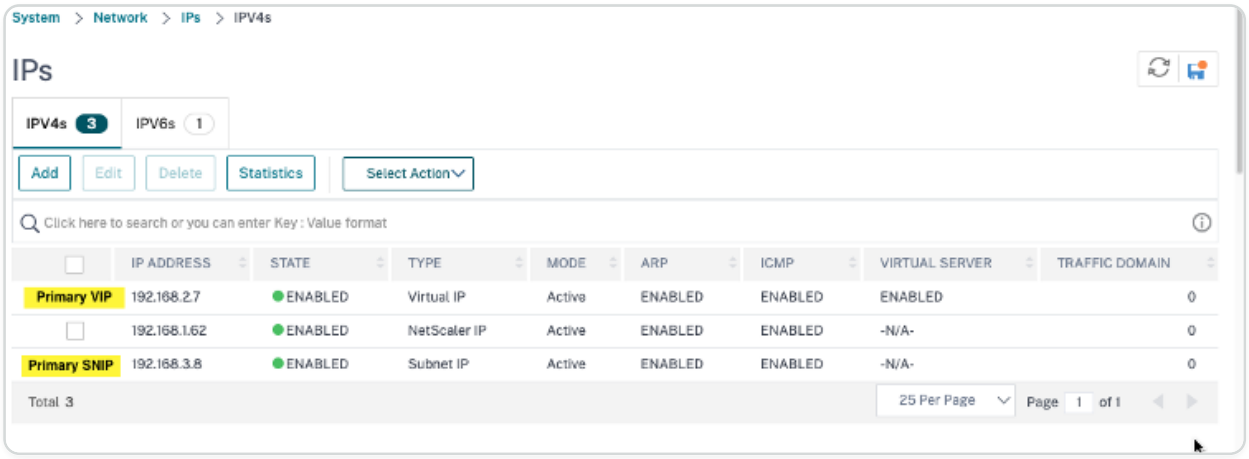
辅助节点与主节点同步后，辅助节点将具有与主节点相同的登录凭据。

步骤 2。在两个节点上添加虚拟 IP 地址和子网 IP 地址。

在主节点上，执行以下步骤：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

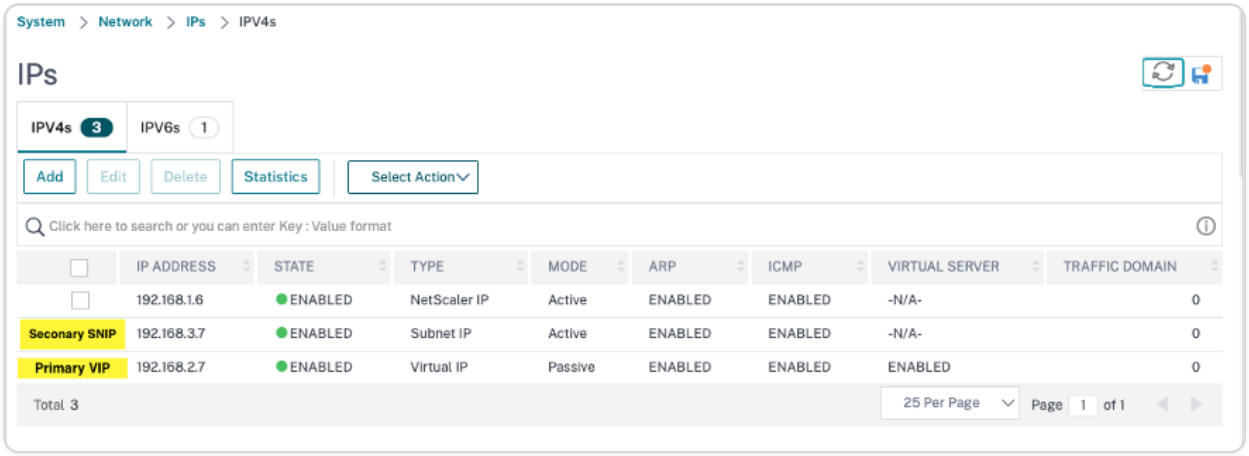
1. 导航到 **System > Network > IPs > IPv4s**，然后单击 **Add**。
2. 要创建客户端别名 IP (VIP) 地址：
   a. 输入在 VM 实例中为客户端子网配置的别名 IP 地址和网络掩码。
   b. 在 **IP Type** 字段中，从下拉菜单中选择 **Virtual IP**。
   c. 点击**创建**。
3. 要创建服务器 IP (SNIP) 地址：
   a. 输入主实例面向服务器的接口的内部 IP 地址以及为服务器子网配置的子网掩码。
   b. 在**IP 类型**字段中，从下拉菜单中选择**子网 IP**。
   c. 点击**创建**。



在辅助节点上，执行以下步骤：

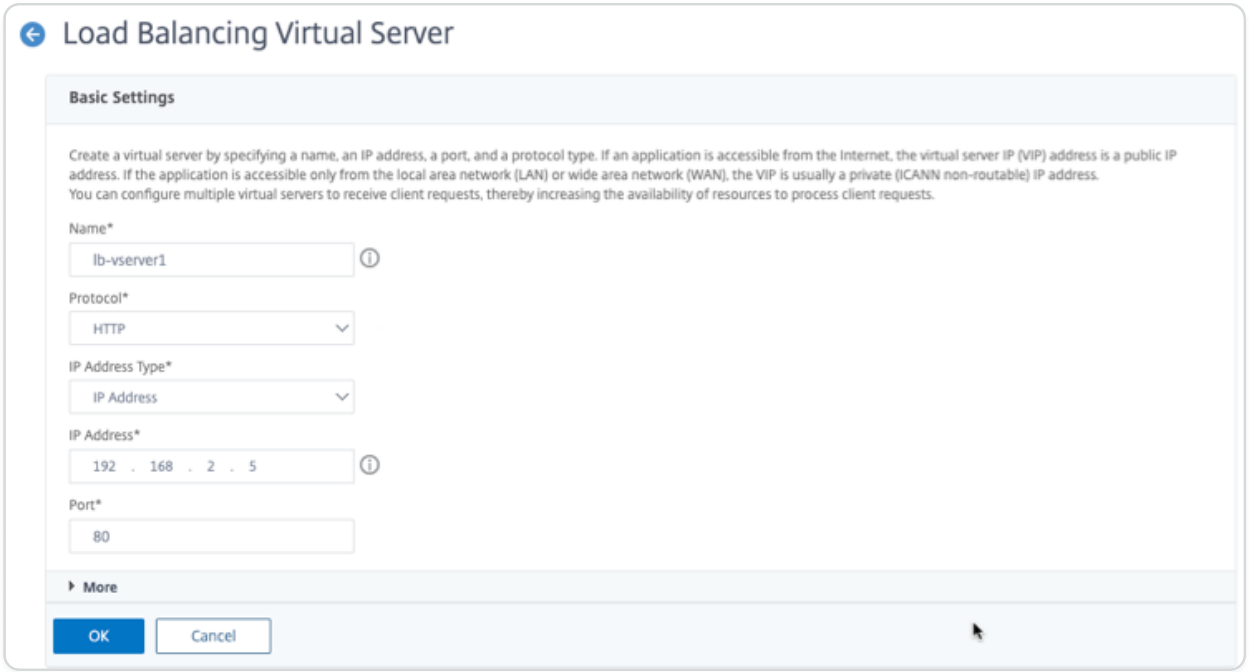
1. 导航到**系统 > 网络 > IP > IPv4**，然后点击**添加**。
2. 要创建客户端别名 IP (VIP) 地址：
   a. 输入在主 VM 实例上为客户端子网配置的别名 IP 地址和子网掩码。
   b. 在**IP 类型**字段中，从下拉菜单中选择**子网 IP**。
   c. 点击**创建**。
3. 要创建服务器 IP (SNIP) 地址：
   a. 输入辅助实例面向服务器的接口的内部 IP 地址以及为服务器子网配置的子网掩码。
   b. 在**IP 类型**字段中，从下拉菜单中选择**子网 IP**。
   c. 单击 **创建**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



步骤 3。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. 添加名称、协议、IP 地址类型（IP 地址）、IP 地址（主客户端别名 IP 地址）和端口的所需值，然后单击 **确定**。



步骤 4。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. 添加服务名称、IP 地址、协议和端口的所需值，然后单击 **确定**。

步骤 5。将服务或服务组绑定到主节点上的负载平衡虚拟服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 **步骤 3** 中配置的负载平衡虚拟服务器，然后单击 **编辑**。
3. 在 **服务和服务器组** 选项卡中，单击 **无负载平衡虚拟服务器服务绑定**。
4. 选择在 **步骤 4** 中配置的服务，然后单击 **绑定**。

步骤 5。保存配置。

强制故障转移后，辅助节点成为新的主节点。旧主节点上的客户端别名 IP (VIP) 和服务器别名 IP (SNIP) 将移动到新主节点。

使用 CLI 配置高可用性

步骤 1。使用 NetScaler CLI 在两个实例中以 **INC Enabled** 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` 指的是辅助节点的管理网卡 (NIC) 的内部 IP 地址。

`prim_ip` 指的是主节点的管理网卡 (NIC) 的内部 IP 地址。

步骤 2。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：

输入为 VM 实例中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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`primary_snip` 指的是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 VM 实例上客户端子网配置的别名 IP 地址和子网掩码。

```
add ns ip <secondary_snip> <subnet> -type SNIP
```

的 `secondary_snip` 指的是辅助实例面向服务器接口的内部 IP 地址。

注意：

输入为 VM 实例中的服务器子网配置的 IP 地址和子网掩码。

步骤 3。在主节点上添加一个虚拟服务器。

键入以下命令：

```
add <server_type> vserver <vserver_name> <protocol>
<primary_client_alias_ip> <port>
```

步骤 4。在主节点上添加一个服务或服务组。

键入以下命令：

```
add service <service_name> <service_ip_address> <protocol> <port>
```

步骤 5。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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

要保存配置，请键入命令 `save config`。否则，重新启动实例后配置将丢失。

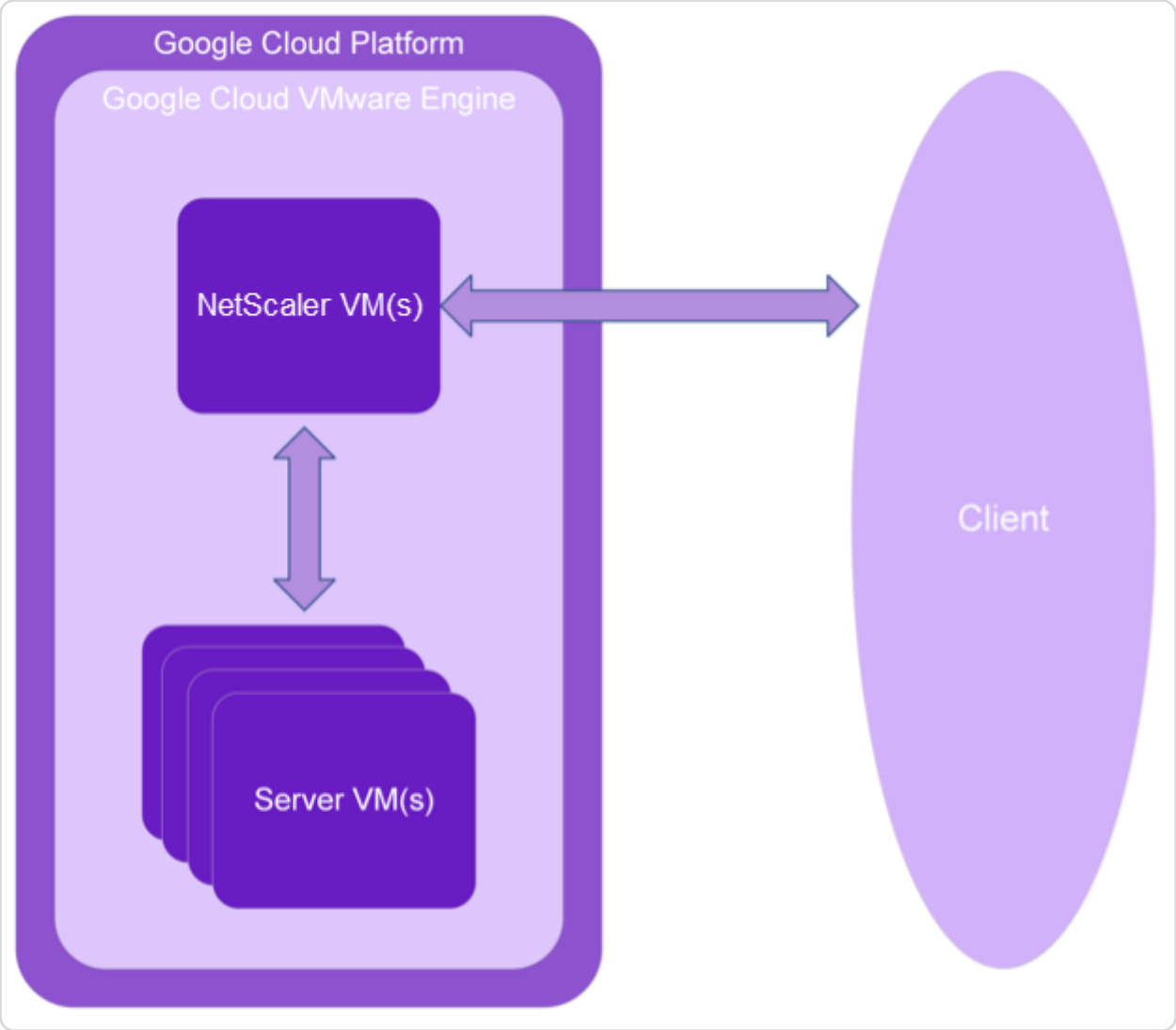
在 Google Cloud VMware Engine 上安装 NetScaler VPX 实例

Google Cloud VMware Engine (GCVE) 为您提供包含 vSphere 群集的私有云，这些群集基于专用的裸机 Google Cloud Platform 基础架构构建。最低初始部署为三个主机，但可以一次添加一个额外主机。所有已预置的私有云都具有 vCenter Server、vSAN、vSphere 和 NSX-T。

GCVE 使您能够在 Google Cloud Platform 上创建具有所需数量 ESX 主机的云软件定义数据中心 (SDDC)。GCVE 支持 NetScaler VPX 部署。GCVE 提供的用户界面与本地 vCenter 相同。它的功能与基于 ESX 的 NetScaler VPX 部署完全相同。

下图显示了 Google Cloud Platform 上的 GCVE，管理员或客户端可以通过互联网访问。管理员可以使用 GCVE 创建、管理和配置工作负载或服务器 VM。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 VM，并使用 NSX-T Manager 管理相应的网络。GCVE 上的 NetScaler VPX 实例的工作方式与本地 VMware 主机群集类似。可以使用 OpenVPN 连接到管理基础架构来管理 GCVE。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



先决条件

在开始安装虚拟设备之前，请执行以下操作：

- 有关 Google Cloud VMware Engine 及其先决条件的更多信息，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。
- 有关使用点到站点 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 VMware SDDC 上创建虚拟机连接到的相应 NSX-T 网络段。有关更多信息，请参阅 在 Google Cloud VMware Engine 中添加网络段。
- 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) 必须连接到网络段。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. 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：

这不包括管理程序的任何磁盘要求。

对于 VPX 虚拟设备的生产用途，必须保留全部内存分配。

OVF Tool 1.0 系统要求

OVF Tool 是一款可在 Windows 和 Linux 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. OVF 工具安装的最低系统要求

组件	要求
操作系统	有关 VMware 的详细要求，请在 `<http://kb.vmware.com/>` 处搜索“OVF Tool 用户指南”PDF 文件。
CPU	最低 750 MHz，推荐 1 GHz 或更快
RAM	最低 1 GB，推荐 2 GB
网卡	100 Mbps 或更快的网卡

© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关安装 OVF 的信息，请在 `<http://kb.vmware.com/>` 处搜索“OVF Tool 用户指南”PDF 文件。

下载 NetScaler VPX 安装文件

适用于 VMware ESX 的 NetScaler VPX 实例安装包遵循开放式虚拟机 (OVF) 格式标准。您可以从 Citrix 网站下载文件。您需要一个 Citrix 帐户才能登录。如果您没有 Citrix 帐户，请访问主页 http://www.citrix.com。单击**新用户链接**，然后按照说明创建一个新的 Citrix 帐户。

