

使用 vRealize Network Insight

VMware vRealize Network Insight 5.0

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

**威睿信息技术（中国）有
限公司**
北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

版权所有 © 2022 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

目录

1	关于 vRealize Network Insight 用户指南	9
2	入门	10
	简介	10
	主页	12
	导航	13
	设置	14
3	在 vRealize Network Insight 中添加数据源	15
	受支持的产品和版本	17
	添加 vCenter Server	20
	添加 VMware NSX Manager	21
	添加 VMware NSX-T Manager	22
	NSX-T 事件	26
	添加 VMware SD-WAN	29
	添加 VMware Cloud on AWS	30
	添加 VMware Cloud on AWS - vCenter	30
	添加 VMware Cloud on AWS - NSX Policy Manager	31
	VMware Cloud on AWS 部署模型	32
	添加 Amazon Web Services	32
	添加主 AWS 帐户	33
	添加标准 AWS 数据源	38
	AWS: 地域阻止支持	41
	添加 Azure 订阅	42
	启用 NSG 流日志	43
	添加 VMware PKS	43
	添加 Kubernetes	44
	添加 OpenShift	45
	添加 Palo Alto Networks Panorama	46
	添加 Check Point 管理服务器	46
	添加 Cisco ASA	47
	添加 Fortinet FortiManager	48
	添加 Dell OS10 交换机	49
	在 Dell OS10 交换机上启用遥测	49
	添加 Huawei 6800/7800/8800 系列	51
	添加 Cisco ACI	52
	为 NetFlow 和 sFlow 添加物理流收集器	53

- 添加 Log Insight 53
- 添加 Infoblox 55
- 添加 F5 BIG-IP 56
- 添加 ServiceNow 58
 - 添加 ServiceNow 59
- 添加新的通用路由器或交换机 74
 - 编辑通用路由器或交换机 75

4 从 vRealize Network Insight 中删除数据源 76

5 迁移数据源 77

6 配置 vRealize Network Insight 设置 78

- 查看系统运行状况 79
- 配置数据保留时间间隔 79
- 配置 IP 属性和子网 80
 - 导入 DNS 映射文件 80
 - 配置子网与 VLAN 之间的映射 80
 - 配置东西向 IP 81
 - 配置南北向 IP 81
- 配置事件和通知 81
 - 查看和编辑系统事件 82
 - 编辑用户定义的事件 86
 - 查看平台运行状况事件 88
 - 通知 88
- 配置身份与访问管理 91
 - 配置 LDAP 91
 - 配置 VMware Identity Manager (vIDM) 92
 - 配置用户管理 94
- 配置日志 95
 - 查看和导出审核日志 95
 - 设置 Syslog 配置 96
- 配置邮件服务器 96
- 配置 SNMP 陷阱目标 97
- 管理许可证 98
 - 添加并更改许可证 99
- 配置自动刷新时间间隔 99
- 配置用户会话超时 100
- 添加 Google Maps API 密钥 100
- 查看审核日志 101
- 加入或退出客户体验提升计划 102

- 查看安装的运行状况 102
- 启用支持通道 102
- 管理磁盘利用率 103
- 查看节点详细信息 103
- 创建支持包 104
- 了解收集器和平台负载的容量 104

7 创建和扩展群集 106

- 创建群集 106
- 扩展群集 107

8 查看实体详细信息 108

- 查看 vRealize Network Insight 系统（NI 系统）详细信息 109
- 查看平台虚拟机详细信息 109
- 查看收集器虚拟机详细信息 110
- 查看 VMware vCenter 数据源详细信息 110
- 查看 PCI 合规性详细信息 110
 - 导出为 PDF 111
- Object Missing 112
- 查看负载均衡器详细信息 112
- 查看虚拟机详细信息 112
- 查看 NSX Manager 详细信息 113
- 查看虚拟服务器详细信息 114
- 查看池成员详细信息 115
- 查看 Microsoft Azure 详细信息 116
- 查看 VeloCloud 企业详细信息 118
 - 查看 VeloCloud Edge 详细信息 119
- 查看 SD-WAN 和 Edge SD-WAN 应用程序详细信息 120
- 查看“流洞察”详细信息 120
- 查看微分段详细信息 124
- 查看应用程序详细信息 125
- 分析 - 异常值检测 126
 - 如何检测离群虚拟机 126
- 分析：静态和动态阈值 128
 - 配置阈值和警示 128
 - 查看“阈值配置”页面 129

9 查看实体拓扑 131

- 虚拟机拓扑 131
- 主机拓扑 132
- VXLAN 拓扑 132

VLAN 拓扑	133
NSX Manager 拓扑	134
Edge 数据收集	134
在 vRealize Network Insight 中查看 NSX 对象的审核信息	135
10 使用看板项	139
看板项	139
插针类型	139
看板	141
插接板的共享和协作	144
将插接板设置为主页	146
复制插接板	146
11 F5 作为负载均衡器	148
NSX-V 作为负载均衡器	149
12 使用网络和安全性的	150
网络可见性	150
路径拓扑	150
监控 BGP 的各种状态	159
到 Internet 的路径	159
安全性	160
跨 vCenter NSX	160
Palo Alto 网络	161
Cisco ASA 防火墙	164
Check Point 防火墙	166
安全组	169
基于策略的 VPN	170
NSX 分布式防火墙非活动规则	170
Fortinet 防火墙	171
13 在 vRealize Network Insight 中配置流	172
启用 IPFIX 配置	172
VDS 和 DVPG 上的 IPFIX 配置	172
VMware NSX IPFIX 配置	174
对物理服务器的流支持	175
在物理设备中配置 NetFlow 收集器	176
扩充流和 IP 端点	180
搜索物理到物理流	181
查看已阻止的流和受保护的流	182
网络地址转换 (NAT)	183

NAT 流支持 - 示例	184
VMware Cloud on AWS 个流	185
创建 VPC 流日志	186
将流记录从 F5 发送到 vRealize Network Insight 收集器	187
创建 IPFIX 收集器池	187
创建 IPFIX 日志目标	188
创建日志发布者	188
创建 iRule	189
将 iRule 添加到虚拟服务器	193
创建路由条目	194
14 Kubernetes 和 VMware PKS 范围和流信息	195
15 使用微分段	196
分析应用程序	196
在环形视图中查看微分段和流数据	197
在网格视图中查看微分段和流数据	199
手动创建应用程序	200
应用程序发现	202
添加已发现的应用程序	203
VMware Cloud on AWS: 规划和微分段	206
16 建议的防火墙规则	208
导出规则	210
NSX DFW 通用项目	211
将 CSV 导出的配置保存为属性模板	213
导出并应用 Kubernetes 网络策略	214
17 使用搜索查询	216
搜索查询	217
Azure 搜索查询	222
Cisco ACI 实体	223
Fortinet 搜索查询	226
使用 Infoblox DNS 数据扩充流	227
Kubernetes 实体的常见搜索查询	227
负载均衡器相关的示例搜索查询	229
NSX 防火墙规则的搜索查询	229
VMware SD-WAN 搜索查询	230
VMware Cloud on AWS for AWS 实体	230
高级查询	231
时间控制	235

搜索结果 235
筛选器 236
vCenter 标记 237

18 规划 vRealize Network Insight 的灾难恢复 240

灾难恢复场景示例 241

19 故障排除 243

常见的数据源错误 243
无法启用 DFW IPFIX 244

20 使用 vRealize Network Insight 计划将应用程序迁移到 VMware Cloud on AWS 247

如何获取 NSX Manager 的 CSP 刷新令牌 248
如何获取 vCenter 凭据 252
计算网关防火墙规则 254

关于 vRealize Network Insight 用户指南

1

vRealize Network Insight 用户指南提供了有关使用 vRealize Network Insight 的信息。

目标读者

这些信息适用于负责使用 vRealize Network Insight 的管理员或专家。本信息的目标读者为熟悉企业管理应用程序和数据中心操作且具有丰富经验的虚拟机管理员。

本章讨论了以下主题：

- 简介
- 主页
- 导航
- 设置

简介

















vRealize Network Insight 为软件定义的网络和安全保护提供智能操作。可帮助客户在多云环境中构建高度可用且安全的优化网络基础架构。vRealize Network Insight 加快了微分段规划和部署，实现了跨虚拟和物理网络的可见性，并提供了操作视图来管理和扩展 VMware NSX 部署。

将整个数据中心视为由实体及其关系组成。例如，一个虚拟机是一个实体，而虚拟机所属的主机则是另一个实体。vRealize Network Insight 提供了有关数据中心的众多实体的可见性和信息。

表 2-1.

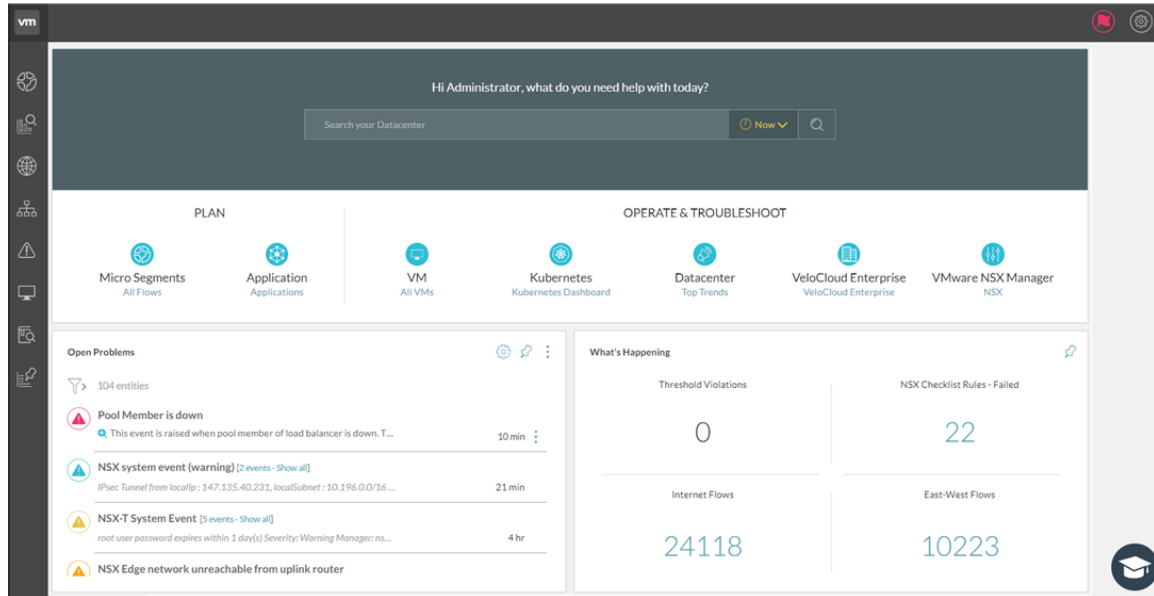
实体	描述
 	主机
 	问题
 	NSX 防火墙
 	虚拟机
	vSphere Distributed Switch