登录后，从 Citrix® 主页导航到以下路径：

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

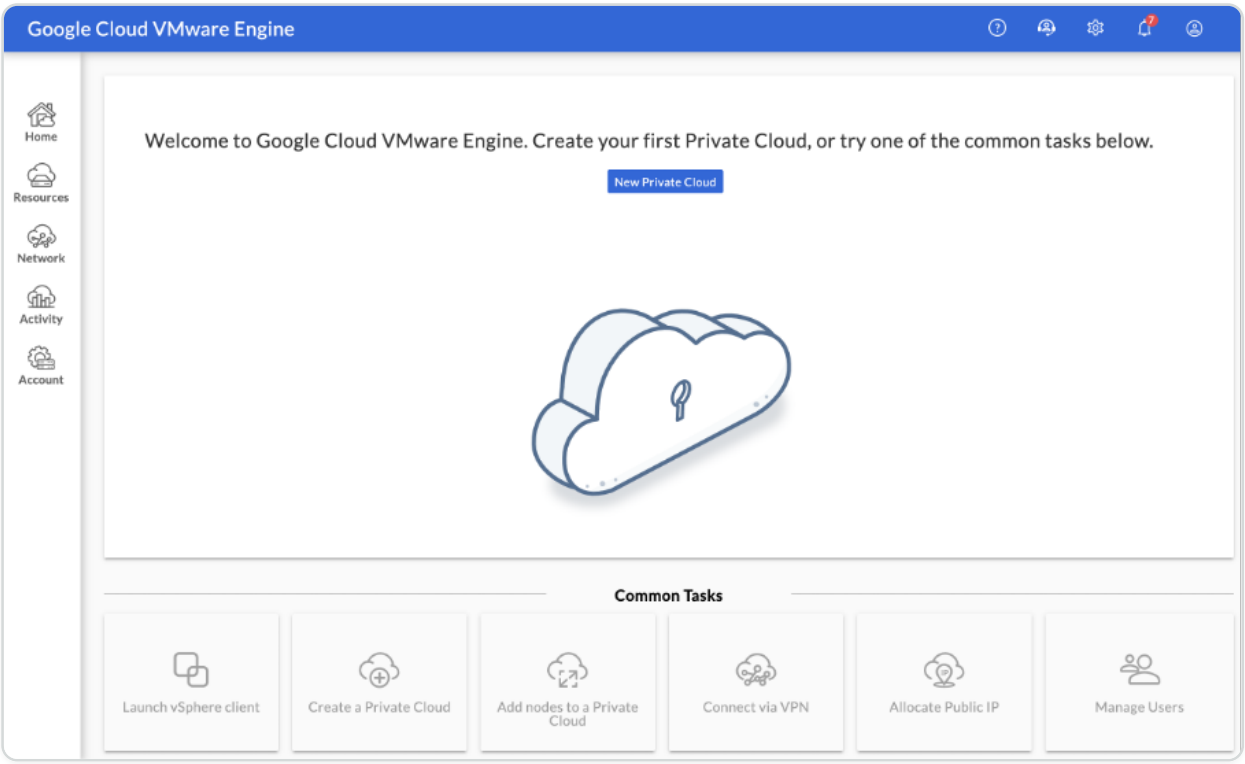
将以下文件复制到与 ESX 服务器位于同一网络的某个工作站。将所有三个文件复制到同一个文件夹中。

- 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 谷歌云 VMware 引擎

1. 登录到您的 GCVE 门户，然后导航到**主页**。

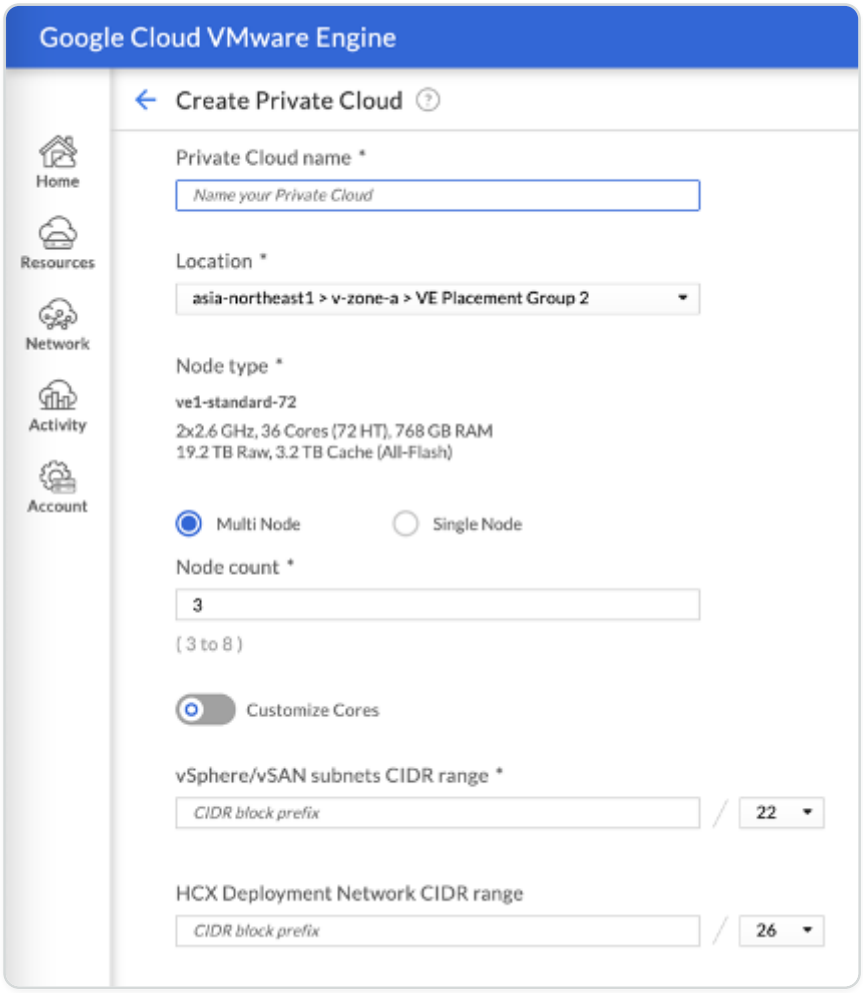
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 在**新建私有云**页面中，输入以下详细信息：

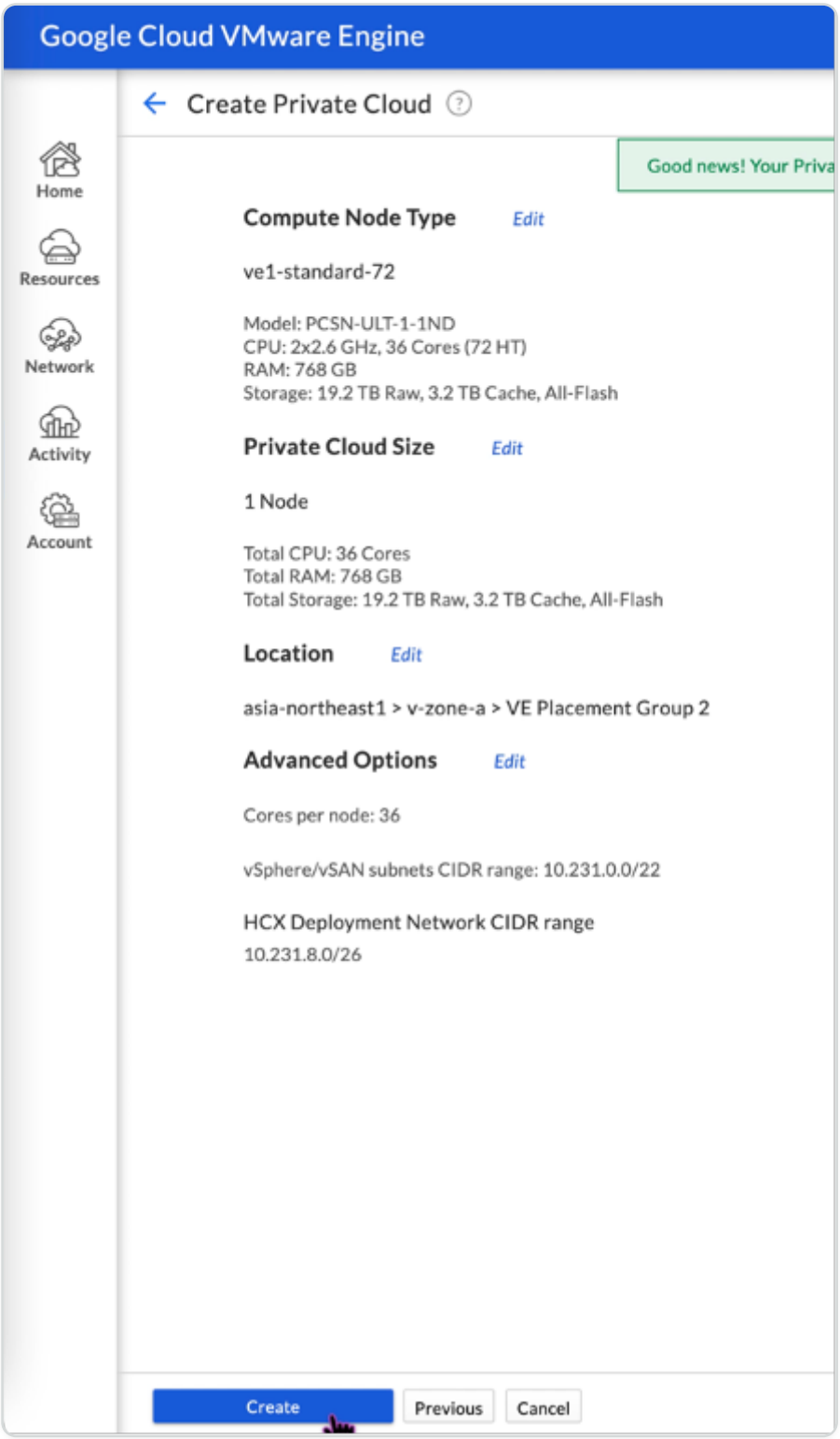
   - 选择至少 3 个 ESXi 主机以创建私有云的默认集群。
   - 对于**vSphere/vSan 子网 CIDR 范围**字段，请使用 /22 地址空间。
   - 对于**HCX 部署网络 CIDR 范围**字段，请使用 /26 地址空间。
   - 对于虚拟网络，请确保 CIDR 范围不与您的任何本地或其他 GCP 子网（虚拟网络）重叠。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

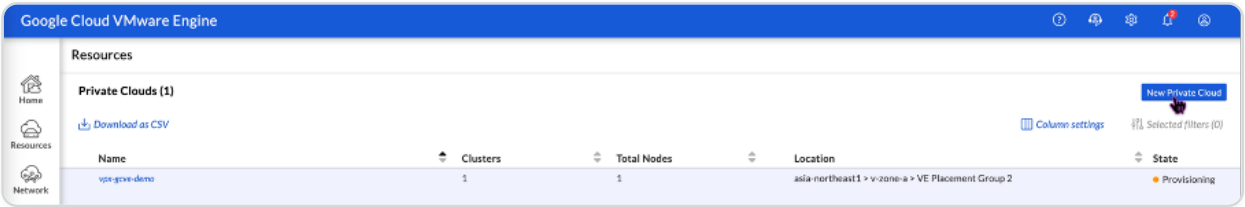


3. 点击 **审核并创建**。
4. 审核设置。如果需要更改任何设置，请点击 **上一步**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 点击 **创建**。私有云预置过程开始。私有云预置可能需要长达两小时。
6. 转到 **资源** 以验证已创建的私有云。

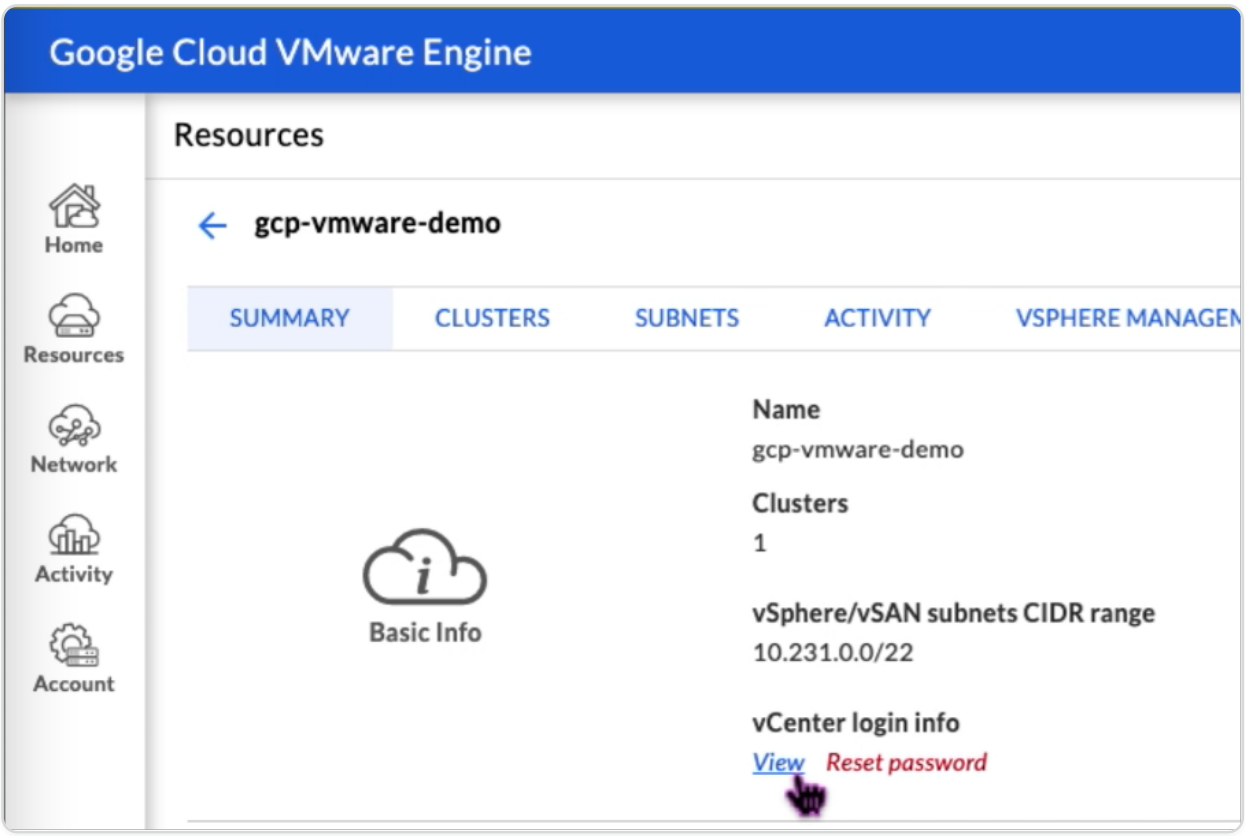


© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. 要访问此资源，您必须使用点到站点 VPN 连接到 GCVE。有关更多信息，请参阅以下文档：
   - VPN 网关
   - 使用 VPN 连接

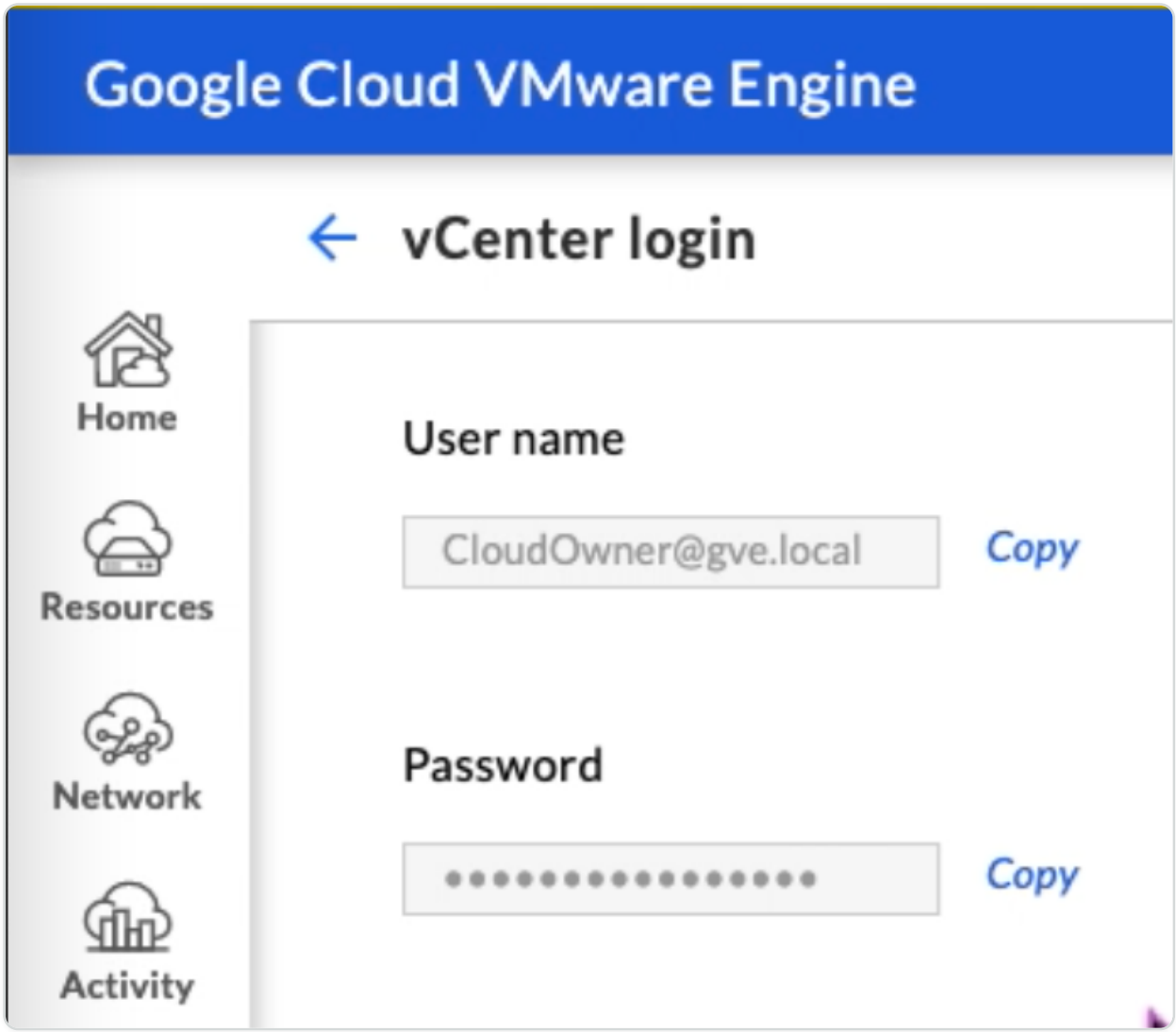
访问您的私有云 vCenter 门户

1. 导航到您的 Google Cloud VMware Engine 私有云。在 **摘要** 选项卡中，在 **vCenter 登录信息** 下，点击 **查看**。

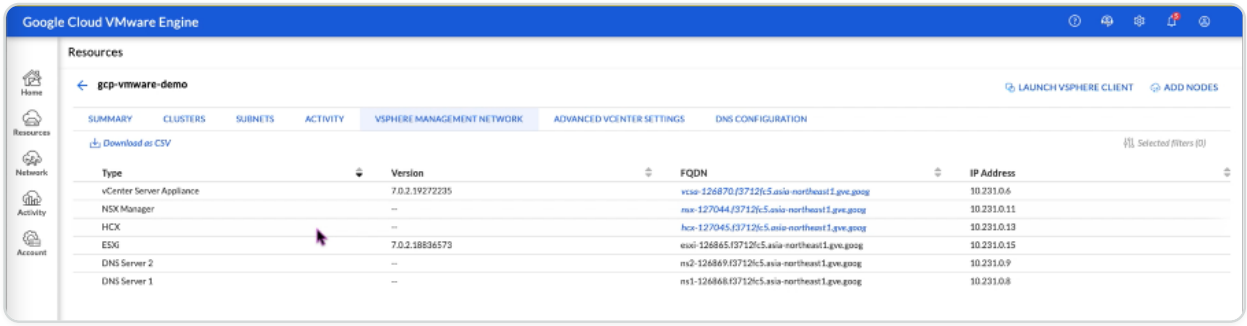


2. 记下 vCenter 凭据。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



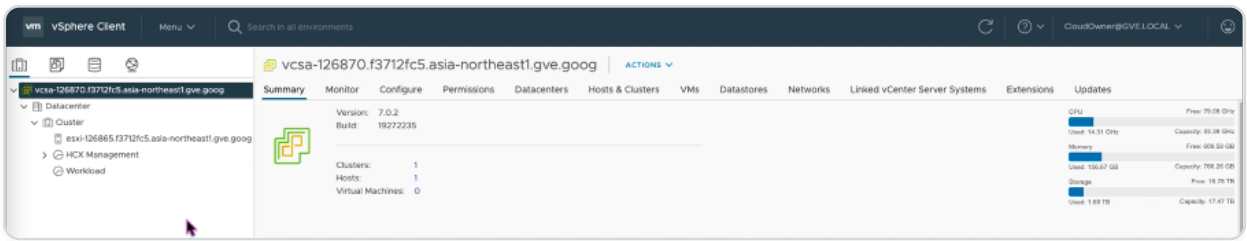
3. 通过点击 **LAUNCH VSPHERE CLIENT** 启动 vSphere 客户端，或者导航到 **VSPHERE MANAGEMENT NETWORK** 并点击 **vCenter Server Appliance** FQDN。



4. 使用本步骤第 2 步中记录的 vCenter 凭据登录到 VMware vSphere。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 在 vSphere 客户端中，您可以验证在 GCVE 门户中创建的 ESXi 主机。

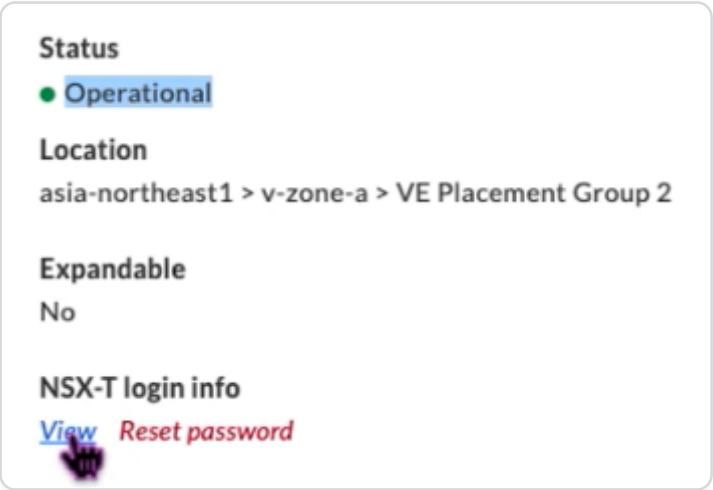


在 GCVE NSX-T 门户中创建 NSX-T 段

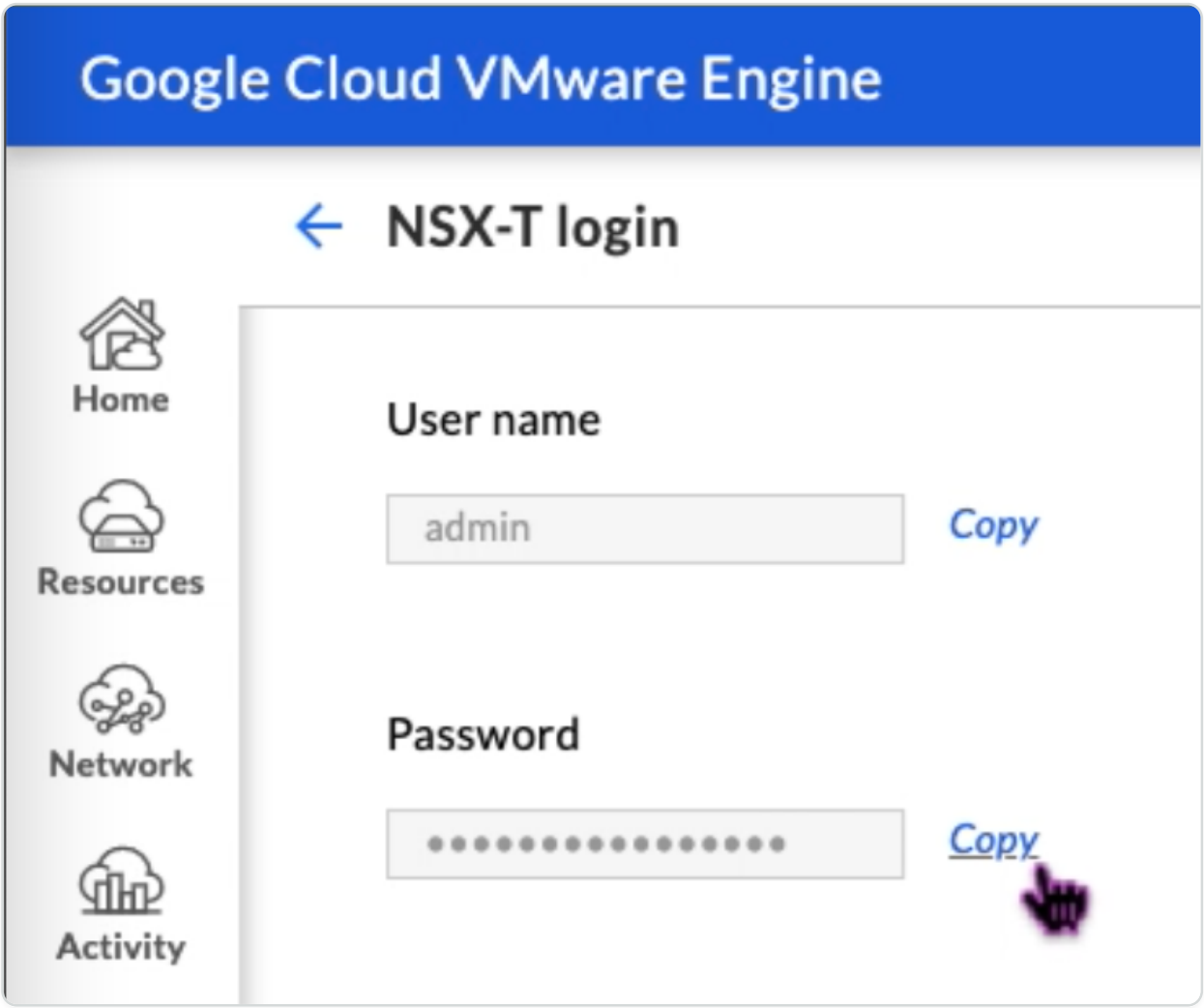
您可以在 Google Cloud VMware Engine 控制台的 NSX Manager 中创建和配置 NSX-T 段。这些段连接到默认的 Tier-1 网关，这些段上的工作负载获得东西向和南北向连接。创建段后，它会显示在 vCenter 中。

1. 在您的 GCVE 私有云中，在 **Summary > NSX-T login info** 下，选择 **View**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

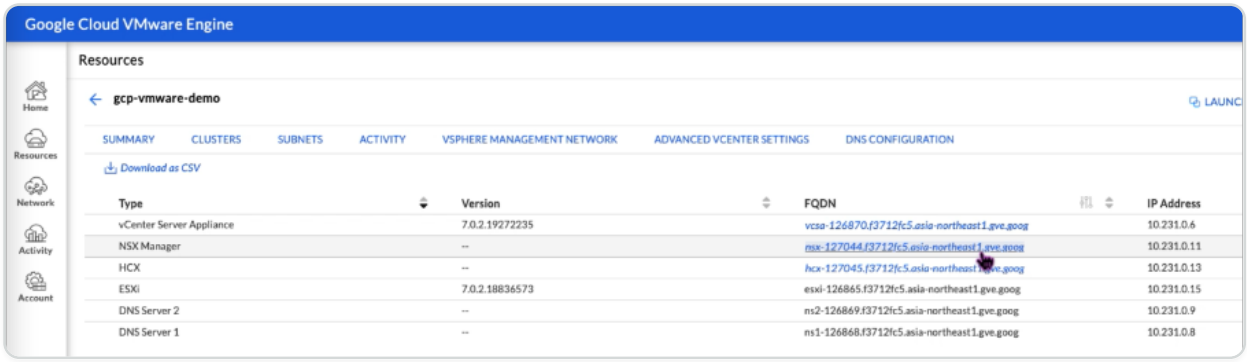


2. 记下 NSX-T 凭据。

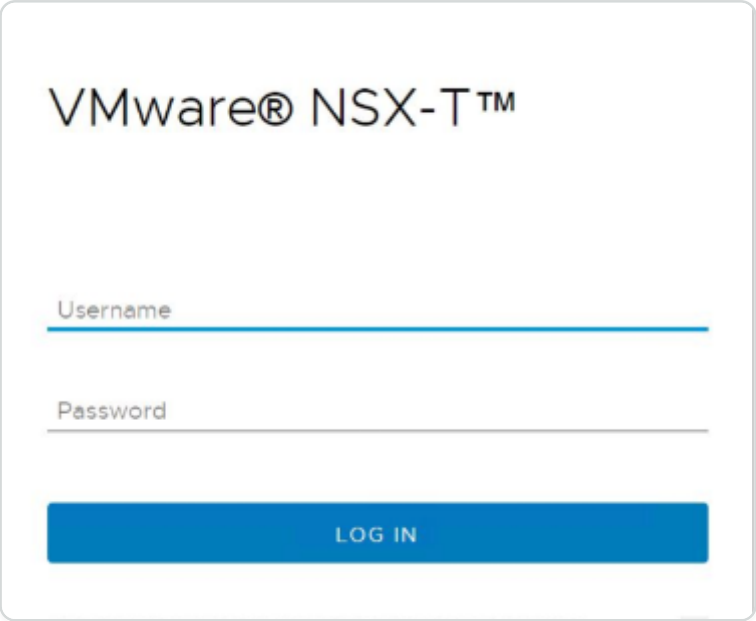


3. 通过导航到 **VSPHERE MANAGEMENT NETWORK** 并点击 **NSX Manager** FQDN 来启动 NSX Manager。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

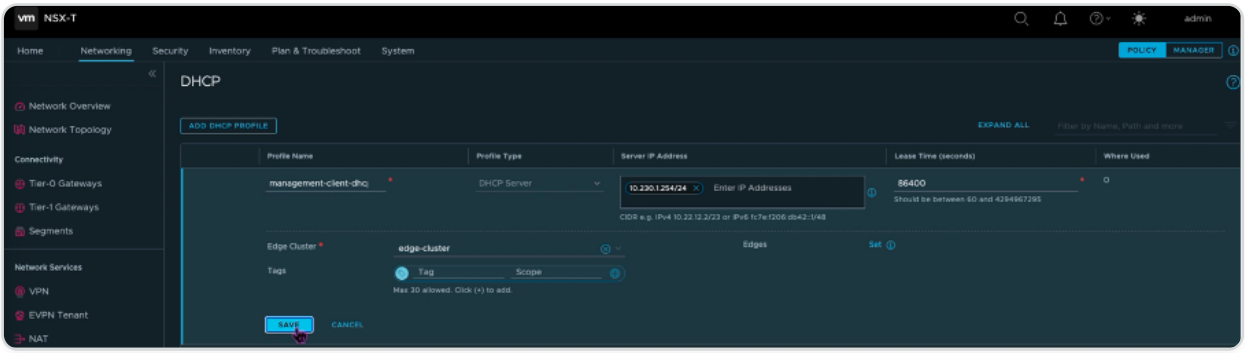


4. 使用本步骤第 2 步中记录的凭据登录到 NSX Manager。

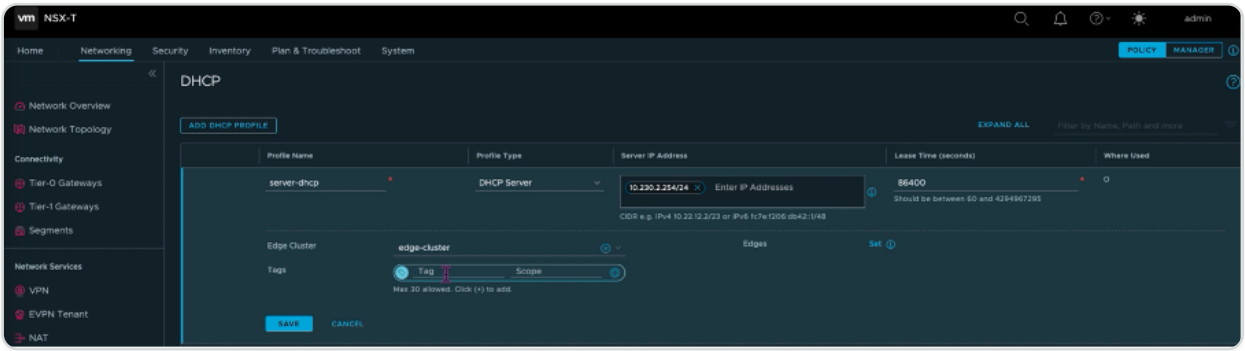


5. 为新的分段或子网设置 DHCP 服务。
6. 在创建子网之前，请设置 DHCP 服务。
7. 在 NSX-T 中，转到“**网络 > DHCP**”。网络仪表板显示该服务创建了一个 tier-0 和一个 tier-1 网关。
8. 要开始预配 DHCP 服务器，请单击“**添加 DHCP 配置文件**”。
9. 在 DHCP 名称字段中，输入 **Client-Management** 配置文件的名称。
10. 选择“**DHCP 服务器**”作为配置文件类型。
11. 在“**服务器 IP 地址**”列中，提供 DHCP 服务 IP 地址范围。
12. 选择您的“**边缘集群**”。
13. 单击“**保存**”以创建 DHCP 服务。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

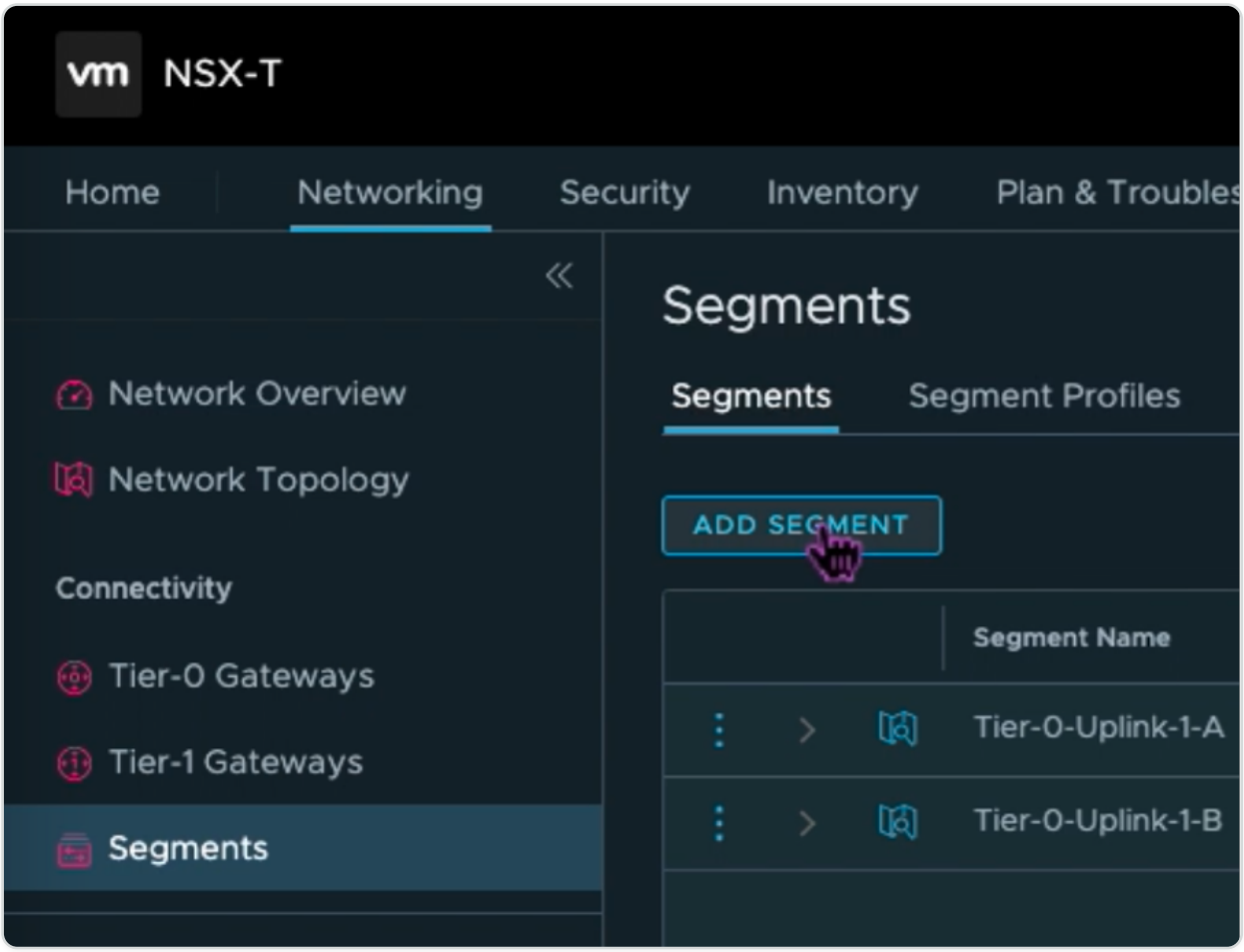


14. 对服务器 DHCP 范围重复步骤 6 到 13。

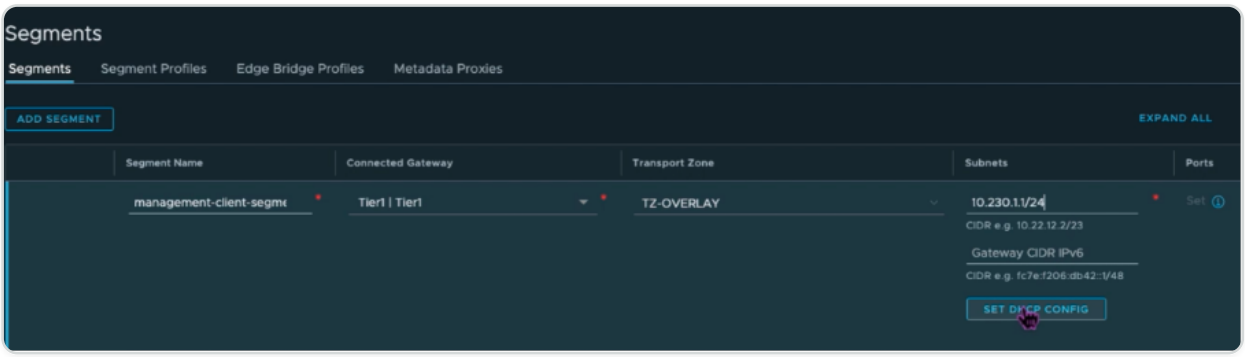


15. 创建两个独立的分段：一个用于客户端和管理接口，另一个用于服务器接口。
16. 在 NSX-T 中，转到“**网络 > 分段**”。
17. 点击 **添加分段**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