表 2-1. (续)

实体	描述
	物理交换机
	虚拟端口组
	Cisco 结构扩展器
	逻辑交换机
	数据存储
	物理网卡
	安全组
	刀片
	路由器
	VLAN
	虚拟机组
	配置更改
	路由器接口
	故障排除
	网络访问转换 (NAT)
	邮件服务器

主页

VMware vRealize Network Insight 主页提供了整个数据中心所发生情况的快速摘要。它使您能够快速访问数据中心的 vRealize Network Insight 的重要组成部分。



主页分为以下几部分：

搜索栏

通过搜索栏，您能够在数据中心网络（及其相应的实体）中进行搜索。您可以使用搜索栏搜索数据中心中可用的实体。搜索栏位于主页的顶部。

根据您的要求，可以按照以下时间线选项执行搜索：

- **预设：** 使用此选项，您可以缩小诸如 last week、last 3 days、last 24 hours、yesterday、today、last 2 hours、last hour 和 now（当前时间）等预设的搜索结果范围。
- **于：** 使用此选项，您可以缩小特定日期和时间的搜索结果范围。
- **区间：** 使用此选项，您可以在特定时间间隔之间搜索数据。

“规划”部分

- **微分段：** 您可以根据所有虚拟机之间的流来规划网络的微分段。
- **应用程序：** 您可以定义应用程序并分析其流，然后规划其安全性。


“操作和故障排除”部分

操作和故障排除部分为以下组件提供可见性、衡量指标和分析：

- 虚拟机 (VM)
- VLAN 网络

- 数据中心
- NSX 安全组
- VMware NSX

未决问题

未决问题部分提供平台在数据中心中找到的严重事件的快速概览。所有类似事件都进行了分组。使用**全部显示**可查看所有事件。要查看事件的更多详细信息，请单击  (**查看详细信息**)。您可以使用“配置事件”图标导航到“系统事件”页面并配置它们。

此外，如果在特定事件的**更多选项**下单击**配置事件**选项，则可以直接导航到特定事件的编辑视图以修改配置。

当前状态

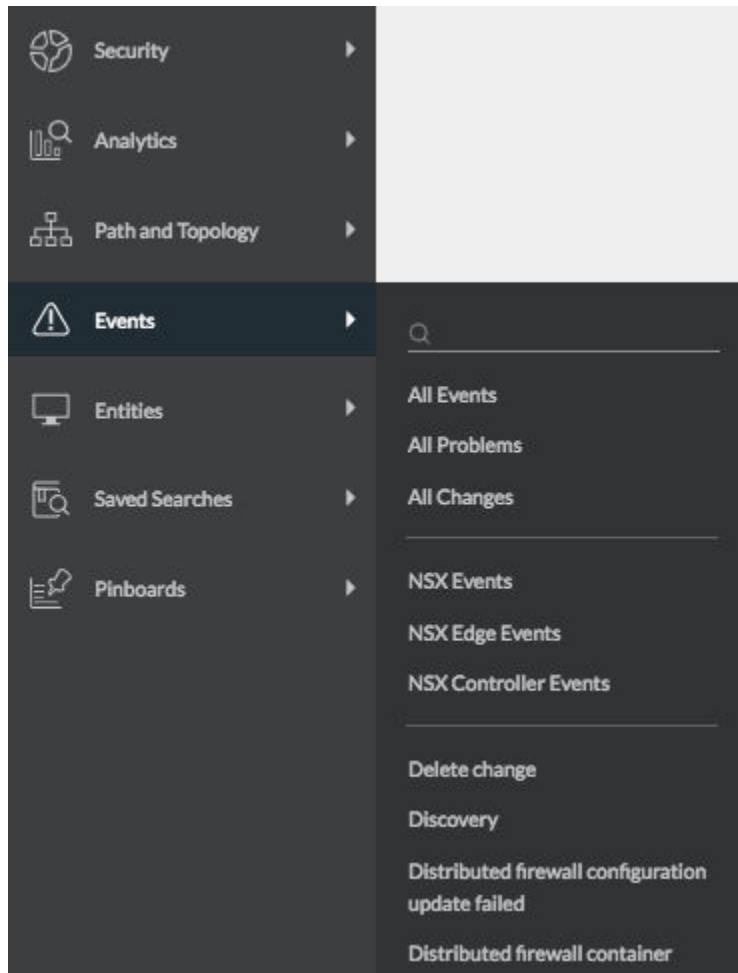
当前状态部分提供数据中心中超高值属性的快速视图。要查看属性详细信息，请单击特定属性的计数。此部分还包含左侧的筛选器（用于筛选事件），以及“全部展开”和“全部折叠”按钮（用于查看事件的详细信息）。

导航

vRealize Network Insight 包含左侧的导航面板，可帮助用户快速导航到关键产品功能（如安全性、拓扑、实体、事件和已保存的搜索），而无需键入任何搜索查询。

导航面板包含以下选项：

- 安全性：提供以下选项：
 - 规划安全性：允许您分析环境中的流并帮助规划环境中的微分段。您可以选择所有实体或选择某个特定实体，然后选择要分析所选实体的时间段。
 - 应用程序：允许您使用自定义搜索在 vRealize Network Insight 中创建应用程序。创建应用程序后，您可以对其进行相应的规划。
 - PCI 合规性：“PCI 合规性”仪表板有助于仅在 NSX 环境中根据 PCI 要求评估合规性。
- 路径和拓扑：允许您查看数据中心的多个实体的虚拟机到虚拟机路径或拓扑。
- 事件：允许您查看环境中的事件（更改和问题）。还提供一个事件类型列表，您可以快速查看特定类型的事件。
- 实体：显示环境中存在的所有不同类型实体的列表。单击给定列表中的任意实体类型可查看该类型的所有实体的列表。使用实体列表上方的文本框可以根据输入的文本缩小列表范围。
- 已保存的搜索：显示之前已保存的搜索。



设置

设置页面提供了用于管理数据提供程序、用户和通知的控件。

转到设置页面：

- 1 在主页的右上角，单击“配置文件”图标。
- 2 单击设置。此时将显示设置页面。

在 vRealize Network Insight 中添加数据源

3

数据源使应用程序能够从数据中心的某些方面收集数据。其范围从 NSX 安装到物理设备（例如 Cisco™ 机箱 4500 和 Cisco™ N5K）。

要添加数据源，请执行以下操作：

- 1 在设置下的安装和支持页面中，单击帐户和数据源。
- 2 单击添加新源。
- 3 选择一个帐户或一种源类型。
- 4 在表单上提供所需的信息。
- 5 单击验证。
- 6 为数据源输入“昵称”和“备注”（如果有）。
- 7 单击提交以将数据源添加到环境中。

对于每个数据源，可以查看以下详细信息：

属性	描述
类型 (昵称)	显示数据源的名称。
IP 地址/FQDN	显示数据源的 IP 地址或 FQDN 详细信息。
上次收集时间	显示上次收集数据的收集时间。
已发现的虚拟机数	显示已为该数据源发现的虚拟机的数量。 注 仅当数据源为 vCenter 或 AWS 源时，才会填充“已发现的虚拟机数”列。
收集器虚拟机	显示已向其添加数据源的收集器的名称。如果所有列出的数据源都已添加到同一收集器上，则此列不可见。仅当数据源存在于不同的收集器上时，才能查看此列。
已启用	指示数据源是否已启用。
操作	显示用于编辑和删除数据源的选项。

vRealize Network Insight 提供了以下功能，以便可以轻松地访问数据源的信息。

- 通过使用列标题上方的搜索栏，可以按名称、IP 地址或收集器虚拟机名称搜索数据源。

- 可以在**类型 (昵称)** 列中按不同数据源筛选信息。
- 可以在**收集器虚拟机**列中按各种收集器虚拟机筛选信息。
- 数据源按其类型和昵称的字母顺序排序。

对于添加的每个数据源，可以查看以下信息：

- **全部**：显示所有可用的数据源。
- **有问题**：显示 vRealize Network Insight 已发现问题的数据源。
- **带有建议**：为需要其他信息的数据源显示从 vRealize Network Insight 自动生成的建议。
- **已禁用**：显示已禁用的数据源。

本章讨论了以下主题：

- [受支持的产品和版本](#)
- [添加 vCenter Server](#)
- [添加 VMware NSX Manager](#)
- [添加 VMware NSX-T Manager](#)
- [添加 VMware SD-WAN](#)
- [添加 VMware Cloud on AWS](#)
- [添加 Amazon Web Services](#)
- [添加 Azure 订阅](#)
- [添加 VMware PKS](#)
- [添加 Kubernetes](#)
- [添加 OpenShift](#)
- [添加 Palo Alto Networks Panorama](#)
- [添加 Check Point 管理服务器](#)
- [添加 Cisco ASA](#)
- [添加 Fortinet FortiManager](#)
- [添加 Dell OS10 交换机](#)
- [添加 Huawei 6800/7800/8800 系列](#)
- [添加 Cisco ACI](#)
- [为 NetFlow 和 sFlow 添加物理流收集器](#)
- [添加 Log Insight](#)
- [添加 Infoblox](#)
- [添加 F5 BIG-IP](#)

- 添加 [ServiceNow](#)
- 添加新的通用路由器或交换机

受支持的产品和版本

vRealize Network Insight 支持多个产品和版本。

数据源	版本/型号	连接协议	权限/特权
Amazon Web Services（仅限企业许可证）	不适用	HTTPS	请参见《vRealize Network Insight 用户指南》中的“添加标准 AWS 数据源”部分。
Arista 交换机	7050TX、7250QX、7050QX-32S、7280SE-72	SSH、SNMP	只读用户 只读 SNMP 用户
Azure 订阅	不适用	HTTPS	您必须具有以下权限： Microsoft.Resources/subscriptions/read Microsoft.Compute/virtualMachines/read Microsoft.Network/virtualNetworks/read Microsoft.Network/networkSecurityGroups/read Microsoft.Network/networkInterfaces/read Microsoft.Network/applicationSecurityGroups/read Microsoft.Storage/storageAccounts/read Microsoft.Storage/storageAccounts/listkeys/action Microsoft.Network/networkWatchers/queryFlowLogStatus/action 或者，为了方便使用，您可以添加 Storage Account Key Operator Service Role、Network Contributor 和 Reader 权限。
Brocade 交换机	VDX 6740、VDX 6940、MLX、MLXe	SSH、SNMP	只读用户 只读 SNMP 用户
Check Point 防火墙	Check Point R80、R80.10	HTTPS、SSH	请参见《vRealize Network Insight 用户指南》中的“Check Point 防火墙”部分。

数据源	版本/型号	连接协议	权限/特权
Cisco ACI	3.2	HTTPS (到 APIC 控制器) SNMP (到 APIC 控制器和 ACI 交换机)	要通过 HTTPS 连接到 APIC 控制器 REST API, 需要有权访问所有租户且具有只读权限的用户 对于 SNMP, 用户需要只读权限。
Cisco ASA	运行操作系统 9.4 的 X 系列	SSH、SNMP	用户应有权切换到启用模式。用户的密码应与用于 Cisco ASA 启用模式的密码相同。
Cisco Catalyst	3000、3750、4500、6000、6500	SSH、SNMP	具有默认特权级别 15 的只读 SNMP 用户
Cisco Nexus	3000、5000、6000、7000、9000	SSH、SNMP	只读用户 只读 SNMP 用户
Cisco UCS (Unified Computing System)	B 系列刀片服务器、C 系列机架服务器、机箱、Fabric Interconnect	UCS Manager: HTTPS UCS Fabric: SSH、SNMP	只读用户 只读 SNMP 用户
Dell 交换机	FORCE10 MXL 10、FORCE10 S6000、S4048、Z9100、S4810、PowerConnect 8024、Dell OS10	SSH、SNMP	只读用户 只读 SNMP 用户
Fortinet FortiManager	6.0.1	HTTPS	用户必须具有： <ul style="list-style-type: none"> 至少能够访问所有 ADOM 和策略软件包的受限用户角色。 已从命令行界面 (CLI) 启用 rpc-permit read 访问权限。
F5 BIG-IP	12.1.2 及更高版本	HTTPS、SSH、SNMP	用户至少必须具有客户机角色。此外, 还必须启用 TMSH, 并且必须有权访问所有分区。F5 BIG-IP 支持路由和负载平衡。
HP	HP Virtual Connect Manager 4.41、HP OneView 3.0	HP OneView 3.0: HTTPS HP Virtual Connect Manager 4.41: SSH	只读用户
Huawei Cloud Engine	6800、7800、8800	SSH、SNMP	只读用户 只读 SNMP 用户
Infoblox	Infoblox NIOS 版本 8.0、8.1、8.2	HTTPS	具有 API 接口访问权限的只读用户 DNS 对象类型的只读权限, 如下所示: <ul style="list-style-type: none"> 权限类型 - DNS 资源 - A 记录、DNS 区域、DNS 视图
Juniper 交换机	EX3300、QFX 51xx 系列 (JunOS v12 和 v15, 无 QFabric)	Netconf、SSH、SNMP	只读用户 只读 SNMP 用户

数据源	版本/型号	连接协议	权限/特权
Kubernetes	<ul style="list-style-type: none"> ■ NSX-T 2.3.1 上的 1.12 ■ NSX-T 2.3.2 上的 1.12 ■ NSX-T 2.3.2 上的 1.13 	HTTPS	用户必须具有群集管理员角色且具有读取权限。
Palo Alto 网络	Panorama 7.0.x、7.1、8.x、9.0	HTTPS	用户必须具有管理员角色且具有 XML API 访问权限。有关详细信息，请参见《vRealize Network Insight 用户指南》中的“Palo Alto Networks”部分。
ServiceNow	London	HTTPS	用户必须具有管理员角色
VMware SD-WAN	VeloCloud Orchestrator 和 Edge 版本 3.3.1 及更高版本	HTTPS	用户必须拥有具有以下任一权限的帐户角色： <ul style="list-style-type: none"> ■ 超级用户 ■ 标准管理员 ■ 客户支持人员
VMC on AWS - vCenter	M5P2 及更高版本 注 仅支持基于 NSX-T 的 VMware Cloud on AWS SDDC。	HTTPS	用户必须具有以下权限： <ul style="list-style-type: none"> ■ 云管理员：添加数据源并启用 IPFIX。
VMC on AWS - NSX Manager	M5P2 及更高版本 注 仅支持基于 NSX-T 的 VMware Cloud on AWS SDDC。	HTTPS	用户必须具有以下任一权限： <ul style="list-style-type: none"> ■ 组织成员.管理员：添加数据源并启用 IPFIX。 ■ 组织成员.云管理员：添加数据源并启用 IPFIX。 ■ 组织成员.VMware Cloud on AWS（所有角色）：添加数据源并启用 IPFIX。 ■ 组织成员.云审核员：添加数据源。
VMware Identity Manager	3.3 及更高版本	HTTPS	用户必须具有管理员角色。
VMware PKS	NSX-T 2.3.1 上的 PKS 1.3.2 NSX-T 2.3.2 上的 PKS 1.3.2		用户必须具有群集管理员角色且具有读取权限。
VMware NSX Manager (VMware NSX-V)	支持的版本	SSH、HTTPS	请参见《vRealize Network Insight 用户指南》中的“Edge 数据收集”部分。
VMware NSX-T Manager	2.4。 有关其他支持的版本，请参见支持的版本	HTTPS	只读用户

数据源	版本/型号	连接协议	权限/特权
VMware vRealize Log Insight	支持的版本	HTTPS	具有安装、配置和管理内容包权限的 API 用户
VMware vSphere	支持的版本 对于 IPFIX，所需的 VMware ESXi 版本为： <ul style="list-style-type: none"> ■ 5.5 Update 2（内部版本 2068190）及更高版本 ■ 6.0 Update 1b（内部版本 3380124）及更高版本 ■ VMware VDS 5.5 及更高版本 注 VMware Tools 应安装在数据中心内的所有虚拟机上，才能识别虚拟机到虚拟机的路径。	HTTPS	只读用户 配置和使用 IPFIX 所需的特权 具有特权的 vCenter Server 凭据： Distributed Switch: Modify dvPort group: Modify vCenter Server 中的预定义角色必须具有在根级别分配的以下特权，且这些特权需要传播到子角色： System.Anonymous System.Read System.View global.settings

添加 vCenter Server

可以将 vCenter Server 作为数据源添加到 vRealize Network Insight。

可以将多个 vCenter Server 添加到 vRealize Network Insight 以开始监控数据。

步骤

- 1 单击**添加 vCenter**。
- 2 单击**添加新源**，然后自定义选项。

选项	操作
源类型	在下拉菜单中选择 vCenter Server 系统。
IP 地址/FQDN	输入 vCenter Server 的 IP 地址或完全限定域名。
用户名	输入具有以下特权的用户名： <ul style="list-style-type: none"> ■ 分布式交换机: 修改 ■ dvPort 组: 修改 有关所需的额外特权的信息，请参见安装指南中的“vCenter 特权”部分。
密码	输入 vRealize Network Insight 软件用于访问 vCenter Server 系统的密码。

- 3 单击**验证**。

如果发现的虚拟机数超出平台和/或收集器节点的容量，则验证将失败。增加平台的块大小或创建群集之后，才可以添加数据源。

带流和不带流的情况下每个块大小的指定容量如下所示：

块大小	虚拟机	流状态
大型	6k	已启用
大型	10k	已禁用
中型	3k	已启用
中型	6k	已禁用

4 选择在此 vCenter 上启用 Netflow (IPFIX) 以启用 IPFIX。

有关 IPFIX 的详细信息，请参见“在 VDS 和 DVPD 上启用 IPFIX 配置”部分。

5 将高级数据收集源添加到 vCenter Server 系统。

6 单击提交以添加 vCenter Server 系统。vCenter Server 系统将显示在主页上。

添加 VMware NSX Manager

可以在 vRealize Network Insight 中将 NSX-V 添加为数据源。

前提条件

确认以下项：

- 您拥有正确的权限。有关权限的信息，请参见《安装 vRealize Network Insight》中的“受支持的产品和版本”部分。
- 您具有所需的特权。有关特权的信息，请参见《安装 vRealize Network Insight》中的“特权”部分。
- 您已经将 vCenter 添加为数据源。

步骤

- 1 在设置页面上，单击帐户和数据源。
- 2 单击添加源。
- 3 在 VMware Manager 下，单击 VMware NSX Manager。
- 4 在添加新 VMware NSX Manager 帐户或源页面中，提供所需的信息。

选项	操作
收集器 (代理) 虚拟机	从下拉菜单中选择一个收集器虚拟机。
主 VMware vCenter	<p>选择要添加到 vRealize Network Insight 中的 vCenter。</p> <p>注 确保 vCenter 和关联的 NSX Manager 数据源添加到同一收集器。否则，您将看不到被拒绝的流（启用 NSX IPFIX 时），并且“应用的防火墙规则”可能在某些流中不可用。</p>
IP 地址/FQDN	输入 IP 地址或 FQDN 详细信息。

选项	操作
用户名	输入用户名。
密码	输入密码。

5 单击**验证**。

6 （可选）如果要收集 NSX Controller 数据，则选中**启用 NSX Controller 数据收集**复选框。

如果选择此选项，vRealize Network Insight 将收集控制器数据，例如逻辑路由器接口、路由、逻辑交换机 mac 表、vtep 记录、控制器群集状态和角色。数据收集由 NSX Central CLI 或控制器-SSH 会话完成。

7 （可选）如果要收集 NSX Edge 数据，则选中**启用 NSX Edge 数据收集**复选框。

有关 NSX Edge 数据收集的信息，请参见 [Edge 数据收集](#)。

8 （可选）如果要收集 IPFIX 流，则选中**启用 IPFIX**复选框。

如果选择此选项，vRealize Network Insight 会接收来自 NSX-V 的 DFW IPFIX 流。有关启用 IPFIX 的详细信息，请参见[启用 VMware NSX-V IPFIX](#)。

9 （可选）如果要收集延迟衡量指标数据，则选中**启用虚拟基础架构延迟**复选框。

如果选择此选项，vRealize Network Insight 会接收来自 NSX 主机的延迟衡量指标。此选项仅适用于 NSX-V 6.4.5 及更高版本。确保在收集器上打开端口 1991，以接收来自 ESXi 主机的延迟数据。

10 在**昵称**文本框中，输入昵称。

11 （可选）在**备注**文本框中，您可以根据需要添加备注。

12 单击**提交**。

添加 VMware NSX-T Manager

VMware NSX-T 旨在处理具有异构端点和技术堆栈的新兴应用程序框架和架构。除了 vSphere 外，这些环境还可能包括其他管理程序、容器、裸机和公有云。vRealize Network Insight 支持虚拟机由 vCenter 管理的 NSX-T 部署。

注意事项

- vRealize Network Insight 仅支持 vCenter 管理 ESXi 主机的 NSX-T 设置。请确保在 NSX-T 中将 vCenter 添加为计算管理器。

注 在将 NSX-T 添加为数据源之前，应先将计算管理器添加为 vRealize Network Insight 中的数据源。

- vRealize Network Insight 支持 NS 组、NSX-T 防火墙规则、IPSet、NSX-T 逻辑端口、NSX-T 逻辑交换机和 NSX-T 分布式防火墙 IPFIX 流、分段、组以及基于策略的 VPN。