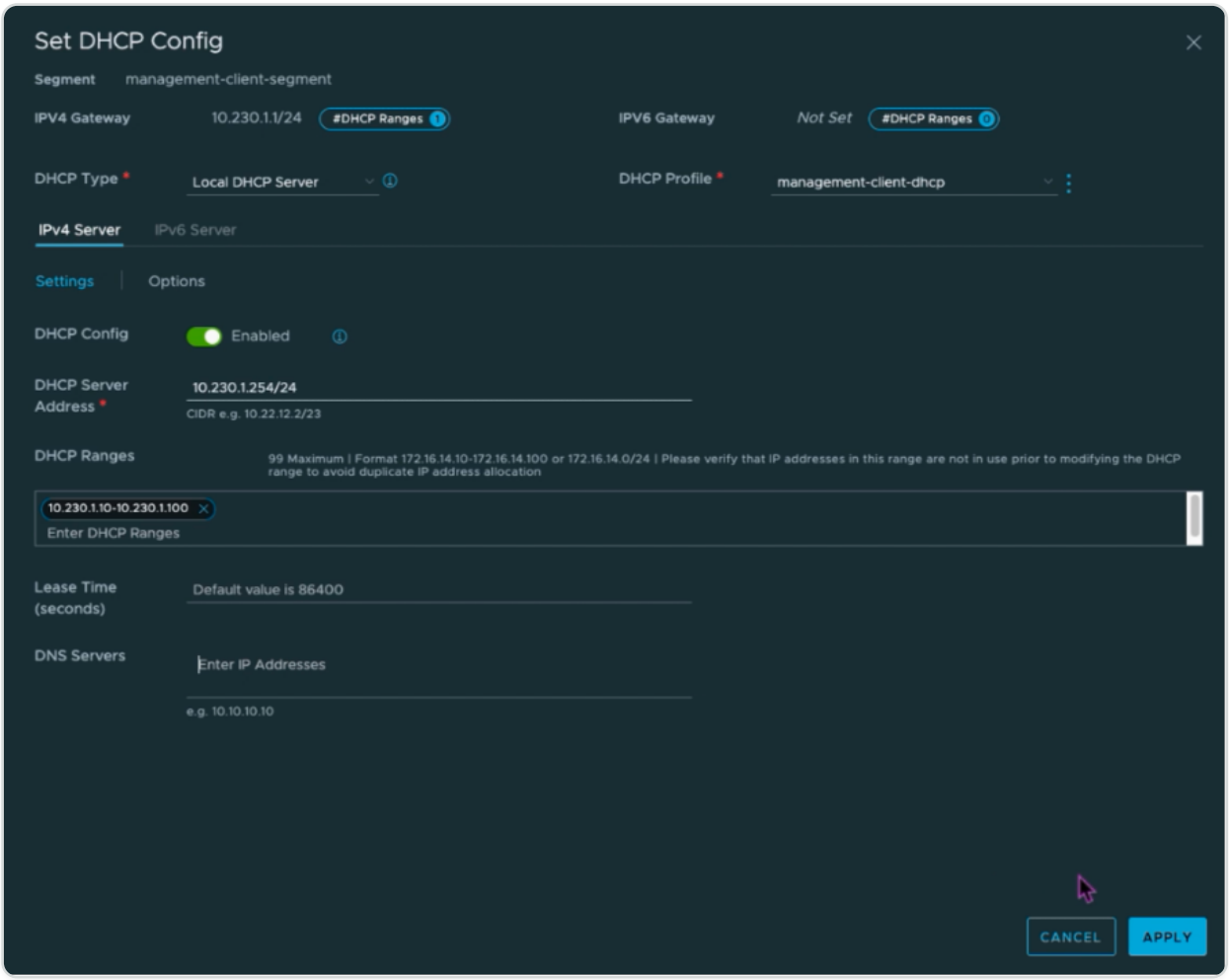


18. 在 **分段名称** 字段中，输入您的 **客户端管理** 分段的名称。
19. 在 **连接的网关** 列表中，选择 **Tier1** 以连接到 Tier-1 网关。
20. 在 **传输区域** 列表中，选择 **TZ-OVERLAY | Overlay**。
21. 在 **子网** 列中，输入子网范围。将 `.1` 指定为最后一个八位字节的子网范围。例如，10.12.2.1/24。



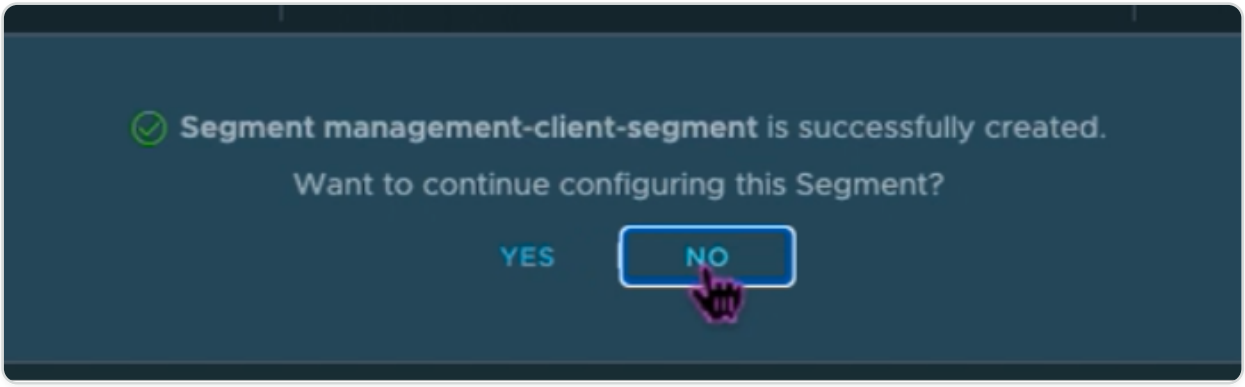
22. 点击 **设置 DHCP 配置**，并为 **DHCP 范围** 字段提供值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



23. 点击 **应用** 以保存您的 DHCP 配置。

24. 点击 **保存**。



25. 对服务器分段重复步骤 17 到 24。

26. 现在，您可以在 vCenter 中创建虚拟机时选择这些网络分段。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 上安装并配置私有云后，您可以使用 vCenter 在 VMware Engine 上安装虚拟设备。您可以安装的虚拟设备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到站点 VPN 的桌面上执行以下步骤：

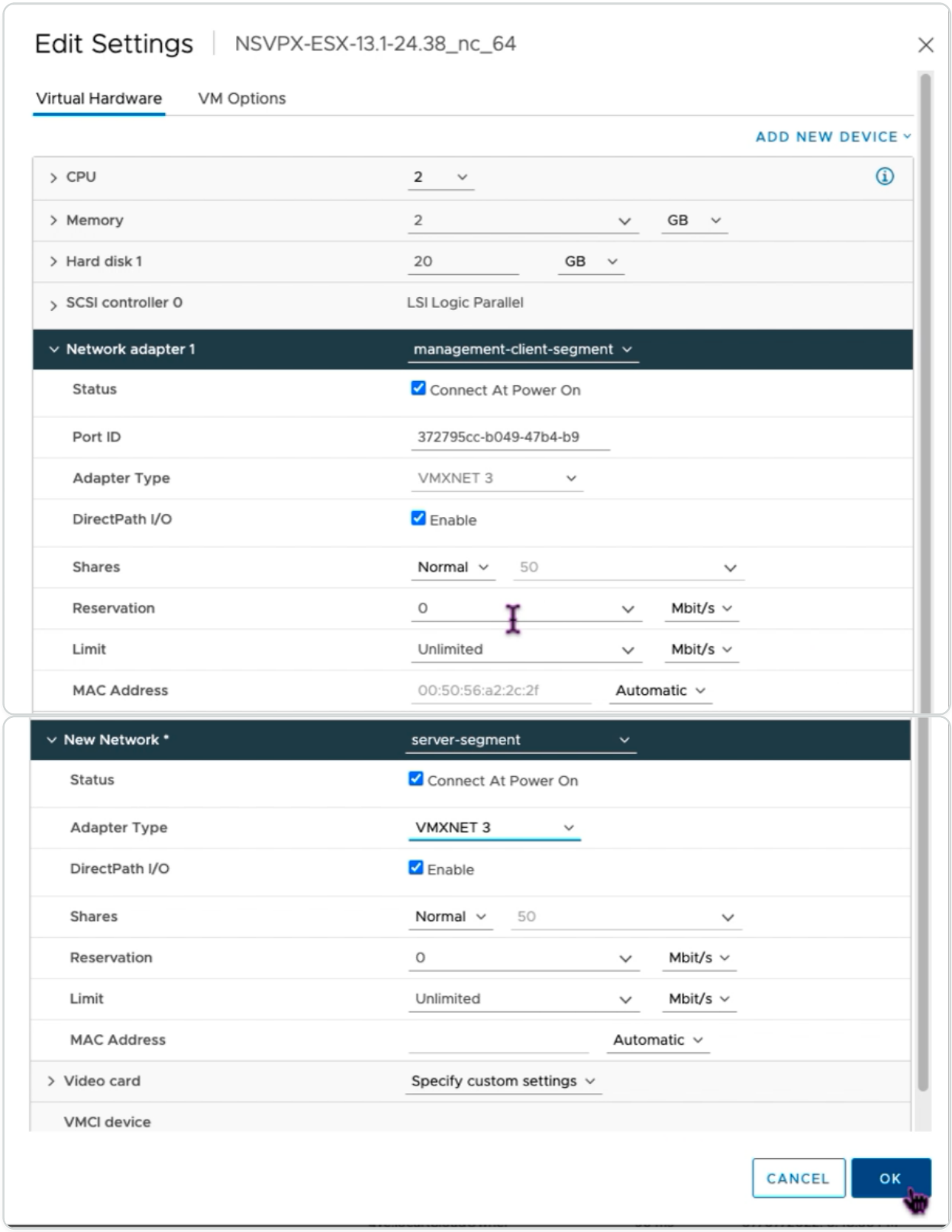
1. 从 NetScaler 下载站点下载适用于 ESXi 主机的 NetScaler VPX 实例安装文件。
2. 在连接到私有云点到站点 VPN 的浏览器中打开 VMware vCenter。
3. 在“**用户名**”和“**密码**”字段中，键入管理员凭据，然后单击“**登录**”。
4. 在“**文件**”菜单上，单击“**部署 OVF 模板**”。
5. 在“**部署 OVF 模板**”对话框中，在“**从文件部署**”字段中，浏览到保存 NetScaler VPX 实例安装文件的位置，选择 .ovf 文件，然后单击“**下一步**”。

   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，请修改 OVF 以使用 VMXNET3 接口而不是 E1000。VMXNET3 接口的可用性受 GCP 基础设施限制，并且可能在 Google Cloud VMware Engine 中不可用。

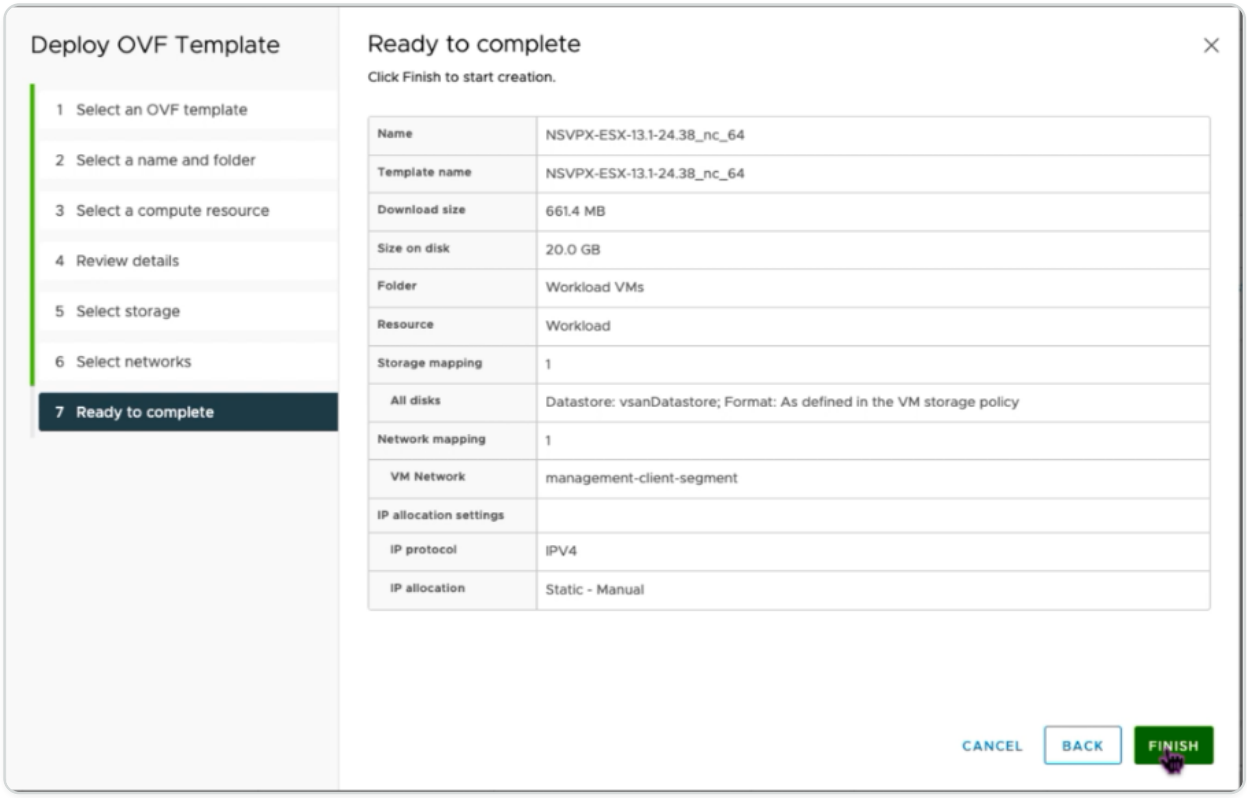
6. 将虚拟设备 OVF 模板中显示的网路映射到您在 NSX-T Manager 上配置的网路。单击“**确定**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. 单击“**完成**”开始在 VMware 云上安装虚拟设备。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. 您现在可以启动 NetScaler VPX 实例了。在导航窗格中，选择您已安装的 NetScaler VPX 实例，然后从右键菜单中选择 **Power On**。单击 **Launch Web Console** 选项卡以模拟控制台端口。

   启动 VPX 实例(/en-us/vpx/media/gcve-power-on-vpx-instance.png)

9. 您现在已通过 vSphere 客户端连接到 NetScaler VM。

   连接到 NetScaler VM(/en-us/vpx/media/avs-adc-vm.png)

10. 首次启动时，为 ADC 实例设置管理 IP 和网关。

    设置管理 IP 和网关(/en-us/vpx/media/gcve-set-management-ip.png)

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>
    ```

    示例：

    ```
    ssh nsroot@10.230.1.10
    ```

12. 您可以使用 `show ns ip` 命令验证 ADC 配置。

    使用 `show nsip` 命令进行验证(/en-us/vpx/media/avs-show-nsip-citrix.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 VMware 云上为 NetScaler VPX 实例分配公共 IP 地址