- vRealize Network Insight 支持 NSX-V 和 NSX-T 部署。在查询中使用 NSX 时，结果将包括 NSX-V 和 NSX-T 实体。NSX Manager 会列出 NSX-V Manager 和 NSX-T Manager。NSX 安全组会列出 NSX-T 和 NSX-V 安全组。如果使用 NSX-V 或 NSX-T 而不是 NSX，则仅显示这些实体。此逻辑同样适用于防火墙规则、IPSet 和逻辑交换机等实体。
- 通过使用 NSX-T 2.4 版本，vRealize Network Insight 支持 NSX 声明性策略管理，从而通过结果驱动的策略声明简化并自动化网络和安全配置。

注 安全组的微分段基于 NSX 策略数据完成。但是，如果没有相应的 NSX 策略组，独立 NS 组将包含在微分段分析中。有关 NS 组的更多详细信息，请参见 [NSX-T 产品文档](#)。

将 NSX-T Manager 添加为数据源

以下是将 NSX-T Manager 添加为数据源的必备条件：

- 至少将一个与 NSX-T 关联的 vCenter 添加到 vRealize Network Insight。
- 建议将与 NSX-T 关联的所有 vCenter 都添加为 vRealize Network Insight 中的数据源。
- 确保在分布式防火墙 (DFW) 的排除列表中没有逻辑交换机。如果此列表中有任何逻辑交换机，则不会报告连接到这些逻辑交换机的任何虚拟机的流。

要添加 NSX-T Manager，请执行以下操作：

- 1 在 **帐户和数据源** 页面的 **设置** 下，单击 **添加源**。
- 2 在 **选择帐户或数据类型** 页面的 **VMware Manager** 下，选择 **VMware NSX-T Manager**。
- 3 提供用户凭据。

注

- 如果在一个 NSX-T 部署中有多个管理节点，则只能在 vRealize Network Insight 中添加一个节点作为数据源，或者使用 VIP（在这些节点中）。如果添加多个管理节点，则 vRealize Network Insight 可能无法正常运行。
 - 如果不需要 IPFIX，则用户必须是具有审核级别权限的本地用户。但是，如果需要 IPFIX，则用户必须具有以下审核级别权限之一：**企业管理员**、**网络工程师** 或 **安全工程师**。
-
- 4 选择 **启用 IPFIX** 以更新 NSX-T 上的 IPFIX 设置。选择此选项后，vRealize Network Insight 会接收来自 NSX-T 的 DFW IPFIX 流。有关启用 IPFIX 的更多信息，请参见 [启用 VMware NSX-T DFW IPFIX](#)。

注

- DFW IPFIX 在 NSX-T 的标准版本中不受支持。
 - vRealize Network Insight 不支持 NSX-T 交换机 IPFIX 流。
-
- 5 （可选）如果要收集延迟衡量指标数据，则选中 **启用虚拟基础架构延迟** 复选框。如果选择此选项，vRealize Network Insight 将接收来自 NSX-T 的延迟衡量指标 (VTEP - VTEP)。此选项仅适用于 NSX-T 2.5（Firestar 版本）及更高版本。确保在收集器上打开端口 1991，以接收来自 ESXi 节点的延迟数据。

查询示例

以下是一些与 NSX-T 相关的查询示例：

表 3-1. NSX-T 查询

查询	搜索结果
<code>NSX-T Manager where VC Manager=10.197.53.214</code>	此特定 VC Manager 已添加为计算管理器的 NSX-T Manager。
<code>NSX-T Logical Switch</code>	列出 vRealize Network Insight 实例中存在的所有 NSX-T 逻辑交换机，包括交换机是系统创建还是用户创建的相关详细信息。
<code>NSX-T Logical Ports where NSX-T Logical Switch = 'DB-Switch'</code>	列出属于该特定 NSX-T 逻辑交换机 DB-Switch 的 NSX-T 逻辑端口。
<code>VMs where NSX-T Security Group = 'Application-Group'</code> 或 <code>VMs where NSGroup = 'Application-Group'</code>	列出该特定安全组 Application-Group 中的所有虚拟机。
<code>NSX-T Firewall Rule where Action='ALLOW'</code>	列出其操作设置为 ALLOW 的所有 NSX-T 防火墙规则。
<code>NSX-T Firewall Rule where Destination Security Group = 'CRM-Group'</code>	列出 CRM-Group 是目标安全组的防火墙规则。结果包括直接目标安全组和间接目标安全组。
<code>NSX-T Firewall Rule where Direct Destination Security Group = 'CRM-Group'</code>	列出 CRM-Group 是目标安全组的防火墙规则。结果仅包括直接目标安全组。
<code>VMs where NSX-T Logical Port = 'App_Port-Id-1'</code>	列出具有该特定 NSX-T 逻辑端口的所有虚拟机。
<code>NSX-T Transport Zone</code>	列出 VLAN 和覆盖网络传输区域以及与其关联的相应详细信息（包括传输节点的类型）。 注 vRealize Network Insight 不支持将 KVM 作为数据源。
<code>NSX-T Router</code>	列出 TIER 1 和 TIER 0 路由器。单击结果中显示的路由器可查看与其关联的更多详细信息，包括 NSX-T Edge 群集和 HA 模式。

表 3-2. NSX 策略查询

<code>NSX Policy Segment</code>	列出 vRealize Network Insight 实例中存在的所有 NSX 策略分段。
<code>NSX Policy Manager</code>	列出 vRealize Network Insight 实例中存在的所有 NSX Policy Manager。
<code>NSX Policy Group</code>	列出 vRealize Network Insight 实例中存在的所有 NSX 策略组。
<code>NSX Policy Firewall</code>	列出 vRealize Network Insight 实例中存在的所有 NSX 策略防火墙。
<code>NSX Policy Firewall Rule</code>	列出 vRealize Network Insight 实例中存在的所有 NSX 策略防火墙规则。

表 3-2. NSX 策略查询（续）

NSX Policy Firewall Rule where Action = 'ALLOW'	列出操作设置为 ALLOW 的所有 NSX 策略防火墙规则。
NSX Policy Based VPN	列出 vRealize Network Insight 实例中存在的所有基于 NSX 策略的 VPN。

注 如果将 NSX-T 2.4 和 VMware Cloud on AWS 添加为 vRealize Network Insight 中的数据源，那么要获取 NSX-T 实体，您必须在查询中添加 **SDDC type = ONPREM** 筛选器。例如，

NSX Policy Based VPN where Tier0 = ‘’ and SDDC Type = ‘ONPREM’。

支持 NSX-T 衡量指标

下表显示了当前支持 NSX-T 衡量指标的 vRealize Network Insight 实体，以及在相应实体仪表板上显示这些衡量指标的小组件。

表 3-3.

实体	实体仪表板上的小组件	支持的 NSX-T 衡量指标
逻辑交换机	逻辑交换机数据包衡量指标 逻辑交换机字节衡量指标	Multicast and Broadcast Rx Multicast and Broadcast Tx Unicast Rx Unicast Tx Dropped Rx Dropped Tx Rx Packets (Total) Tx Packets (Total)
逻辑端口	逻辑端口数据包衡量指标 逻辑端口字节衡量指标	Multicast and Broadcast Rx Multicast and Broadcast Tx Unicast Rx Unicast Tx Rx Packets (Total) Tx Packets (Total)
路由器接口	路由器接口衡量指标	Rx Packets Tx Packets Dropped Rx Packets Dropped Tx Packets Rx Bytes Tx Bytes
防火墙规则	防火墙规则衡量指标	Hit Count Flow Bytes Flow Packets

以下是一些有关 NSX-T 衡量指标的查询示例：

■ `nsx-t logical switch where Rx Packet Drops > 0`

此查询列出丢弃的已接收数据包计数大于 0 的所有逻辑交换机。

- `nsx-t logical port where Tx Packet Drops > 0`

此查询列出丢弃的已传输数据包计数大于 0 的所有逻辑端口。

- `top 10 nsx-t firewall rules order by Connection count`

此查询基于连接计数 (Hit Count) 列出前 10 个防火墙规则。

NSX-T 事件

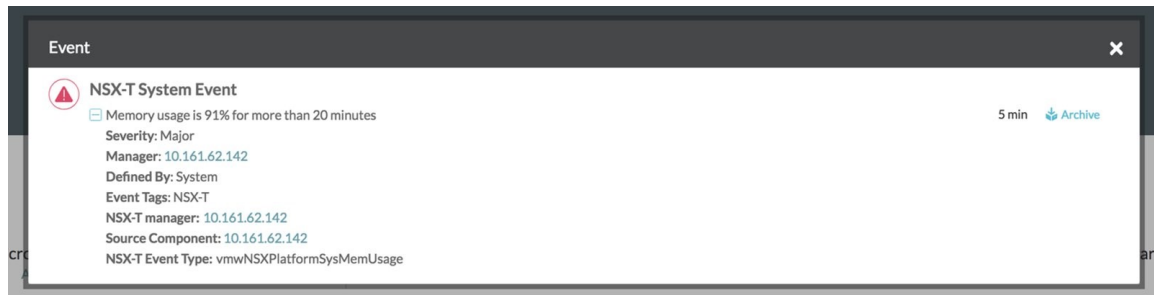
通过 vRealize Network Insight，可以查看 NSX-T 2.3 及更高版本的 NSX-T 事件。

源组件是引发事件的源。它可以是管理器、控制器或 Edge。

以下 NSX-T 事件由 vRealize Network Insight 生成：

系统事件

- `NSX-T Edge Node has no manager connectivity`
- `NSX-T Edge Node has no controller connectivity`
- `NSX-T Edge Node's controller connectivity degraded`



自定义事件

- `NSX-T MTU Mismatch`

注 在 TO 的上行链路和上行链路设备的对应接口之间存在不匹配。

- `Routing Advertisement disabled for Tier-1 router`
- `No Uplink Connectivity for Tier-1 router`

注 Tier-1 路由器未连接到 Tier-0。

- `NSX-T IPFIX Switch data is not supported in Network Insight`

注 vRealize Network Insight 不支持 IPFIX 流。将从 NSX-T 交换机 IPFIX 配置文件所使用的 NSX-T 交换机收集器配置文件中移除 vRealize Network Insight 收集器虚拟机 IP 地址。

- `No vtep is available on the transport node`

- NSX-T Vlan misconfiguration on Tier 0 router
- NSX-T VMs included in the firewall exclusion list
- No transport zone attached on the transport node

NSX-T 和 PKS 事件

vRealize Network Insight 中支持的 NSX-T 和 PKS 事件列表。

事件名称	事件源	描述
vmwNSXPlatformSysCpuUsage	NSX-T 系统事件	管理器和 Edge 设备上的 CPU 使用情况 (Equinox)。
vmwNSXPlatformSysDiskUsage	NSX-T 系统事件	管理器和 Edge 设备上 /var/log 分区的磁盘空间使用情况 (Equinox)。
vmwNSXPlatformSysMemUsage	NSX-T 系统事件	管理器和 Edge 设备上的内存使用情况 (Equinox)。
vmwNSXPlatformSysConfigDiskUsage	NSX-T 系统事件	管理器和 Edge 设备上 /config 分区的磁盘使用情况 (Flash)。
vmwNSXPlatformSysVarDumpDiskUsage	NSX-T 系统事件	管理器和 Edge 设备上 /var/dump 分区的磁盘使用情况 (Firestar)。
vmwNSXPlatformSysRepositoryDiskUsage	NSX-T 系统事件	管理器和 Edge 设备上 /repository 分区的磁盘使用情况 (Firestar)。
vmwNSXPlatformSysRootDiskUsage	NSX-T 系统事件	管理器和 Edge 设备上根分区的磁盘使用情况 (Firestar)。
vmwNSXPlatformSysTmpDiskUsage	NSX-T 系统事件	管理器和 Edge 设备上 tmp 分区的磁盘使用情况 (Firestar)。
vmwNSXPlatformSysImageDiskUsage	NSX-T 系统事件	管理器和 Edge 设备上 /image 分区的磁盘使用情况 (Firestar)。
vmwNSXDhcpPoolUsageOverloadedEvent	NSX-T 系统事件	DHCP 池过载/正常 (Firestar)。
vmwNSXDhcpPoolLeaseAllocationFailedEvent	NSX-T 系统事件	DHCP 池租约分配失败/成功 (Firestar)。
vmwNSXPlatformPasswordExpiryStatus	NSX-T 系统事件	管理器密码过期 (Flash)。
vmwNSXPlatformCertificateExpiryStatus	NSX-T 系统事件	管理器证书过期 (Flash)。
vmwNSXRoutingBgpNeighborStatus	NSX-T 系统事件	BGP 邻居状态 (Equinox)。
vmwNSXVpnTunnelState	NSX-T 系统事件	VPN 隧道启动/关闭 (Equinox)。
vmwNSXVpnL2TunnelStatus	NSX-T 系统事件	L2 VPN 会话启动/关闭 (Equinox)。
vmwNSXVpnIkeSessionStatus	NSX-T 系统事件	IKE 会话启动/关闭 (Equinox)。
vmwNSXDnsForwarderStatus	NSX-T 系统事件	DNS 转发器状态 (Flash)。
vmwNSXClusterNodeStatus	NSX-T 系统事件	群集节点状态 (Flash)。

事件名称	事件源	描述
vmwNSXFabricCryptoStatus	NSX-T 系统事件	Edge 加密 mux 驱动程序未通过/通过 Known_Answer_Tests(KAT) (Flash)。
NSX-T Edge 节点未连接快照器	vRNI 计算	vRNI (NSX-T Edge 节点无法与任何控制器通信)。
NSX-T Edge 节点未连接管理器	vRNI 计算	NSX-T Edge 节点已断开与管理器的连接。
NSX-T Edge 节点的控制器连接已降级	vRNI 计算	NSX-T Edge 节点无法与一个或多个控制器通信。
NSX-T MTU 不匹配	vRNI 计算	在第 0 层逻辑路由器的接口上配置的 MTU 与同一 L2 网络中上行链路交换机/路由器的接口不匹配。这可能会影响网络性能。
NSX-T 虚拟机包含在防火墙排除列表中	vRNI 计算	一个或多个虚拟机未受到 NSX-T DFW 防火墙的保护。vRealize Network Insight 将不会收到这些虚拟机的 IPFIX 流。
第 0 层路由器上的 NSX-T VLAN 配置错误	vRNI 计算	通信中断，因为第 0 层路由器上行链路端口上的 VLAN 与外部网关上的 VLAN 不同。
无上行链路连接	vRNI 计算	NSX-T 第 1 层逻辑路由器已与第 0 层路由器断开连接。无法从外部访问此路由器下的网络，反之亦然。
传输节点上未连接任何传输区域	vRNI 计算	传输节点上未连接任何传输区域。导致虚拟机断开连接。
传输节点上没有可用的 VTEP	vRNI 计算	将从传输节点中删除所有 VTEP。导致虚拟机断开连接。
已禁用路由通告	vRNI 计算	已对 NSX-T 第 1 层逻辑路由器禁用路由通告。无法从外部访问此路由器下的网络。
管理器磁盘利用率不正常	NSX-T 系统事件 (vmwNSXPlatformSysDiskUsage)	
BGP 邻居已关闭	NSX-T 系统事件 (vmwNSXRoutingBgpNeighborStatus)	BGP 邻居关闭时需要警示。
BGP 邻居已启动	NSX-T 系统事件 (vmwNSXRoutingBgpNeighborStatus)	邻居启动时清除警报。
存储使用情况超过 X	NSX-T 系统事件 (vmwNSXPlatformSysDiskUsage)	针对所有设备虚拟机 (MP、CCP) 或传输节点 (Edge、主机) 发出“存储超过 X - 事件”警报。

事件名称	事件源	描述
内存使用情况超过 X	NSX-T 系统事件 (vmwNSXPlatformSysMemUsage)	针对所有设备虚拟机（MP、CCP）或传输节点（Edge、主机）发出“内存超过 X - 事件”警报。
CPU 使用情况超过 X	NSX-T 系统事件 (vmwNSXPlatformSysCpuUsage)	针对所有设备虚拟机（MP、CCP）或传输节点（Edge、主机）发出“CPU 超过 X - 事件”警报。

添加 VMware SD-WAN

您可以在 vRealize Network Insight 中将 VMware SD-WAN by VeloCloud 添加为数据源。

前提条件

确保以下事项：

- 您拥有正确的权限，可以添加数据源。有关权限的信息，请参见[受支持的产品和版本](#)。
- 使用 VeloCloud Orchestrator 和 Edge 版本 3.3.1 或更高版本。
- 您至少添加了一个 VMware SD-WAN 许可证。
- 没有添加其他 VMware SD-WAN 作为数据源。

步骤

- 1 在**设置**页面上，单击**帐户和数据源**。
- 2 单击**添加源**。
- 3 在**SD-WAN**下，单击**VeloCloud**。
- 4 在**添加新 VeloCloud 帐户或源**页面中，提供所需的信息。

选项	操作
收集器 (代理) 虚拟机	从下拉菜单中选择一个收集器虚拟机。
VCO URL	输入要添加为数据源的 VCO URL。
用户名	输入用户名。
密码	输入密码。

- 5 单击**验证**。
- 6 在**昵称**文本框中，输入昵称。
- 7 （可选）在**备注**文本框中，您可以根据需要添加备注。
- 8 单击**提交**。

后续步骤

必须在端口 2055 上对所有配置文件和 Edge 启用 NetFlow。要了解如何启用 NetFlow 收集，请在 VMware SD-WAN 的[编辑数据源](#)页面中，单击[查看说明](#)。

注 您会在注意：应对所有配置文件和 Edge 启用 Netflow 收集中看到[查看说明](#)选项。

添加 VMware Cloud on AWS

vRealize Network Insight 仅针对企业许可证用户提供 VMware Cloud on AWS 支持。可以将 VMware Cloud on AWS (vCenter) 或 VMware Cloud on AWS (NSX Policy Manager) 添加为数据源。

添加 VMware Cloud on AWS - vCenter

可以将 VMware Cloud on AWS - vCenter 添加为数据源。

前提条件

- 您必须具有 Cloud Administrator 特权。
- 获取将 NSX Manager 添加为数据源的凭据
 - a 登录到 VMWare Cloud Services 控制台。
 - b 单击[我的服务](#)下的 **VMware Cloud on AWS**。
 - c 单击所需 SDDC 的名称。
 - d 在[设置](#)选项卡中，复制 **vCenter FQDN** 选项卡中的 **vCenter FQDN**。从[默认 vCenter 用户帐户](#)选项卡中，复制用户凭据。

步骤

- 1 单击[设置](#) > [帐户和数据源](#) > [添加源](#)。
- 2 在 **VMware Cloud on AWS** 下，单击 **VMware Cloud on AWS - vCenter**。
- 3 在[添加 VMware Cloud on AWS - VMware vCenter](#) 页面中，
 - 选择收集器虚拟机。
 - 提供已从 VMware Cloud Services 检索的 vCenter FQDN。
 - 提供已从 VMware Cloud Services 检索的用户凭据。
- 4 单击[验证](#)。
- 5 为数据源输入[昵称](#)和[备注](#)（如果有），然后单击[提交](#)。
- 6 添加 [VMware Cloud on AWS - NSX Policy Manager](#)。

添加 VMware Cloud on AWS - NSX Policy Manager

可以将 VMware Cloud on AWS - NSX Policy Manager 添加为数据源。

前提条件

- 您必须具有 Cloud Administrator 特权。
- 获取将 NSX Manager 添加为数据源的凭据
 - a 登录到 VMWare Cloud Services 控制台。
 - b 单击**我的服务**下的 **VMware Cloud on AWS**。
 - c 单击所需 SDDC 的名称。
 - d 在**设置**选项卡中，复制 **vCenter FQDN** 选项卡中的 **vCenter FQDN**。从**默认 vCenter** 用户帐户选项卡中，复制用户凭据。

步骤

- 1 执行以下操作之一：
 - 如果您尚未添加 VMware Cloud on AWS - vCenter，
 - a 添加 [VMware Cloud on AWS - vCenter](#)。
 - b 单击**添加 NSX Manager**。
 - 如果您已添加 VMware Cloud on AWS - vCenter，
 - a 单击**设置 > 帐户和数据源 > 添加源**。
 - b 在 **VMware Cloud on AWS** 下，单击 **VMware Cloud on AWS - NSX Manager**。
- 2 在**添加新的 VMC NSX Manager 帐户**页面中，
 - 选择相应的 vCenter。

将基于选择的 vCenter 自动选择收集器。VMware Cloud on AWS。您必须将 NSX Manager 添加到相应 vCenter 的收集器虚拟机。
 - 提供 IP 地址和 CSP 刷新令牌。
 - 提供用户凭据。
- 3 单击**验证**。
- 4 如果要收集 DFW 的 IPFIX 流，则选择**启用 DFW IPFIX**。

注 如果未满足以下条件，会弹出错误消息：

- 要启用 DFW IPFIX，需要具有 Cloud Administrator 特权。
 - VMware Cloud on AWS NSX Manager 仅允许将四个收集器添加到其 DFW IPFIX 收集器配置文件。另请参见[无法启用 DFW IPFIX](#)。
-

- 5 为数据源输入**昵称**和**备注**（如果有），然后单击**提交**

VMware Cloud on AWS 部署模型

vRealize Network Insight 支持以下部署模型：

- 收集器部署在 VMware Cloud on AWS 中：
 - a 在此部署模型中，收集器作为工作负载部署在 VMware Cloud on AWS 中的计算网关中。平台在 SDDC 内部部署版本中进行部署。
 - b 管理网关的防火墙规则允许通过 HTTPS 与 VMware Cloud on AWS vCenter 和 VMware Cloud on AWS NSX Manager 通信。
 - c 收集器使用通过 VPN 或 Direct Connect 的现有通信机制与平台进行通信。