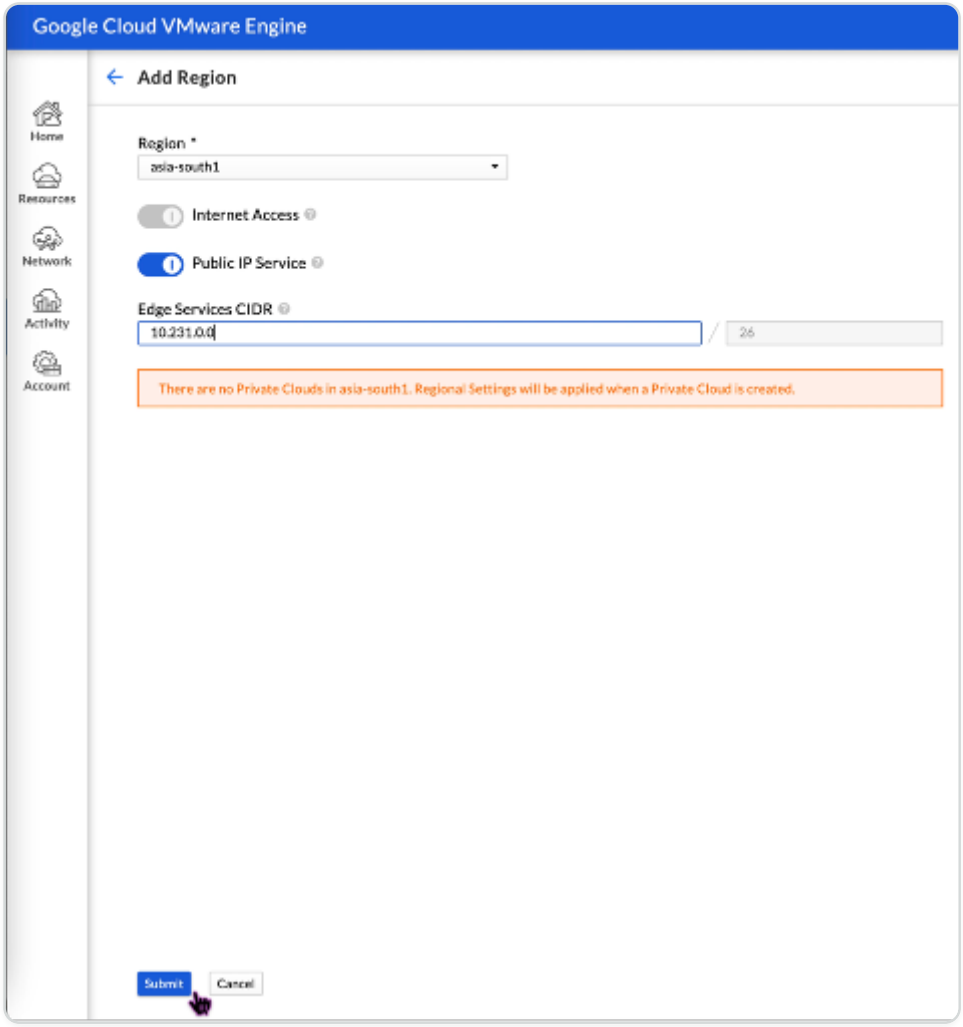
在 GCVE 上安装并配置 NetScaler VPX 实例后，您必须为客户端接口分配一个公共 IP 地址。在为您的 VM 分配公共 IP 地址之前，请确保您的 Google Cloud 区域已启用公共 IP 服务。

要为新区域启用公共 IP 服务，请按照以下步骤操作：

1. 在 GCVE 控制台中，导航到 **Network > REGIONAL SETTINGS > Add Region**。

   GCVE 区域设置(/en-us/vpx/media/gcve-regional-settings.png)

2. 选择您的区域并启用**互联网访问**和**公共 IP 服务**。
3. 分配一个边缘服务 CIDR，确保该 CIDR 范围不与您的任何本地或其它 GCP/GCVE 子网（虚拟网络）重叠。

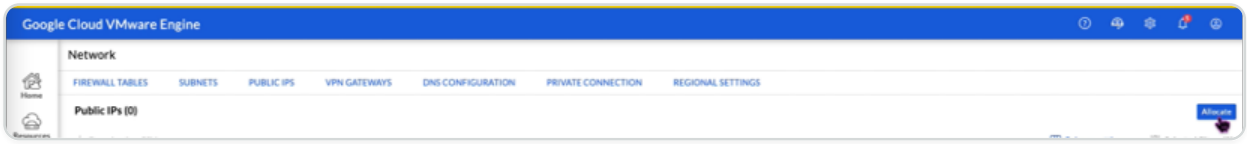


4. 公共 IP 服务将在几分钟内为所选区域启用。

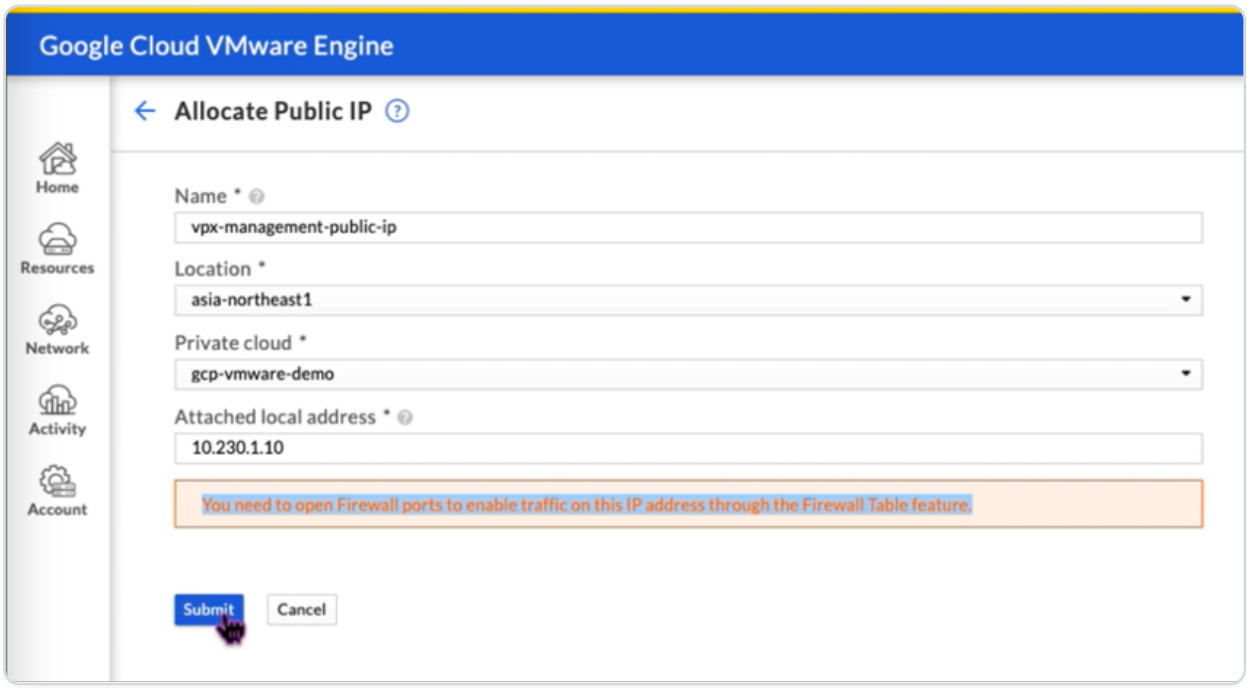
要将公共 IP 分配给 GCVE 上的 NetScaler VPX 实例上的客户端接口，请在 GCVE 门户上执行以下步骤：

1. 在 GCVE 控制台上，导航到**网络 > 公共 IP > 分配**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 输入公共 IP 的名称。选择您的区域，并选择将使用该 IP 的私有云。
3. 提供您希望公共 IP 映射到的接口的私有 IP。这将是您的**客户端**接口的**私有 IP**。
4. 单击**提交**。



5. 公共 IP 在几分钟内即可使用。
6. 在您使用公共 IP 之前，必须添加防火墙规则以允许访问它。有关更多信息，请参阅防火墙规则。

添加后端 GCP 自动扩缩服务

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。为了满足不断增长的需求，您必须向上扩展网络资源。当需求减少时，您需要向下扩展以避免未充分利用资源造成不必要的成本。为了最大限度地降低应用程序运行成本，您必须持续监控流量、内存和 CPU 使用率等。然而，手动监控流量非常繁琐。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流量监控和资源扩展过程。

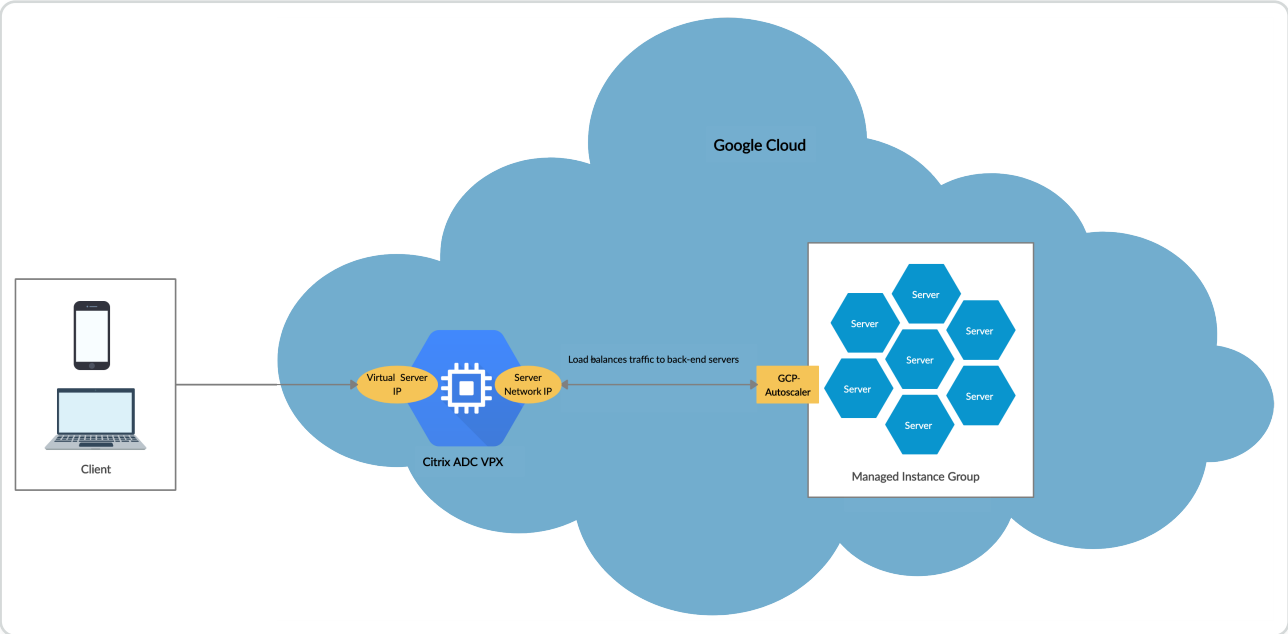
NetScaler VPX 实例与 GCP 自动扩缩服务集成，提供以下优势：

- **负载平衡和管理**：根据需求自动配置服务器以进行扩缩。VPX 实例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以平衡负载。虚拟 IP 地址和子网 IP 地址在 VPX 实例上自动配置。
- **高可用性**：检测跨多个区域的托管实例组并平衡服务器负载。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **更好的网络可用性**：VPX 实例支持：
  - 同一放置组中的后端服务器
  - 不同区域中的后端服务器

此图说明了 GCP 自动扩缩服务如何在充当负载平衡虚拟服务器的 NetScaler VPX 实例中工作。

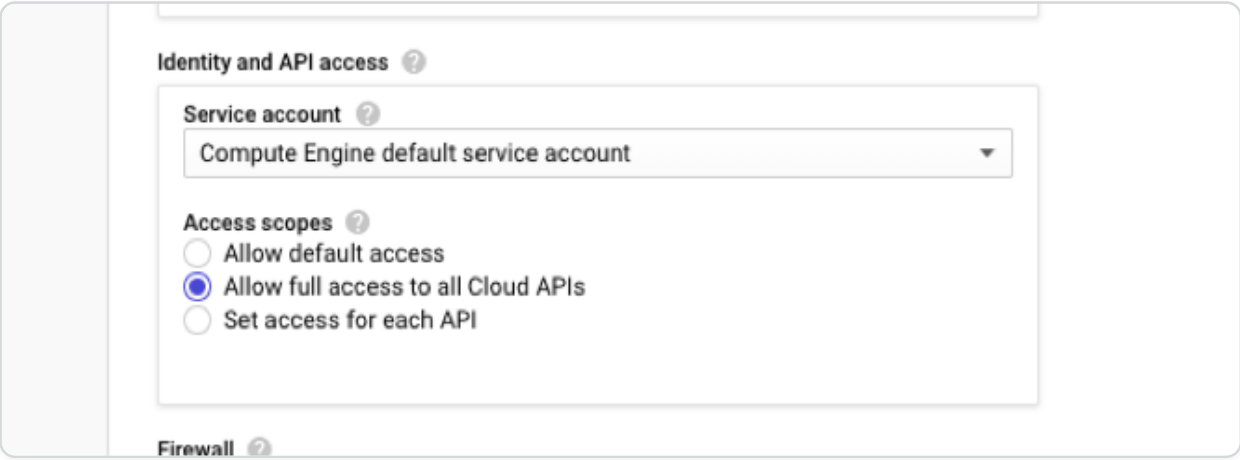


开始之前

在开始将自动扩缩与 NetScaler VPX 实例结合使用之前，您必须完成以下任务。

- 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，允许完全访问所有 Cloud API。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 确保您的 GCP 服务帐户具有以下 IAM 权限：

```
REQUIRED_INSTANCE_IAM_PERMS = [



"compute.instances.get",

"compute.zones.list",

"compute.instanceGroupManagers.list",

"compute.instanceGroupManagers.get"

]
```

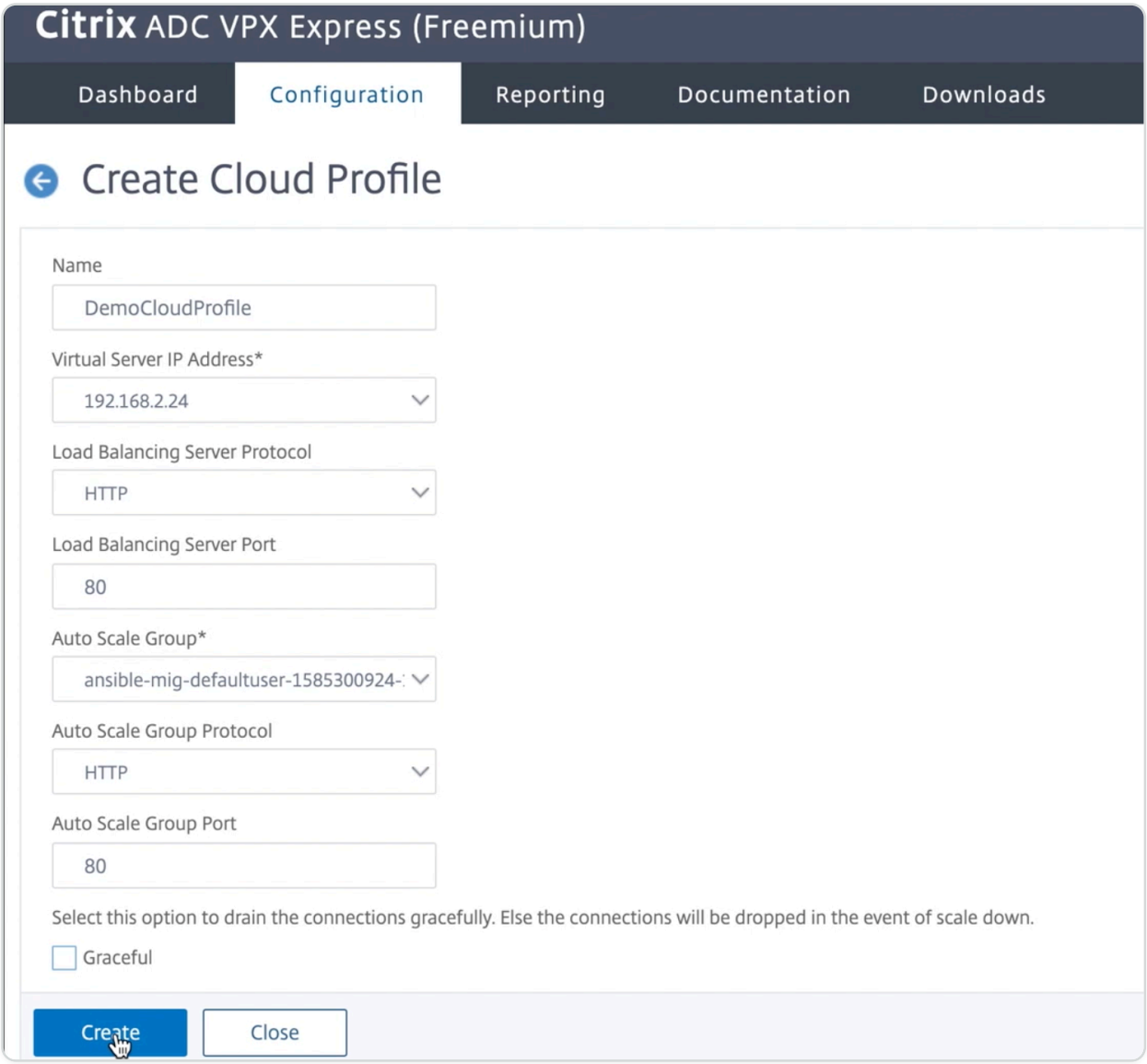
- 要设置自动扩缩，请确保已配置以下各项：
  - 实例模板
  - 托管实例组
  - 自动扩缩策略

将 GCP 自动扩缩服务添加到 NetScaler VPX 实例

您可以通过使用 GUI 单击一下即可将自动扩缩服务添加到 VPX 实例。完成以下步骤以将自动扩缩服务添加到 VPX 实例：

1. 使用您的 `nsroot` 凭据登录到 VPX 实例。
2. 首次登录 NetScaler VPX 实例时，您会看到默认的云配置文件页面。从下拉菜单中选择 GCP 托管实例组，然后单击“**创建**”以创建云配置文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