上述部署模型的必备条件如下：

- 应存在管理网关防火墙规则，以允许 vRealize Network Insight 收集器通过 HTTPS (443) 调用 vCenter 和 NSX Manager API。
- 网关防火墙中应存在计算网关规则，以允许收集器与内部部署平台或 SaaS 平台进行通信。

注

- 对于 VMware Cloud on AWS 中的单节点 SDDC，应将代理虚拟机的 CPU 资源预留设置为 1251 MHz。当前，作为版本一部分提供的代理 OVA 将资源预留设置为 2048 MHz。在 SDDC vCenter 中导入此 OVA 后，修改代理虚拟机的设置，以使用允许的最大 CPU 预留，即 1251 MHz。

添加 Amazon Web Services

您可以在 vRealize Network Insight 中将 Amazon Web Services (AWS) 添加为数据源。

您可以将以下两种类型的 AWS 帐户添加为数据源。

- 主 AWS 帐户和链接 AWS 帐户
- 标准 AWS 帐户

主 AWS 帐户和链接 AWS 帐户

主 AWS 帐户（组织帐户或付款人帐户）具有组织级访问权限，可通过 API 调用发现和列出您组织中的所有链接 AWS 帐户。

您组织中添加到主帐户的所有 AWS 帐户都称为链接帐户。有关详细信息，请参见 [ListAccount](#)。

主 AWS 帐户必须承担链接 AWS 帐户的角色，才能访问和控制链接 AWS 帐户的资源。所有链接 AWS 帐户必须通过角色 ARN 信任主 AWS 帐户。有关角色的详细信息，请参见 [AssumeRole](#)。

将主 AWS 帐户添加为数据源时，会自动将所有链接 AWS 帐户添加为数据源。

标准 AWS 帐户

标准 AWS 帐户没有主帐户和链接帐户关系。

添加主 AWS 帐户

通过添加主 AWS 帐户，您可以在 vRealize Network Insight 中自动添加组织中的所有链接 AWS 帐户。

前提条件

- 为 AWS API 访问配置防火墙。
- 创建主帐户策略和链接帐户策略。
- 在 AWS 中创建角色。
- 在主 AWS 帐户中创建用户。
- 获取您在 AWS 控制台中创建的 Amazon 访问密钥 ID。有关更多详细信息，请参见 <http://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html>。
- 获取链接 AWS 帐户的角色 Amazon 资源名称 (ARN)。请参见 [Amazon 资源名称 \(ARN\)](#) 和 [AWS 服务命名空间](#)。

步骤

- 1 登录到 vRealize Network Insight。
- 2 转到 **设置 > 帐户和数据源 > 添加源**。
- 3 在“公有云”部分下，单击 **Amazon Web Services**。
- 4 选择“收集器 (代理) 虚拟机”。
- 5 输入 Amazon 访问密钥 ID 和相应的私有访问密钥。

vRealize Network Insight 需要 15 到 20 分钟的时间来收集您的 AWS 帐户数据。

- 6 单击 **验证**。

如果发现的虚拟机数超出平台或收集器节点的容量，则验证将失败。增加平台的块大小或创建群集之后，才可以添加数据源。带流和不带流的情况下每个块大小的指定容量如下所示：

块大小	虚拟机	流状态
大型	6k	已启用
大型	10k	已禁用
中型	3k	已启用
中型	6k	已禁用

- 7 完成 AWS 帐户验证后，选择 **自动添加链接帐户** 选项。
- 8 在 **角色 ARN** 中，输入链接 AWS 帐户的角色 Amazon 资源名称以信任主 AWS 帐户。
- 9 为数据源输入 **昵称** 和 **备注**。
- 10 单击 **提交**。

vRealize Network Insight 会验证角色 ARN 并添加帐户。

创建主帐户策略和链接帐户策略

您必须为主 Amazon Web Services (AWS) 帐户创建主帐户策略，并为所有链接 AWS 帐户创建链接帐户策略。您可以在 AWS 中使用这些策略管理访问权限。

您可以将 AWS 策略附加到 IAM 身份，例如“用户”或“角色”。有关详细信息，请参见[策略和权限](#)。

步骤

- 1 在 AWS 控制台中，转到 **IAM > 策略 > 创建策略**。
- 2 在**创建策略**页面中，单击 **JSON** 选项卡。

3 在 JSON 文本框中，输入策略

选项	描述
添加主帐户策略 <hr/> 注 您必须在主 AWS 帐户中添加主帐户策略。	<pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iam:ListAccountAliases"], "Resource": ["*"] }, { "Effect": "Allow", "Action": ["ec2:Describe*"], "Resource": "*" }, { "Action": ["logs:Describe*", "logs:Get*", "logs:TestMetricFilter", "logs:FilterLogEvents"], "Effect": "Allow", "Resource": "*" }, { "Effect": "Allow", "Action": ["organizations:ListAccounts"], "Resource": "*" }, { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "<Role ARNs>" }] }</pre>
添加链接帐户 <hr/> 注 您必须在主 AWS 帐户中添加的所有链接帐户中添加链接帐户策略。	<pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iam:ListAccountAliases"], "Resource": ["*"] }, { "Effect": "Allow", "Action": [</pre>

选项	描述
	<pre> "ec2:Describe*"], "Resource": "*" }, { "Action": ["logs:Describe*", "logs:Get*", "logs:TestMetricFilter", "logs:FilterLogEvents"], "Effect": "Allow", "Resource": "*" }] }</pre>

4 单击**查看策略**。

5 在**查看策略**部分中，输入策略名称，然后单击**创建策略**。

后续步骤

依次登录所有链接帐户，并添加角色以信任要添加到 vRealize Network Insight 的主 AWS 帐户，然后连接链接帐户策略。要创建角色并附加链接帐户策略，请参见在 [AWS 中创建角色](#)。

注 如果在所有链接帐户中创建的角色已包含标准策略权限并信任主帐户，则跳过此步骤。

在 AWS 中创建角色

您可以创建 AWS 角色，以信任要添加到 vRealize Network Insight 的帐户。

前提条件

创建您在 [创建主帐户策略和链接帐户策略](#) 中创建的所有链接帐户策略的列表

步骤

- 1 在 AWS 控制台中，转到**服务 > IAM > 角色 > 创建角色**。
- 2 在**创建角色**页面中，单击**另一个 AWS 帐户**。
- 3 在**帐户 ID** 文本框中，输入要信任的主帐户 ID，然后单击**下一步: 权限**。
- 4 搜索并选择所有链接帐户策略，然后单击**下一步: 标记**。
- 5 在**检查**部分中，输入**角色名称**，然后单击**创建角色**。

后续步骤

在主 [AWS 帐户](#) 中创建用户。

在主 AWS 帐户中创建用户

您必须在 AWS 帐户中创建一个用户以获取 Amazon 访问密钥 ID 以及对应的私有访问密钥，以便用于在 vRealize Network Insight 中添加数据源。

步骤

- 1 登录到 AWS 控制台。
- 2 转到**服务 > IAM > 用户 > 添加用户**。
- 3 在**添加用户**页面上，输入**用户名**，选择**编程访问**复选框，然后单击**下一个权限**。
- 4 在**设置权限**组下，单击**直接附加现有策略**，然后搜索并选择您之前创建的帐户策略。
 - 对于主 AWS 帐户，选择主帐户策略。
 - 对于标准 AWS 帐户，选择标准帐户策略。
- 5 单击**下一步: 标记 > 下一步: 检查**。
- 6 单击**创建分支**。
- 7 记下**访问密钥 ID**和**私有访问密钥**。

后续步骤

- 添加主 AWS 帐户。
- 添加标准 AWS 数据源。

为 AWS API 访问配置防火墙

收集器虚拟机需要一个 URL 列表才能访问 AWS。

- AWS 可以在多个区域中部署。存在与不同区域关联的单独 URL。如果您不知道区域或服务，请为 URL 提供通配符条目，如 `*.amazonaws.com`。

注 该通配符条目不适用于中国区域。

如果您希望对单独的 URL 进行精细访问，则有以下 4 个基于区域的服务：

- 除 GovCloud 和中国以外的区域
 - `ec2.<REGION>.amazonaws.com`
 - `logs.<REGION>.amazonaws.com`
 - `sts.<REGION>.amazonaws.com`
 - `iam.amazonaws.com`

GovCloud 区域

- `ec2.us-gov-west-1.amazonaws.com`
- `logs.us-gov-west-1.amazonaws.com`
- `sts.us-gov-west-1.amazonaws.com`

- iam.us-gov.amazonaws.com

中国（北京）区域

- ec2.cn-north-1.amazonaws.cn
- logs.cn-north-1.amazonaws.com.cn
- sts.cn-north-1.amazonaws.com.cn
- iam.cn-north-1.amazonaws.com.cn

可以基于 AWS 区域使用 REGION 的以下任何值：

区域名称	区域
美国东部（俄亥俄州）	us-east-2
美国东部（北弗吉尼亚州）	us-east-1
美国西部（北加利福尼亚州）	us-west-1
美国西部（俄勒冈州）	us-west-2
亚太地区（孟买）	ap-south-1
亚太地区（首尔）	ap-northeast-2
亚太地区（新加坡）	ap-southeast-1
亚太地区（悉尼）	ap-southeast-2
亚太地区（东京）	ap-northeast-1
加拿大（中部）	ca-central-1
欧盟（法兰克福）	eu-central-1
欧盟（爱尔兰）	eu-west-1
欧盟（伦敦）	eu-west-2
南美（圣保罗）	sa-east-1
Gov Cloud	us-gov-west-1
中国（北京）	cn-north-1

添加标准 AWS 数据源

要添加 AWS 数据源，请执行以下操作：

前提条件

- 为 AWS API 访问配置组织防火墙。请参见 [为 AWS API 访问配置防火墙](#)。
- 为要添加到 vRealize Network Insight 中的 AWS 帐户创建标准帐户策略。要创建策略，请参见 [创建标准帐户策略](#)。

- 在标准 AWS 帐户中创建用户。要在 AWS 中创建用户，请参见在主 [AWS 帐户中创建用户](#)。

步骤

- 1 转到 **设置 > 帐户和数据源 > 添加源**。
- 2 在公有云下，单击 **Amazon Web Services**。
- 3 选择“收集器 (代理) 虚拟机”。
- 4 输入 Amazon 访问密钥 ID 和相应的私有访问密钥。

注 Amazon 访问密钥 ID 是一个包含对应私有访问密钥的 20 位字符串。有关更多详细信息，请参见 <http://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html>。

注 要将 AWS Gov Cloud 区域添加为数据源，请通过使用有权访问 Gov Cloud 区域的 AWS 帐户中的建议策略来创建 AWS IAM 用户。使用新创建帐户的访问密钥和私有密钥，将数据源添加到 vRealize Network Insight。

此过程需要约 15 到 20 分钟来添加和显示您的帐户数据。

- 5 单击 **验证**。

如果发现的虚拟机数量超出平台和/或代理节点的容量，则验证失败。增加平台的块大小或创建群集之后，才可以添加数据源。

带流和不带流的情况下每个块大小的指定容量如下所示：

块大小	虚拟机	流状态
大型	6k	已启用
大型	10k	已禁用
中型	3k	已启用
中型	6k	已禁用

- 6 验证 AWS 帐户后，可以选择 **启用流数据收集** 以获取更深入的洞察。

在主 AWS 帐户中创建用户

您必须在 AWS 帐户中创建一个用户以获取 Amazon 访问密钥 ID 以及对应的私有访问密钥，以便用于在 vRealize Network Insight 中添加数据源。

步骤

- 1 登录到 AWS 控制台。
- 2 转到 **服务 > IAM > 用户 > 添加用户**。
- 3 在 **添加用户** 页面上，输入 **用户名**，选择 **编程访问** 复选框，然后单击 **下一个权限**。
- 4 在 **设置权限** 组下，单击 **直接附加现有策略**，然后搜索并选择您之前创建的帐户策略。
 - 对于主 AWS 帐户，选择主帐户策略。

- 对于标准 AWS 帐户，选择标准帐户策略。

5 单击 **下一步: 标记 > 下一步: 检查**。

6 单击 **创建分支**。

7 记下 **访问密钥 ID** 和 **私有访问密钥**。

后续步骤

- 添加主 [AWS 帐户](#)。
- 添加标准 [AWS 数据源](#)。

创建标准帐户策略

您必须为标准 AWS 帐户创建标准帐户策略。通过此策略，您可以在 AWS 中管理访问。

您可以将 AWS 策略附加到 IAM 身份，例如“用户”或“角色”。有关详细信息，请参见[策略和权限](#)。

步骤

- 1 在 AWS 控制台中，转到 **IAM > 策略 > 创建策略**。
- 2 在 **创建策略** 页面中，单击 **JSON** 选项卡。

3 在 JSON 文本框中，输入以下帐户策略：

选项	描述
添加标准帐户策略 <hr/> 注 您必须在要添加为数据源的标准 AWS 帐户中添加标准帐户策略。	<pre> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iam:ListAccountAliases"], "Resource": ["*"] }, { "Effect": "Allow", "Action": ["ec2:Describe*"], "Resource": "*" }, { "Action": ["logs:Describe*", "logs:Get*", "logs:TestMetricFilter", "logs:FilterLogEvents"], "Effect": "Allow", "Resource": "*" }] }</pre>

4 单击查看策略。

5 在查看策略部分中，输入策略名称，然后单击创建策略。

后续步骤

- 在主 AWS 帐户中创建用户。

AWS：地域阻止支持

由于在企业防火墙上严格实施地域阻止策略，因此 AWS API 调用仅限于特定的 AWS 区域。vRealize Network Insight 支持 AWS 环境的地域阻止策略。

要在 vRealize Network Insight 中启用地域阻止策略，请执行以下操作：

步骤

- 1 在添加 AWS 数据源页面上，输入 AWS 访问密钥和私有密钥。单击验证。
- 2 选择仅允许访问特定的 AWS 区域。从列表中选择 AWS 区域以启用从区域自动收集。如果未选择此选项，则不会发生自动收集。

3 单击**提交**。

添加 Azure 订阅

可以在 vRealize Network Insight 中将 Microsoft Azure 订阅添加为数据源。

您必须具有以下权限：

- Microsoft.Resources/subscriptions/read
- Microsoft.Compute/virtualMachines/read
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/networkSecurityGroups/read
- Microsoft.Network/networkInterfaces/read
- Microsoft.Network/applicationSecurityGroups/read
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Network/networkWatchers/queryFlowLogStatus/*
- Microsoft.Network/networkWatchers/read
- Microsoft.Network/publicIPAddresses/read

或者，为了方便使用，您可以添加存储帐户密钥操作员服务角色、网络参与者和读者权限。

步骤

- 1 在**设置**页面上，单击**帐户和数据源**。
- 2 单击**添加源**。
- 3 在公有云组下，单击 **Microsoft Azure**。
- 4 在**添加新的 Azure 订阅**页面中，提供所需的信息。

选项	操作
收集器虚拟机	从下拉菜单中选择一个收集器虚拟机。
租户 ID	输入 Azure Active Directory (AD) 的租户 ID。
应用程序 ID	输入应用程序 ID。
应用程序密钥	输入应用程序密钥。
订阅 ID	输入订阅 ID。

- 5 单击**验证**。

必须至少有一个虚拟机、网络安全组 (NSG)、网卡和 VNet 才能成功进行验证。

- 6 （可选）如果要收集 NSG 流日志以获取流的详细信息见解，请选择**启用 NSG 流数据收集**复选框。

- 7 在**昵称**文本框中，输入昵称。
- 8 （可选）在**备注**文本框中，您可以根据需要添加备注。
- 9 单击**提交**。

启用 NSG 流日志

要在 vRealize Network Insight 中启用网络安全组 (NSG) 流数据收集，必须在 Azure 环境中启用 NSG 流日志。

与 Azure 相关的过程和任务记录在 <https://docs.microsoft.com/en-us/azure/network-watcher/> 中。

前提条件

确认您拥有正确的权限。有关权限的信息，请参见[受支持的产品和版本](#)。

步骤

- 1 在 Azure 环境中启用网络观察程序。有关详细信息，请参见 Azure《网络观察程序文档》中的“记录虚拟机网络流量”教程。
- 2 在 Azure 环境中注册 Insights Provider。有关详细信息，请参见 Azure《网络观察程序文档》中的“记录虚拟机网络流量”教程。
- 3 在 Azure 环境中启用 NSG 流日志。有关详细信息，请参见 Azure《网络观察程序文档》中的“记录虚拟机网络流量”教程。
- 4 在 **Microsoft Azure** 门户中，单击**存储帐户 > Blob**。
- 5 选择要在其中存储流日志的容器，然后单击**更改访问级别**并选择**容器 (容器和 Blob 的匿名读取访问权限)**。

必须对要存储流日志的所有容器执行此步骤。

添加 VMware PKS

您可以将 VMware PKS 添加为数据源，并提取 vRealize Network Insight 中的 PKS 群集详细信息。

前提条件

您必须添加相应的 NSX-T Manager。

步骤

- 1 在“设置”页面上，单击**帐户和数据源**。
- 2 单击**添加源**。
- 3 在“容器”下，选择 **VMware PKS**。

- 4 在“添加数据源”页面上，提供以下详细信息：

字段名称	描述
NSX-T Manager	选择支持 VMware PKS 部署的底层网络的 NSX-T Manager。
收集器 (代理) 虚拟机	vRealize Network Insight 会自动选择与所选的 NSX-T Manager 关联的相应收集器虚拟机。 注 作为 NetFlow 收集器添加的收集器虚拟机在列表中不可用。
API 主机名 (FQDN)	输入 PKS API 服务器的 FQDN 详细信息。
用户名	输入有权访问群集的 PKS 用户名。
密码	输入密码。

- 5 单击**验证**。

您会看到 Validation Successful 消息。

- 6 输入数据源的昵称，并根据需要添加任何描述备注。

- 7 单击**提交**。

添加 Kubernetes

您可以将 Kubernetes 添加为数据源，并将 Kubernetes 群集详细信息提取到 vRealize Network Insight。

[注](#) 必须将 Kubernetes 群集和相应的 NSX-T Manager 添加到同一收集器虚拟机。

前提条件

- 在 vRealize Network Insight 中添加 NSX-T Manager。
- 确保可以从收集器虚拟机访问 Kubernetes API 服务器。

步骤

- 1 在“设置”页面上，单击**帐户和数据源**。
- 2 单击**添加源**。
- 3 在“容器”下，选择 **Kubernetes**。
- 4 在“添加数据源”页面上，提供以下详细信息：

字段名称	描述
NSX-T Manager	选择支持 Kubernetes 的底层网络的 NSX-T Manager。
收集器 (代理) 虚拟机	vRealize Network Insight 会自动选择与所选的 NSX-T Manager 关联的相应收集器虚拟机。 注 作为 NetFlow 收集器添加的收集器虚拟机在列表中不可用。
Kubeconfig	单击 浏览 并上传具有 Kubernetes 群集详细信息的 Kubernetes 配置文件。有关 Kubeconfig 配置文件格式的详细信息，请参阅 Kubernetes 文档 。 注 在 Kubeconfig 文件中配置的用户必须具有 列出 和 监视 特权。

5 单击**验证**。

您会看到 Validation Successful 消息。

6 输入数据源的昵称，并根据需要添加任何描述备注。

7 单击**提交**。

结果

现在，vRealize Network Insight 可以提取 Kubernetes 群集详细信息。

后续步骤

转到 Kubernetes 仪表板并查看详细信息，请参见[#unique_40](#)。

添加 OpenShift

您可以将 OpenShift 添加为数据源，并将 OpenShift 详细信息提取到 vRealize Network Insight。

注 必须将 OpenShift 和相应的 NSX-T Manager 添加到同一收集器虚拟机。

前提条件

- 在 vRealize Network Insight 中添加 NSX-T Manager。

步骤

- 1 在“设置”页面上，单击**帐户和数据源**。
- 2 单击**添加源**。
- 3 在“容器”下，选择 **OpenShift**。
- 4 在“添加数据源”页面上，提供以下详细信息：

字段名称	描述
NSX-T Manager	选择支持 OpenShift 的底层网络的 NSX-T Manager。
收集器 (代理) 虚拟机	vRealize Network Insight 会自动选择与所选的 NSX-T Manager 关联的相应收集器虚拟机。 注 作为 NetFlow 收集器添加的收集器虚拟机在列表中不可用。
Kubeconfig	单击 浏览 并上载具有 Kubernetes 群集详细信息的 Kubernetes 配置文件。有关 Kubeconfig 配置文件格式的详细信息，请参阅 Kubernetes 文档 。 注 在 Kubeconfig 文件中配置的用户必须具有 列出 和 监视 特权。

5 单击**验证**。

您会看到 Validation Successful 消息。

6 输入数据源的昵称，并根据需要添加任何描述备注。

7 单击**提交**。

结果

现在，vRealize Network Insight 可以提取 OpenShift 详细信息。

后续步骤

有关详细信息，请参见[#unique_40](#)。

添加 Palo Alto Networks Panorama

可以在 vRealize Network Insight 中将 Palo Alto Networks Panorama 添加为数据源。

前提条件

请确保您具有**管理员角色**且具有 XML API 访问权限。有关更多详细信息，请参见 [Palo Alto 网络](#)。

步骤

- 1 在**设置**页面上，单击**帐户和数据源**。
- 2 单击**添加源**。
- 3 在**防火墙**下，单击 **Palo Alto Networks Panorama**。
- 4 在**添加新 Palo Alto Networks Panorama 帐户或源**页面中，提供所需的信息。