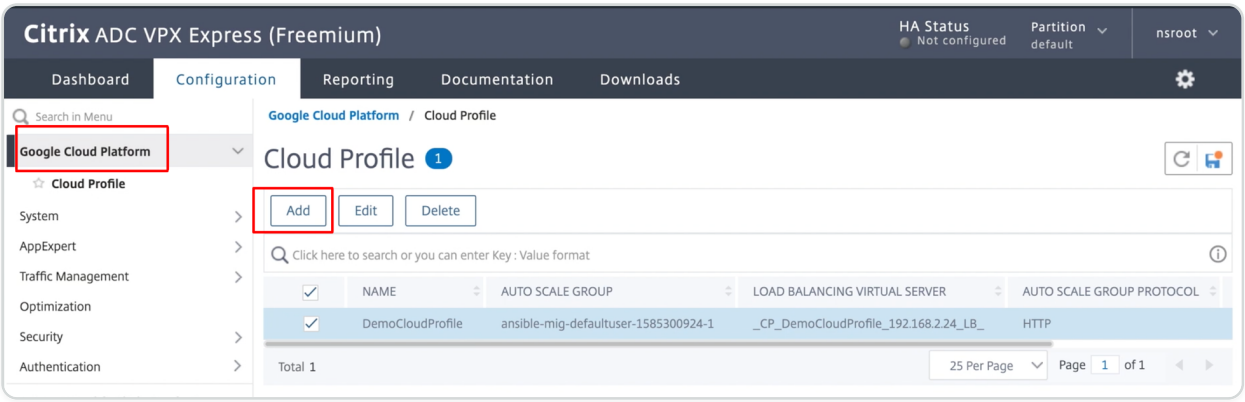
- **虚拟服务器 IP 地址**字段会自动填充与实例关联的所有 IP 地址。
- **自动扩缩™ 组**会预填充您 GCP 帐户上配置的托管实例组。
- 选择“**自动扩缩组协议**”和“**自动扩缩组端口**”时，请确保您的服务器侦听配置的协议和端口。在服务组中绑定正确的监视器。默认情况下，使用 TCP 监视器。
- 取消选中“**Graceful**”复选框，因为它不受支持。

注意：

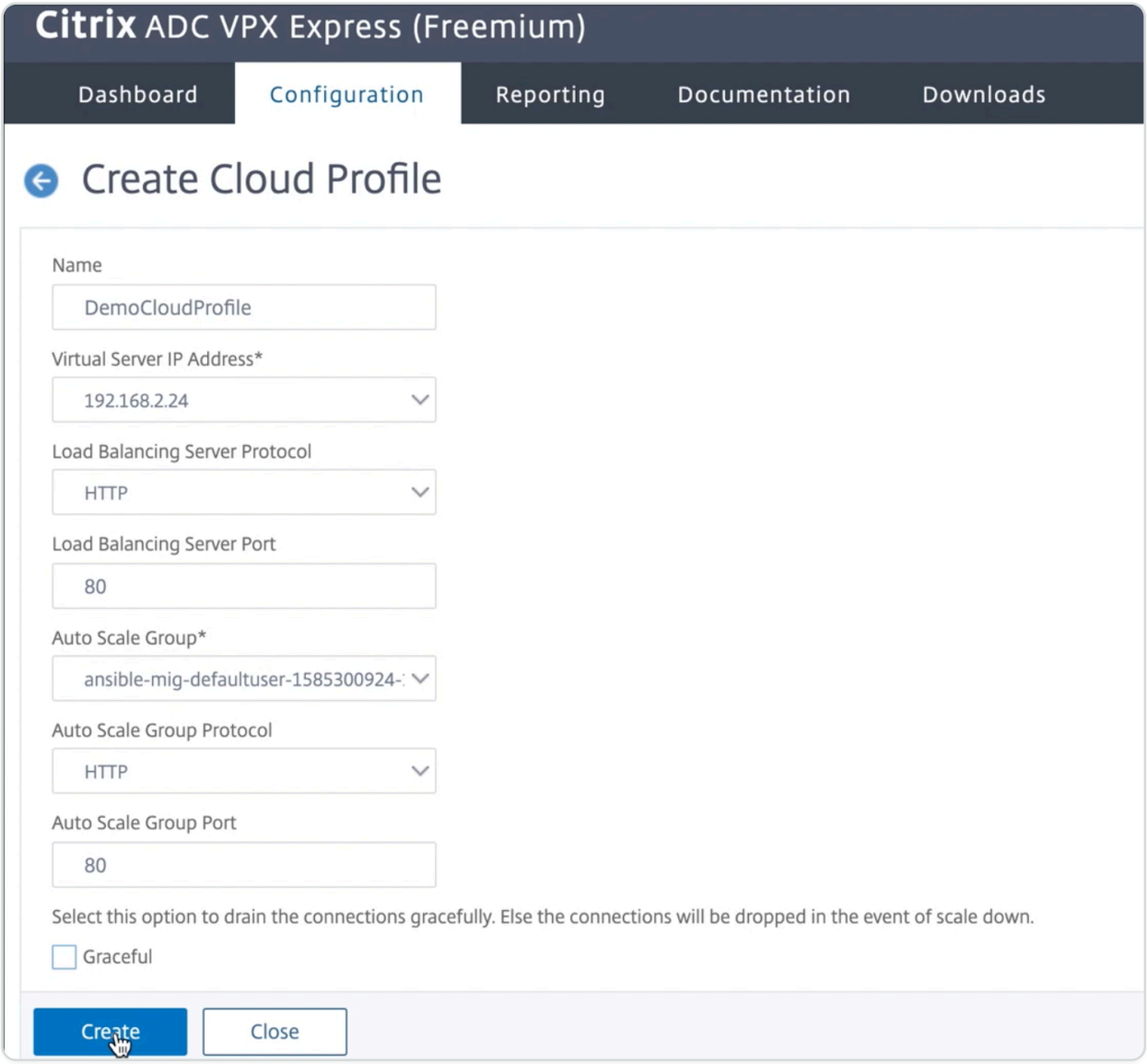
对于 SSL 协议类型的自动扩缩，在创建云配置文件后，负载均衡虚拟服务器或服务组将处于关闭状态，因为缺少证书。您可以手动将证书绑定到虚拟服务器或服务组。

3. 首次登录后，如果您想创建云配置文件，请在 GUI 上转到“**System > Google Cloud Platform > Cloud Profile**”，然后单击“**Add**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



出现“**创建云配置文件**”配置页面。

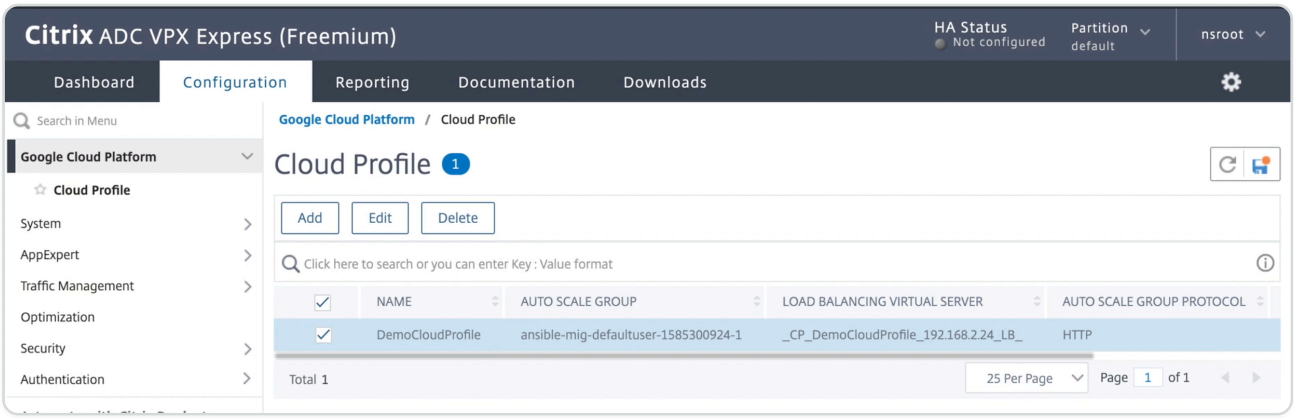


云配置文件会创建一个 NetScaler 负载均衡虚拟服务器和一个服务组，其成员是托管实例组的服务器。您的后端服务器必须可以通过 VPX 实例上配置的 SNIP 访问。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

从 NetScaler 13.1-42.x 版本开始，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 实例支持在公有云中使用相同的自动扩缩组提供多个服务。



GCP 上的 NetScaler VPX 实例的 VIP 扩展支持

NetScaler 设备位于客户端和服务器之间，因此客户端请求和服务器响应都通过它。在典型安装中，设备上配置的虚拟服务器提供客户端用于访问设备背后应用程序的连接点。部署所需的公共虚拟 IP (VIP) 地址数量因情况而异。

GCP 架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，每个子网可以跨区域的多个可用区。此外，GCP 还有以下限制：

- 公共 IP 地址数量与 NIC 数量之间存在 1:1 映射。每个 NIC 只能分配一个公共 IP 地址。
- 更高容量的实例类型最多只能连接 8 个 NIC。

例如，n1-standard-2 实例只能有 2 个 NIC，并且可以添加的公共 VIP 数量限制为 2。有关详细信息，请参阅 VPC 资源配额。

为了在 NetScaler VPX 实例上实现更高规模的公共虚拟 IP 地址，您可以将 VIP 地址配置为实例元数据的一部分。NetScaler VPX 实例内部使用 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，您可以使用用于创建转发规则的相同 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 实例中使用公共 VIP 地址时在规模方面的限制。

有关转发规则的更多信息，请参阅转发规则概览。

有关 HA 的更多信息，请参阅 (/zh-cn/citrix-adc/13-1/system/high-availability-introduction.html)。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意事项

- Google 对每个虚拟 IP 转发规则收取额外费用。实际费用取决于创建的条目数量。相关费用可在 Google 定价文档中找到。
- 转发规则仅适用于公共 VIP。当部署需要私有 IP 地址作为 VIP 时，您可以使用别名 IP 地址。
- 您只能为需要 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。您还可以添加具有相同 VIP 地址但协议不同的新负载平衡虚拟服务器。

开始之前

- NetScaler VPX 实例必须部署在 GCP 上。
- 必须预留外部 IP 地址。有关详细信息，请参阅预留静态外部 IP 地址。
- 确保您的 GCP 服务帐号具有以下 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",

]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 服务帐号具有以下 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 服务帐号具有以下 IAM 权限：

```
REQUIRED_IAM_PERMS = [
"compute.addresses.get",
"compute.addresses.list",
"compute.addresses.use",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"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，您必须将 **Service Account User role** 添加到您的服务帐号。

在 NetScaler VPX 实例上为 VIP 扩展配置外部 IP 地址

1. 在 Google Cloud Console 中，导航到 **VM 实例**页面。
2. 创建新的 VM 实例或使用现有实例。
3. 单击实例名称。在 **VM 实例详细信息**页面上，单击**编辑**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 通过输入以下内容更新**自定义元数据**：

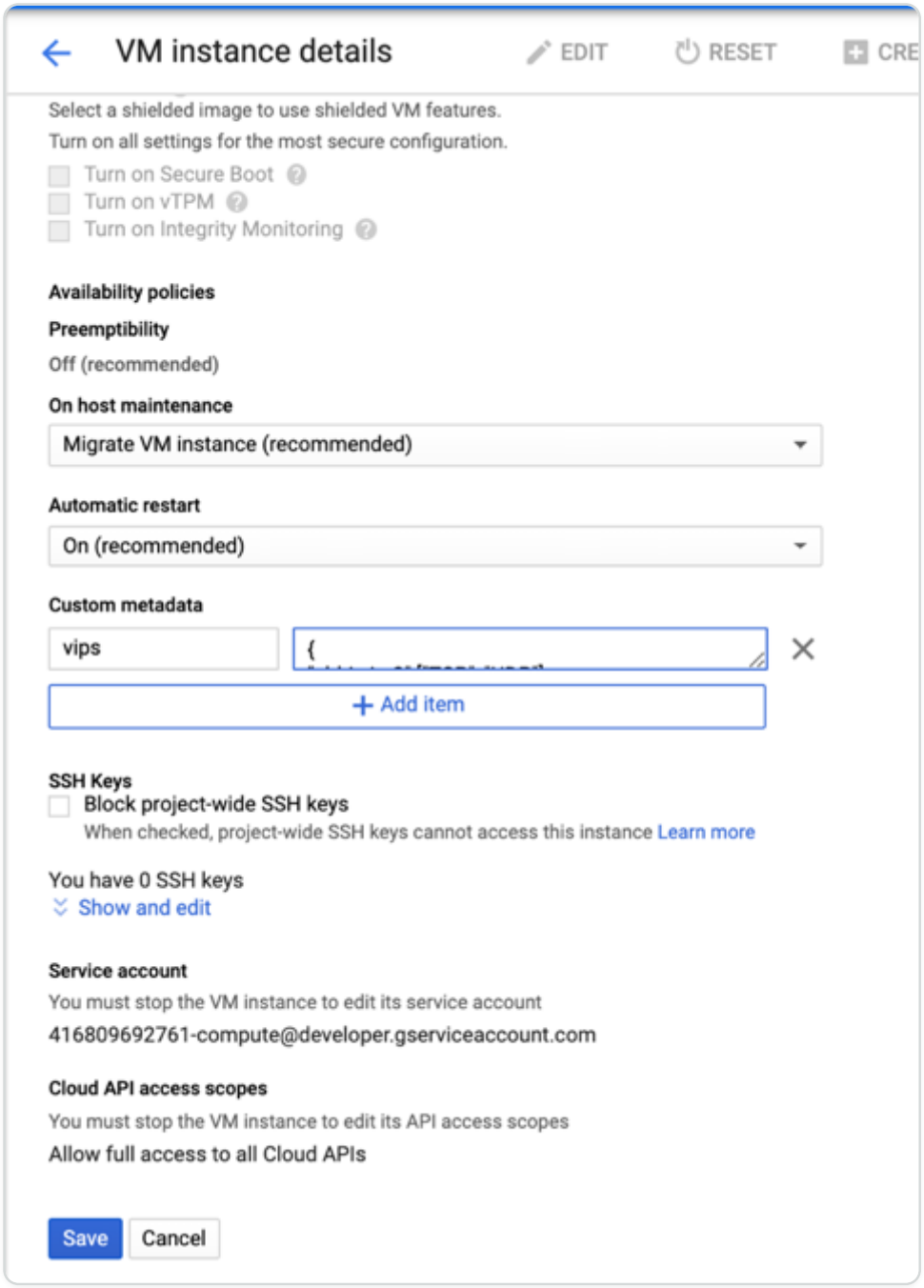
   - 键 = vips
   - 值 = 以以下 JSON 格式提供值：

     { "外部预留 IP 的名称": , }

   GCP 支持以下协议：

   - AH
   - ESP
   - ICMP
   - SCT
   - TCP
   - UDP

© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关更多信息，请参阅自定义元数据。

自定义元数据示例：

{ "外部IP1名称":, "外部IP2名称": }

在此示例中，NetScaler VPX 实例为每个 IP-协议对内部创建一个转发规则。元数据条目映射到转发规则。此示例可帮助您了解为元数据条目创建了多少个转发规则。

创建了四个转发规则，如下所示：

a. external-ip1-name 和 传输控制协议

b. 外部 IP1 名称 和 UDP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. 外部 IP2 名称 和 ICMP

d. 外部 IP2 名称 和 AH

注意：

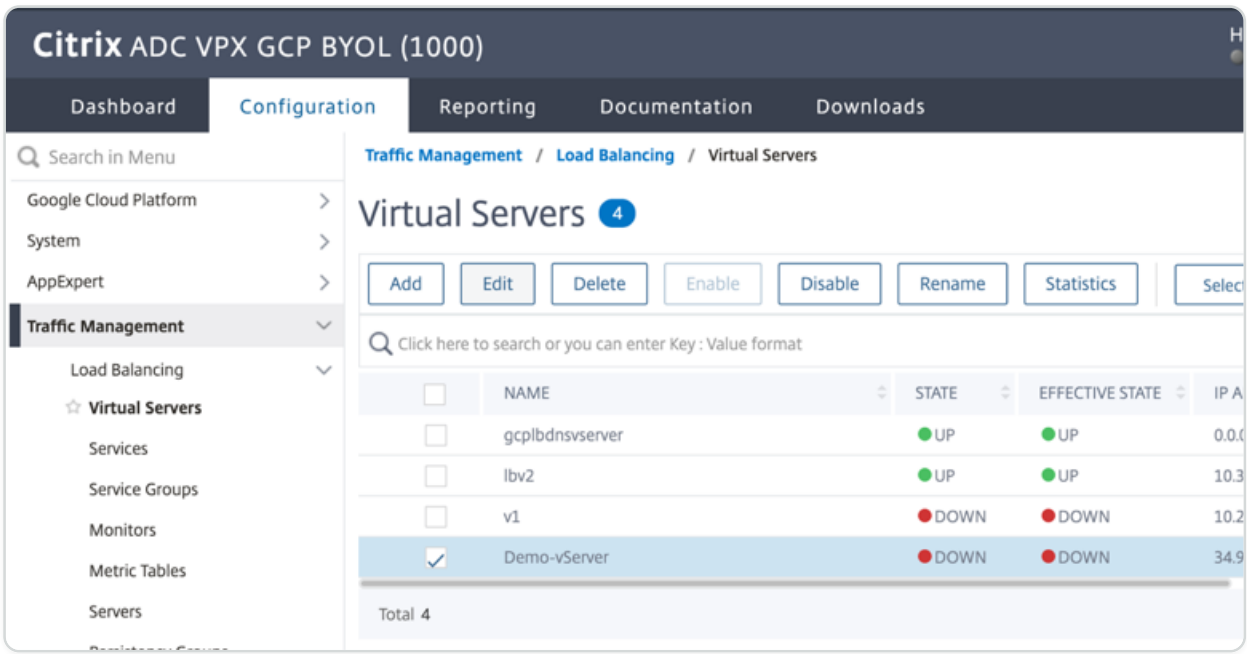
在 HA 模式下，您必须仅在主实例上添加自定义元数据。在故障转移时，自定义元数据将同步到新的主实例。

5. 单击“**保存**”。

在 NetScaler VPX 实例上设置具有外部 IP 地址的负载平衡虚拟服务器

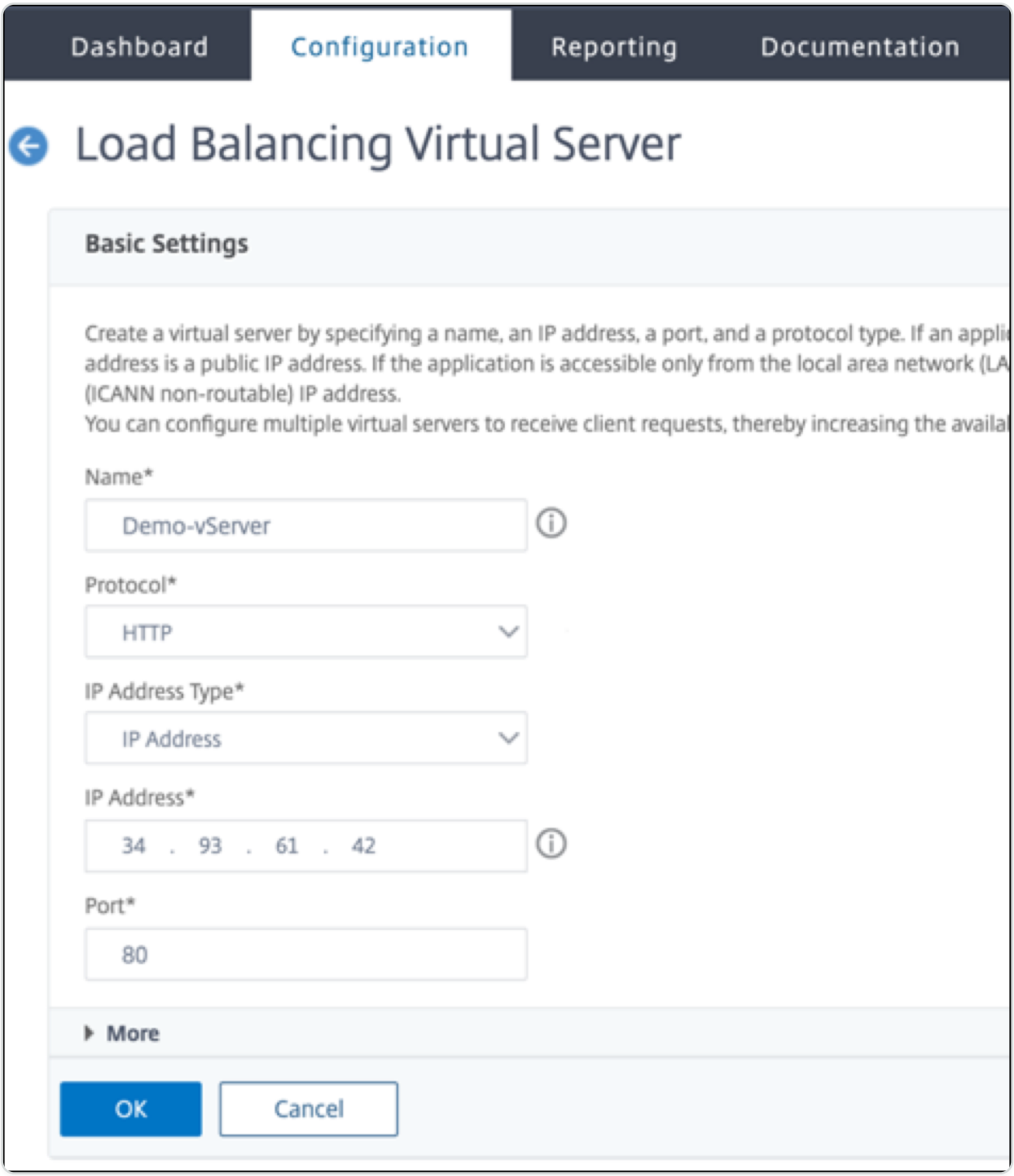
步骤 1。添加负载平衡虚拟服务器。

1. 导航到“**配置 > 流量管理 > 负载平衡 > 虚拟服务器 > 添加**”。



2. 为“名称”、“协议”、“IP 地址类型 (IP 地址)”、“IP 地址”（作为 VIP 添加到 ADC 的转发规则的外部 IP 地址）和“端口”添加所需值，然后单击“**确定**”。

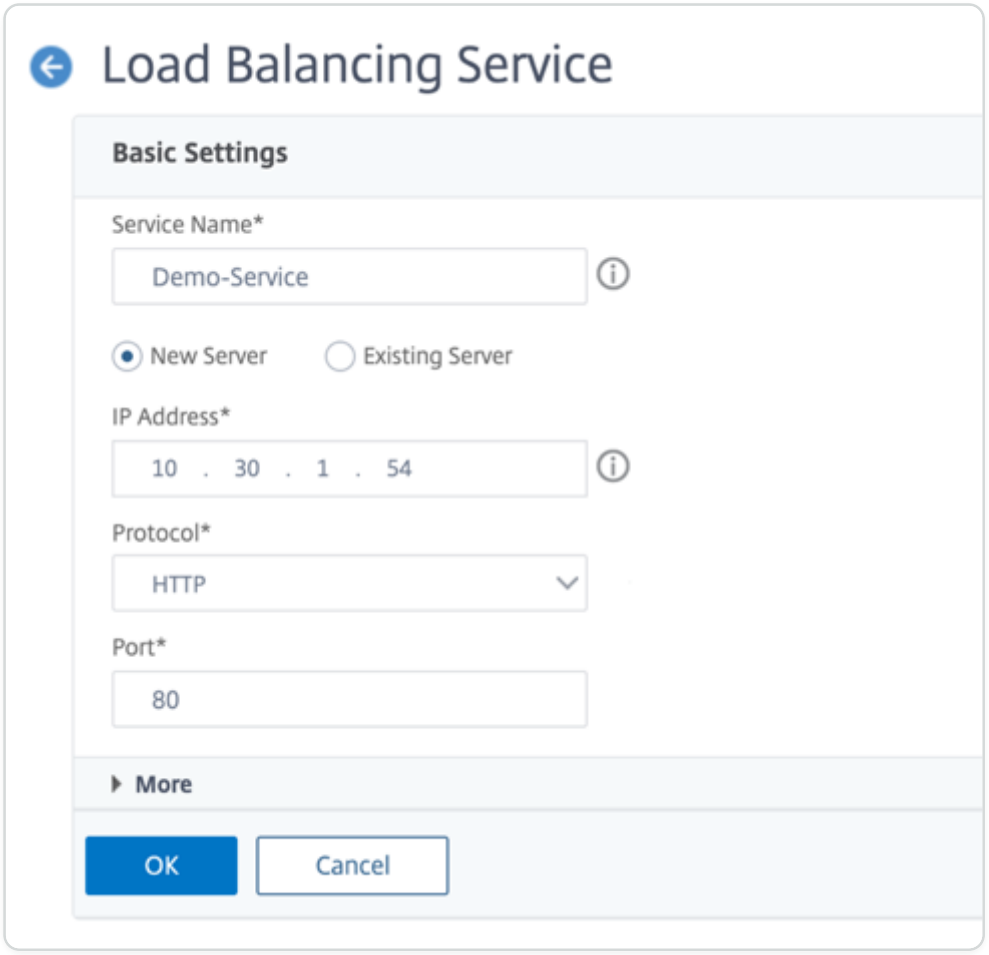
© 1997–2026 Citrix Systems, Inc. All rights reserved.



步骤 2。添加服务或服务组。

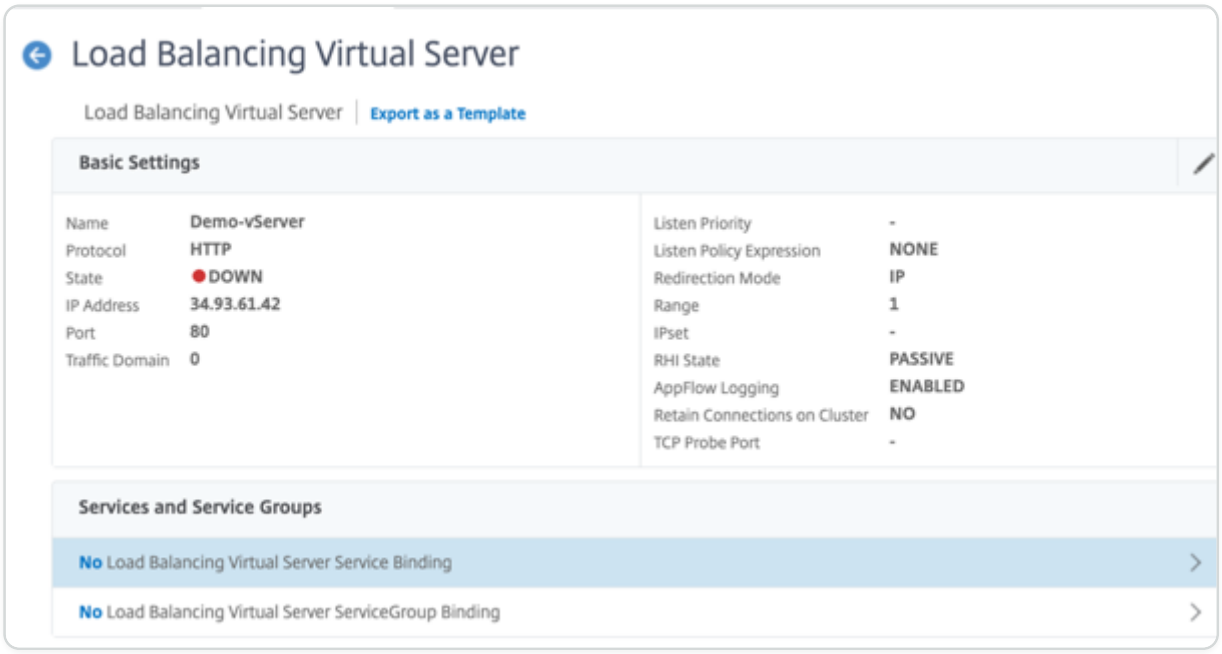
1. 导航到“**配置 > 流量管理 > 负载平衡 > 服务 > 添加**”。
2. 为“服务名称”、“IP 地址”、“协议”和“端口”添加所需值，然后单击“**确定**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



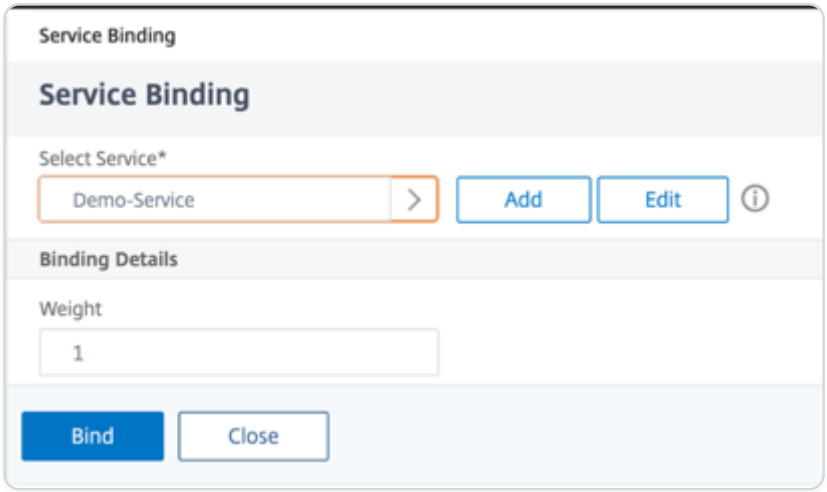
步骤 3。将服务或服务组绑定到负载平衡虚拟服务器。

1. 导航到 **配置 > 流量管理 > 负载均衡 > 虚拟服务器**。
2. 选择在 **步骤 1** 中配置的负载平衡虚拟服务器，然后单击 **Edit**。
3. 在 **服务和服务组** 页面中，单击 **无负载均衡虚拟服务器服务绑定**。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 选择在 **步骤 3** 中配置的服务，然后单击 **Bind**。



5. 保存配置。

在 GCP 上排查 VPX 实例故障

Google Cloud Platform (GCP) 提供对 NetScaler VPX 实例的控制台访问权限。仅当网络连接时才能进行调试。要查看实例的系统日志，请访问控制台并检查 **系统日志文件**。

要提交支持案例，请查找您的 GCP 账号和支持 PIN 码，并致电 NetScaler® 支持。系统会要求您提供姓名和电子邮件地址。要查找支持 PIN 码，请登录 VPX GUI 并导航到 **系统** 页面。

这是一个显示支持 PIN 码的系统页面示例。

GCP 技术 PIN 码(/en-us/vpx/media/gcp-technical-pin.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler VPX 实例上的巨型帧

NetScaler VPX 设备支持接收和传输包含多达 9216 字节 IP 数据的巨型帧。与标准 IP MTU 大小为 1500 字节相比，巨型帧可以更高效地传输大型文件。

NetScaler 设备可以在以下部署场景中使用巨型帧：

- 巨型帧到巨型帧。设备以巨型帧形式接收数据并以巨型帧形式发送。
- 非巨型帧到巨型帧。设备以常规帧形式接收数据并以巨型帧形式发送。
- 巨型帧到非巨型帧。设备以巨型帧形式接收数据并以常规帧形式发送。

有关详细信息，请参阅在 NetScaler 设备上配置巨型帧支持。

巨型帧支持可在以下虚拟化平台上运行的 NetScaler VPX 设备上使用：

- VMware ESX 平台
- Linux-KVM 平台
- Citrix® XenServer® 虚拟化平台
- 亚马逊网络服务 (AWS)

VPX 设备上的巨型帧工作方式与 MPX 设备上的巨型帧类似。有关巨型帧及其用例的更多信息，请参阅在 MPX 设备上配置巨型帧。MPX 设备上巨型帧的用例也适用于 VPX 设备。

为在 VMware ESX 上运行的 VPX 实例配置巨型帧

执行以下任务以在 VMware ESX 服务器上运行的 NetScaler VPX 设备上配置巨型帧：

1. 将 VPX 设备接口或通道的 MTU 设置为 1501–9000 范围内的值。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包含最多 9000 字节 IP 数据的巨型帧。
2. 使用 VMware ESX 服务器的管理应用程序，在其相应的物理接口上设置相同的 MTU 大小。有关在 VMware ESX 物理接口上设置 MTU 大小的更多信息，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

执行以下任务以在 Linux-KVM 服务器上运行的 NetScaler VPX 设备上配置巨型帧：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 将 VPX 设备接口或通道的 MTU 设置为 1501–9216 范围内的值。使用 NetScaler VPX CLI 或 GUI 设置 MTU 大小。
2. 使用 Linux-KVM 服务器的管理应用程序，在其相应的物理接口上设置相同的 MTU 大小。有关在 Linux-KVM 物理接口上设置 MTU 大小的更多信息，请参阅 `<http://www.linux-kvm.org/>` 。

为在 Citrix XenServer 上运行的 VPX 实例配置巨型帧

执行以下任务以在 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. 关闭所有使用需要更改 MTU 的网络的 VPX 实例。
3. 在“**网络**”选项卡上，选择网络 - 网络 0/1/2。
4. 选择“**属性**”并编辑 MTU。

在 XenServer 上配置巨型帧后，您可以在 ADC 设备上配置巨型帧。有关更多信息，请参阅 (/zh-cn/citrix-adc/13-1/networking/interfaces/jumbo-frames/configuring-jumbo-frames-support-on-citrix-adc-appliance.html)。

为在 AWS 上运行的 VPX 实例配置巨型帧

Azure 上的 VPX 不需要主机级配置。要在 VPX 上配置巨型帧，请按照 (/zh-cn/citrix-adc/13-1/networking/interfaces/jumbo-frames/configuring-jumbo-frames-support-on-citrix-adc-appliance.html) 中给出的步骤操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

常见问题

以下部分帮助您根据 Citrix® Application Delivery Controller™ (ADC) VPX 对常见问题进行分类。

- 功能和特性
- 加密
- 定价和打包
- 虚拟机管理程序
- 容量规划或规模调整
- 系统要求
- 其他技术常见问题

功能和特性

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 是否包含 ADC 设备的所有 Web 应用程序优化功能?

是的。NetScaler VPX 包含所有负载平衡、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）和卸载功能。有关 NetScaler 功能和特性的完整概述，请参阅 按您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 Application Firewall 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 与 NetScaler 设备上的 NetScaler Gateway 之间是否存在任何差异?

功能上，它们是相同的。NetScaler VPX 上的 NetScaler Gateway 支持 NetScaler 软件版本 9.1 中提供的所有 NetScaler Gateway 功能。但是，由于 NetScaler 设备提供专用的 SSL 加速硬件，因此它比 NetScaler VPX 实例提供更大的 SSL VPN 可扩展性。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

除了能够在虚拟机监控程序上运行这一明显差异之外，NetScaler VPX 与 NetScaler 物理设备有何不同?

客户在行为上看到差异主要体现在两个方面。首先是 NetScaler VPX 无法提供与许多 NetScaler 设备相同的性能。其次是，虽然 NetScaler 设备集成了自己的 L2 网络功能，但 NetScaler VPX 依赖于虚拟机监控程序提供其 L2 网络服务。通常，这不会限制 NetScaler VPX 的部署方式。物理 NetScaler 设备上配置的某些 L2 功能可能必须在底层虚拟机监控程序上进行配置。

NetScaler VPX 在应用交付市场中扮演着怎样的角色?

NetScaler VPX 通过以下方式改变了应用交付市场的格局：

- 通过使 NetScaler 设备更经济实惠，NetScaler VPX 使任何 IT 组织都能够部署 NetScaler 设备。它不仅适用于他们最关键的 Web 应用程序，还适用于他们所有的 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 不仅可以用于优化托管在虚拟化服务器上的 Web 应用程序。它还使 Web 应用程序交付本身成为一种虚拟化服务，可以轻松快速地部署到任何地方。IT 组织使用标准数据中心流程来完成诸如 Web 应用程序交付基础设施的配置、自动化和费用分摊等任务。
- NetScaler VPX 开辟了新的部署架构，如果仅使用物理设备，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特定需求进行定制，以处理处理器密集型操作，例如压缩和应用防火墙检查。在数据中心边缘，NetScaler MPX 设备处理高容量的全网络任务，例如初始流量分发、SSL 加密或解密、拒绝服务 (DoS) 攻击防御和全局负载均衡。将高性能 NetScaler MPX 设备与易于部署的 NetScaler VPX 虚拟设备相结合，为现代大规模数据中心环境带来了无与伦比的灵活性和定制能力，同时还降低了整体数据中心成本。

NetScaler VPX 如何融入我们的 Citrix 交付中心战略?

随着 NetScaler VPX 的推出，整个 Citrix 交付中心产品都可作为虚拟化产品提供。整个 Citrix 交付中心受益于 Citrix XenCenter 中提供的强大管理、配置、监控和报告功能。这可以快速部署到几乎任何环境中，并可以从任何地方进行集中管理。借助一个集成式虚拟化应用交付基础设施，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 是否支持 SSL 卸载?

是的。但是，NetScaler VPX 在软件中执行所有 SSL 处理，因此 NetScaler VPX 无法提供与 NetScaler 设备相同的 SSL 性能。NetScaler VPX 每秒最多可支持 750 个新的 SSL 事务。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安装在托管 NetScaler VPX 的服务器上的第三方 SSL 卡是否能加速 SSL 加密或解密?

否。支持第三方 SSL 卡无法将 NetScaler VPX 与特定的硬件实现关联起来。这极大地削弱了组织在数据中心内灵活托管 NetScaler VPX 的能力。当需要比 NetScaler VPX 提供更高的 SSL 吞吐量时，必须使用 NetScaler MPX 设备。

NetScaler VPX 是否支持与物理 NetScaler 设备相同的加密密码?

VPX 支持所有与物理 NetScaler 设备相同的加密密码，但 ECDSA 除外。

NetScaler VPX 的 SSL 事务吞吐量是多少?

有关 SSL 事务吞吐量的信息，请参阅 NetScaler VPX 数据表。

定价和打包

NetScaler VPX 如何打包?

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 提供标准版、高级版和高级版。NetScaler VPX 提供从 10 Mbps (VPX 10) 到 100 Gbps (VPX 100G) 的带宽。更多详细信息可在 NetScaler VPX 数据表中找到。

NetScaler VPX 在所有虚拟机管理程序上的定价都相同?

是的。

所有虚拟机管理程序上的 VPX 都使用相同的 NetScaler SKU?

是的。

NetScaler VPX 许可证可以从一个虚拟机管理程序移动到另一个（例如从 VMware 到 Hyper-V）？

是的。NetScaler VPX 许可证独立于底层 Hypervisor。如果您决定将 NetScaler VPX 虚拟机从一个 Hypervisor 移动到另一个，则无需获取新许可证。但是，您可能需要重新托管现有的 NetScaler VPX 许可证。

NetScaler VPX 实例可以升级?

是的。吞吐量限制和 NetScaler 系列版本都可以升级。两种类型的升级都有可用的升级 SKU。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

如果我想以高可用性对的形式部署 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 Express 是否包含所有 NetScaler 标准功能 它是否包含 NetScaler Gateway 以及用于 Citrix Virtual Apps（以前称为 XenApp）Web Interface 和 XML 代理的负载均衡?

是的。NetScaler VPX Express 包含完整的 NetScaler Standard 功能。从 NetScaler 12.0–56.20 版本开始，Citrix 修改了 VPX Express 的行为。

NetScaler VPX Express 是否包含所有 NetScaler 标准功能？它是否包含 NetScaler Gateway 以及用于 Citrix Virtual Apps Web Interface 和 XML 代理的负载均衡?

从 NetScaler 12.0–56.20 版本开始，VPX Express 提供 NetScaler Standard Edition 功能集，但 Gateway 功能除外。在 12.0–56.20 版本之前，VPX Express 包含标准版中的所有功能。

NetScaler VPX Express 需要许可证吗?

随着新的 NetScaler VPX Express 版本（12.0–56.20 及更高版本）的发布，VPX Express 是免费的，无需安装许可证文件，并且不附带任何承诺。如果您已经拥有 VPX Express 许可证，则会保留之前的 VPX Express 行为。如果移除 VPX Express *许可证文件* 并使用 12.0–56.20 及更高版本，则新的 VPX Express 行为将生效。

NetScaler VPX Express 许可证会过期吗?

对于新的 VPX Express，不会。没有许可证，也没有到期日期。如果您已经拥有 VPX Express 许可证，则该许可证在下载后一年过期。

NetScaler VPX Express 是否包含五个免费的 NetScaler Gateway 并发许可证?

是的，如果您拥有 VPX Express 许可证。

客户可以下载的 NetScaler VPX Express 数量是否有限制?

五个。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler VPX Express 是否支持与 NetScaler MPX 设备相同的加密密码?

对于普遍可用性，NetScaler 设备上支持的所有相同强加密密码在 NetScaler VPX 和 NetScaler VPX Express 上均可用。它受相同的进出口法规约束。

我可以为 NetScaler VPX Express 提交技术支持案例?

不可以。需要零售版 NetScaler VPX 许可证（例如 VPX-10、VPX-200、VPX-1000、VPX-3000）才能提交技术支持案例。但是，NetScaler VPX Express 用户可以自由使用 NetScaler VPX 知识中心，并使用 Z 讨论论坛向社区寻求帮助。

NetScaler VPX Express 可以升级到零售版本吗?

是的。只需购买您需要的零售版 NetScaler VPX 许可证，然后将相应的许可证应用到 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 VMware ESX 和 ESXi 3.5 或更高版本。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。

如何从 vSphere 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 命令行界面的内置访问。此外，您可以使用任何 SSH 或 Telnet 客户端访问命令行界面。您可以在 SSH 或 Telnet 客户端中使用 NetScaler VPX 的 NSIP 地址。

如何访问 NetScaler VPX GUI?

要访问 NetScaler VPX GUI，请在任何浏览器的地址字段中键入 NetScaler VPX 的 NSIP，例如 `http://NSIP address`。

安装在同一 VMware ESX 上的两个 NetScaler VPX 实例能否配置为高可用性设置?

可以，但不建议这样做。硬件故障会影响两个 NetScaler VPX 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

运行在两个不同 VMware ESX 系统上的两个 NetScaler VPX 实例能否配置为高可用性设置?

可以。在高可用性设置中建议这样做。

对于 VMware，NetScaler VPX 是否支持接口相关事件?

不支持。不支持接口相关事件。

对于 VMware，NetScaler VPX 是否支持标记 VLAN?

是的。NetScaler 标记 VLAN 从 11.0 及更高版本开始在 NetScaler VPX 上受支持。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?

不支持。NetScaler VPX 不支持链路聚合和 LACP。链路聚合必须在 VMware 级别配置。

如何访问 NetScaler VPX 文档?

文档可从 NetScaler VPX GUI 获取。登录后，选择“**文档**”选项卡。

容量规划或大小调整

NetScaler VPX 的预期性能如何?

NetScaler VPX 提供了良好的性能。有关使用 NetScaler VPX 可实现的特定性能级别，请参阅 NetScaler VPX 数据表。

鉴于服务器 CPU 功率各不相同，我们如何估算 NetScaler 实例的最大性能?

使用更快的 CPU 可以带来更高的性能（最高可达许可证允许的最大值），而使用较慢的 CPU 则肯定会限制性能。

NetScaler VPX 带宽或吞吐量限制：仅入站流量，还是入站和出站流量?

NetScaler VPX 带宽限制仅对进入 NetScaler 的流量强制执行，无论其是请求流量还是响应流量。这意味着 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和响应流量不同。对于 NetScaler 而言，来自端点（请求流量）和来自源服务器（响应流量）的流量都是“入站”流量（即进入 NetScaler 的流量）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

同一服务器上是否可以运行多个 NetScaler VPX 实例?

可以。但是，请确保物理服务器具有足够的 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。

如果物理服务器上运行了多个 NetScaler VPX 实例，每个 NetScaler VPX 实例的最低硬件要求是什么?

每个 NetScaler VPX 实例必须分配 2 GB 物理 RAM、20 GB 硬盘空间和 2 个 vCPU。对于关键部署，我们不建议为 VPX 使用 2 GB RAM，因为系统在内存受限的环境中运行。这可能会导致扩展、性能或稳定性相关问题。建议使用 4 GB RAM 或 8 GB RAM。

注意：

NetScaler VPX 是一种对延迟敏感的高性能虚拟设备。为了提供其预期的性能，该设备需要 vCPU 预留、内存预留以及主机上的 vCPU 绑定。此外，主机上必须禁用超线程。如果主机不满足这些要求，则会出现高可用性故障转移、VPX 实例内 CPU 峰值、访问 VPX CLI 迟缓、pit boss 守护程序崩溃、数据包丢失和吞吐量低等问题。

确保每个 VPX 实例都满足预定义条件。

我可以在同一服务器上托管 NetScaler VPX 和其他应用程序吗?

是的。例如，NetScaler VPX、Citrix Virtual Apps Web Interface 和 Citrix Virtual Apps XML Broker 都可以虚拟化并在同一服务器上运行。为获得最佳性能，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。

CPU 核心增加对单个 NetScaler VPX 实例性能的影响?

是的，添加 CPU 核心可以提高 NetScaler VPX 性能，前提是 NetScaler VPX 实例已获得额外 vCPU 的许可。NetScaler VPX 最多支持 20 个 vCPU（适用于 41 Gbps - 100 Gbps 性能），具体取决于配置和性能层级。更多的 vCPU 有助于提高吞吐量，尤其是在高性能场景中。但是，性能影响还取决于网络驱动程序（例如，PCI 直通或 SR-IOV）和特定工作负载等因素。有关不同 VPX 性能层级支持的 vCPU 数量的信息，请参阅 NetScaler VPX 数据表。

NetScaler VPX 在空闲时 CPU 占用率超过 90% 的原因?

这是正常行为，NetScaler 设备也表现出相同的行为。要查看 NetScaler VPX CPU 利用率的真实程度，请在 NetScaler CLI 中使用 stat CPU 命令，或从 NetScaler GUI 查看 NetScaler VPX CPU 利用率。NetScaler 数据包处理引擎始终在“寻找工作”，即使没有工作可做。因此，它会尽一切努力控制 CPU 并且不释放它。在仅安装了 NetScaler VPX 的服务器上，（从管理程序的角度来看）结果

© 1997–2026 Citrix Systems, Inc. All rights reserved.

看起来像是 NetScaler VPX 正在占用整个 CPU。从“NetScaler 内部”（通过使用 CLI 或 GUI）查看 CPU 利用率，可以了解 NetScaler VPX CPU 容量的使用情况。

系统要求

NetScaler VPX 的最低硬件要求是什么?

下表说明了 NetScaler VPX 的最低硬件要求。

类型	要求
处理器	有关 VPX 平台的处理器要求，请参阅 NetScaler VPX 支持的处理器 表。
内存	最低 2 GB。但是，建议使用 4 GB。
磁盘	最小 20 GB 硬盘。
管理程序	Citrix Hypervisor 5.6 或更高版本、VMware ESX/ESXi 3.5 或更高版本，或带有 Hyper-V 的 Windows Server 2008 R2
网络连接	最低 100 Mbps，建议 1 Gbps。
网卡	使用与您的管理程序兼容的网卡。有关更多信息，请参阅 NetScaler VPX 支持的网卡。

注意：

- 对于关键部署，NetScaler VPX 最好使用 4 GB 内存。如果使用 2 GB 内存，NetScaler VPX 将在内存非常受限的环境中运行。这可能会导致扩展性、性能或稳定性方面的问题。
- 从 NetScaler 13.1 版本开始，VMware ESXi 管理程序上的 NetScaler VPX 实例支持 AMD EPYC 处理器。

有关系统要求的更多信息，请参阅 NetScaler VPX 数据表。

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”，它们将客户操作系统运行的敏感或特权 CPU 指令捕获到管理程序。这简化了在管理程序上托管客户操作系统（NetScaler VPX 的 BSD）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VT-x 有多常见?

许多服务器在 BIOS 设置中默认禁用虚拟化辅助功能（例如 VT-x 或 AMD-V）。在断定无法运行 NetScaler VPX 之前，请检查 BIOS 配置。如果虚拟化支持被禁用，您可能需要在 BIOS 中启用它，以确保您的服务器可以正常运行 NetScaler VPX 等虚拟化应用程序。

NetScaler VPX 是否有硬件兼容性列表 (HCL)?

只要服务器支持 Intel VT-x，NetScaler VPX 就可以在任何与底层 Hypervisor 兼容的服务器上运行。有关支持平台的完整列表，请参阅 Hypervisor HCL。

NetScaler VPX 基于哪个版本的 NetScaler OS?

NetScaler VPX 基于 NetScaler 9.1 或更高版本。

既然 NetScaler VPX 在 BSD 上运行，它能否在安装了 BSD Unix 的服务器上原生运行?

不能。NetScaler VPX 需要 Hypervisor 才能运行。有关 Hypervisor 支持的详细信息，请参阅 NetScaler VPX 数据表。

其他技术常见问题

具有多个网卡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，其限制为四个通道和七个虚拟接口。对于 VMware，NetScaler VPX 中不支持静态链路聚合，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 设备实现相比是否有任何变化?

支持 MBF，其行为与 NetScaler 设备相同。Hypervisor 基本上将从 NetScaler VPX 接收到的所有数据包切换到外部，反之亦然。

NetScaler VPX 升级过程如何执行?

升级方式与 NetScaler 设备相同：下载内核文件并使用 install ns 或 GUI 中的升级实用程序。

闪存和磁盘空间如何分配 我们可以更改它吗?

必须为每个 NetScaler VPX 实例分配至少 2 GB 内存。NetScaler VPX 磁盘映像大小为 20 GB，以满足可维护性需求，包括存储多达 4 GB 的核心转储以及日志和跟踪文件的空间。虽然可以生成更小

© 1997–2026 Citrix Systems, Inc. All rights reserved.

的磁盘映像，但目前没有计划这样做。`/flash` 和 `/var` 都位于同一个磁盘映像中。出于兼容性目的，它们被保留为单独的文件系统。

以下值表示 NetScaler VPX 实例上特定目录分配的磁盘空间：

- /flash 为 965M
- /var 为 14G

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以增加 NetScaler VPX 实例上的空间?

是的。从 NetScaler 13.1 版本 21.x 及更高版本开始，您可以通过添加第二个磁盘来增加 NetScaler VPX 实例上的磁盘空间。当您连接第二个磁盘时，“/var/crash”目录会自动挂载到此磁盘上。第二个磁盘用于存储核心文件和日志。用于存储核心文件和日志文件的现有目录将继续像以前一样工作。

注意：

在降级 NetScaler 设备时进行外部备份，以避免数据丢失。

有关如何在云上将新的硬盘驱动器 (HDD) 连接到 NetScaler VPX 实例的信息，请参阅以下内容：

- Azure 文档

  注意：

  要在部署在 Azure 上的 VPX 实例上连接辅助磁盘，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 VM 大小。

- AWS 文档
- GCP 文档

警告：

将新 HDD 添加到 VPX 后，处理已移动到新 HDD 的文件的某些脚本可能会在以下情况下失败：

如果您使用“link”shell 命令为已移动到新 HDD 的文件创建硬链接。
所有此类命令都必须替换为“ln -s”以使用符号链接。此外，请相应地修改失败的脚本。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler VPX 的版本编号以及与其他版本的互操作性如何?

NetScaler VPX 的版本编号与 9.1. Cl (classic) 和 9.1. Nc (nCore) 版本类似，例如 9.1_97.3.vpx、9.1_97.3.nc 和 9.1_97.3.cl。

NetScaler VPX 可以与 NetScaler 设备一起构成高可用性设置?

不支持此配置。

NetScaler VPX 中可见的所有接口是否与 Hypervisor 上的接口数量直接相关?

否。您可以通过 NetScaler VPX 配置实用程序添加最多七个接口（VMware 为 10 个），而 Hypervisor 上只有一个物理 NIC。

为什么 NetScaler VPX 上的半虚拟化 (PV) 接口显示为 1G 接口 (`1/x`)，即使底层物理接口是 10G？这是否意味着最大吞吐量限制为 1 Gbps?

在 NetScaler VPX 上，所有半虚拟化 NIC（例如 VMXNET3）都显示为 `1/x`，无论其背后的物理 NIC 速度如何。这是预期行为，并不意味着吞吐量上限为 1 Gbps。实际吞吐量由底层物理 NIC 的容量决定，因此由 10G NIC 支持的 PV 接口可以提供远超 1 Gbps 的吞吐量。

Citrix Hypervisor XenMotion、VMware VMotion 或 Hyper-V 实时迁移能否用于移动 NetScaler VPX 的活动实例?

NetScaler VPX 不支持 XenMotion 或 Hyper-V 实时迁移。从 NetScaler 12.1 版本开始支持 VMotion。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

fix

This is the content for the sample heading topic. It is hidden from the main table of contents but remains accessible via links.

© 1997–2026 Citrix Systems, Inc. All rights reserved.