选项	操作
收集器 (代理) 虚拟机	从下拉菜单中选择一个收集器虚拟机。
IP 地址/FQDN	输入 IP 地址或 FQDN 详细信息。
用户名	输入用户名。
密码	输入密码。

- 5 单击**验证**。
- 6 在**昵称**文本框中，输入昵称。
- 7 （可选）在**备注**文本框中，您可以根据需要添加备注。
- 8 单击**提交**。

添加 Check Point 管理服务器

可以在 vRealize Network Insight 中将 Check Point 管理服务器添加为数据源。

前提条件

确保您拥有正确的权限。有关权限的信息，请参见 [Check Point 防火墙](#)。

步骤

- 1 在**设置**页面上，单击**帐户和数据源**。

- 2 单击**添加源**。
- 3 在**防火墙组**下，单击 **Check Point 管理服务器**。
- 4 在**添加新 Check Point 管理服务器帐户或源**页面中，提供所需的信息。

选项	操作
收集器 (代理) 虚拟机	从下拉菜单中选择一个收集器虚拟机。
IP 地址/FQDN	输入 IP 地址或 FQDN 详细信息。
用户名	输入用户名。
密码	输入密码。

- 5 单击**验证**。
- 6 在**昵称**文本框中，输入昵称。
- 7 （可选）在**备注**文本框中，您可以根据需要添加备注。
- 8 单击**提交**。

添加 Cisco ASA

可以在 vRealize Network Insight 中将 Cisco ASA 添加为数据源。

前提条件

确保您拥有正确的权限。有关权限的信息，请参见[受支持的产品和版本](#)。

步骤

- 1 在**设置**页面上，单击**帐户和数据源**。
- 2 单击**添加源**。
- 3 在**防火墙组**下，单击 **Cisco ASA**。
- 4 在**添加新 Cisco ASA 帐户或源**页面中，提供所需的信息。

选项	操作
收集器 (代理) 虚拟机	从下拉菜单中选择一个收集器虚拟机。
IP 地址/FQDN	输入 IP 地址或 FQDN 详细信息。
用户名	输入用户名。 注 用户应具有启用模式特权，以便将终端长度设置为 0 以及切换安全上下文。
密码	输入密码。 注 请确保输入与用于 Cisco ASA 的启用模式的密码相同的密码。

- 5 （可选）要启用更丰富的数据收集，请单击**使用 SNMP (建议用于收集更丰富的数据)**复选框。
- 6 单击**验证**。

- 7 在**昵称**文本框中，输入昵称。
- 8 （可选）在**备注**文本框中，您可以根据需要添加备注。
- 9 单击**提交**。

添加 Fortinet FortiManager

在 vRealize Network Insight 中，可以将 Fortinet FortiManager 添加为数据源。

前提条件

确认以下项：

- 您使用的是 FortiManager 版本 6.0.1。
- 您至少具有可以访问所有 ADOM 和策略包的**受限用户**角色。
- 您已从命令行界面 (CLI) 启用 **rpc-permit read-write** 访问权限。

要配置 **rpc** 权限，请在 FortiManager CLI 中使用以下命令：

```
config system admin user
edit "<administrator name>"
set rpc-permit [none | read | read-write ]
end
```

步骤

- 1 在**设置**页面中，单击**帐户和数据源 > 添加源**。
- 2 在**防火墙**部分下，单击 **Fortinet FortiManager**。
- 3 在**添加新 Fortinet FortiManager 帐户或源**页面中，输入所需的信息：

选项	操作
收集器 (代理) 虚拟机	从下拉菜单中选择收集器虚拟机。
IP 地址/FQDN	输入 IP 地址或 FQDN 详细信息。
用户名	输入要用于此数据源的用户名。
密码	输入密码。

- 4 单击**验证**。
- 5 在**昵称**文本框中，输入数据源的昵称。
- 6 （可选）在**备注**文本框中，您可以根据需要添加备注。
- 7 单击**提交**。

添加 Dell OS10 交换机

可以在 vRealize Network Insight 中将 Dell OS10 交换机添加为数据源。

前提条件

有关受支持的 Dell 交换机的信息，请参见[受支持的产品和版本](#)。

步骤

- 1 在**设置**页面上，单击**帐户和数据源**。
- 2 单击**添加源**。
- 3 在**路由器和交换机组**下，单击 **Dell OS10**。
- 4 在**添加新帐户或源**页面中，提供所需的信息。

选项	操作
收集器虚拟机	从下拉菜单中选择一个收集器虚拟机。
IP 地址/FQDN	输入 IP 地址或 FQDN 详细信息。
用户名	输入用户名。
密码	输入密码。

- 5 单击**验证**。
您会看到 Validation Successful 消息。
- 6 要启用 SNMP 或数据收集，请选择**使用 SNMP**。
- 7 在**昵称**文本框中，输入昵称。
- 8 在**备注**文本框中，您可以根据需要添加备注。
- 9 单击**提交**。

后续步骤

在 [Dell OS10 交换机上启用遥测](#)

在 Dell OS10 交换机上启用遥测

可以在 Dell OS10 交换机上启用遥测，以集成 Dell 交换机上的缓冲区统计信息和跟踪功能。

前提条件

添加 [Dell OS10 交换机](#)

从交换机收到请求时，vRealize Network Insight 收集器会在定义的端口上存储或缓冲数据包。

如果缓冲区大小因输入速率的增加（相比于输出速率）而增加，请求可能会变慢或超时。Dell OS10 交换机使用 gRPC 捕获此类衡量指标信息，您可以在 vRealize Network Insight 上看到此信息。这样，您可以诊断因网络拥堵而可能导致的应用程序性能问题，同时会主动提供拥堵对应用程序和网络造成的影响。

步骤

- ◆ 在 Dell OS10 交换机上运行以下命令：

```
telemetry
enable
!
destination-group dg03
  destination vRNI Collector IP 50000
!
subscription-profile sp03
  sensor-group bgp
  sensor-group buffer
  sensor-group device
  sensor-group environment
  sensor-group interface
  sensor-group lag
  sensor-group system
  destination-group dg03
  encoding gpb
  transport grpc no-tls
  source-interface ethernet1/1/1
```

结果

vRealize Network Insight 收集器从 Dell OS10 交换机收集以下遥测信息。

- per-port egress unicast queues
- per-port egress multicast queues
- per-port egress service pool
- per priority group ingress shared headroom
- per service pool ingress

后续步骤

运行以下任一查询：

- `show ports where metric > X in time range`
- `show switches where metric > X in time range`
- `port show metrics in time range`
- `switch show metrics in time range`
- `show switches where at least one port metric > X in time range`

您会看到相应的事件已触发。例如，SwitchPort Buffer Threshold Exceeded Event。

此外，还可以搜索接口峰值缓冲区利用率衡量指标，并确定请求速度减慢的原因。

添加 Huawei 6800/7800/8800 系列

vRealize Network Insight 支持多个系列的 Huawei Cloud Engine。

前提条件

用户必须至少具有只读权限。

步骤

- 1 在“设置”页面上，单击**帐户和数据源**。
- 2 单击**添加源**。
- 3 在**路由器和交换机**下，选择 **Huawei 6800/7800/8800 系列**。
- 4 输入以下信息：

属性	描述
收集器 (代理) 虚拟机	从下拉菜单中选择代理虚拟机。
IP 地址/FQDN	输入 IP 地址或 FQDN 详细信息。
Username	输入要用于此数据源的用户名。
Password	输入密码。

- 5 单击**验证**。
- 6 如果为数据收集启用 SNMP，则选择 **SNMP 版本**。
 - a 对于 **2c**，请输入关联的社区字符串。
 - b 对于 **3**，请输入以下内容：
 - Username
 - Context Name
 - Authentication Type
- 7 根据需要，提供**昵称**和**备注**。
- 8 单击**提交**。

后续步骤

您可以将 vRealize Network Insight 的以下功能与 Huawei 设备或路由器配合使用。

- 虚拟机-虚拟机路径
- 虚拟机底层拓扑
- Huawei 路由器或交换机仪表板
- 衡量指标：交换机端口和路由器接口衡量指标

- 仪表板
 - Huawei 路由器或交换机
 - 路由器接口
 - 端口通道
 - 交换机端口
 - 路由
- 高可用性：支持 M-LAG（多机架链路聚合组）和 VRRP（虚拟路由器冗余协议）
- 搜索
 - Huawei VRF（虚拟路由和转发）
 - Huawei 路由器接口
 - Huawei 交换机端口
 - Huawei 端口通道
 - Huawei 路由
- Huawei NetStream 数据监控

添加 Cisco ACI

可以将 Cisco ACI 添加为数据源。此功能仅适用于企业级许可证用户。

要将 Cisco ACI 添加为数据源，用户应有权访问所有租户和只读特权。以下是 Cisco ACI 数据源添加的步骤：

步骤

- 1 在**帐户和数据源**页面的**设置**下，单击**添加源**。
- 2 在**其他**下，单击 **Cisco ACI**。
- 3 在**添加新 Cisco ACI 帐户或源**页面中，提供以下信息：
 - 选择收集器虚拟机。
 - 提供群集中任何 APIC 控制器的 IP 地址。

注 不必在 ACI 结构层中添加各个交换机。

 - 提供用户凭据。
 - vRealize Network Insight 从各个交换机通过 SNMP 收集衡量指标数据。要启用此任务，请选择**使用 SNMP**。
- 4 单击**验证**。

5 为数据源输入**昵称**和**备注**（如果有），然后单击**提交**

为 NetFlow 和 sFlow 添加物理流收集器

可以添加物理流收集器并配置交换机，以将 sFlow 和 NetFlow 记录推送到收集器。用于 NetFlow 或 sFlow 的收集器虚拟机是一个专用收集器。它不能用于任何其他数据源。如果在代理服务器上还添加了任何其他数据源，则它不能用作 sFlow 和 NetFlow 的物理流收集器。

步骤

- 1 在**设置**页面中，单击**帐户和数据源**。
- 2 单击**添加源**。
- 3 在**流**下，单击**物理流收集器 (Netflow、sFlow)**。
 仅在物理收集器上接受 sFlow。
- 4 根据需要，输入**昵称**和**备注**。
- 5 单击**提交**。

结果

注 vRealize Network Insight 收集 sFlow 的数据包样本，因此无法显示流的完整衡量指标。

后续步骤

配置交换机以将流推送到物理流收集器。

- 定义目标（您在 vRealize Network Insight 中添加的收集器 IP 地址）。
- 设置流收集器的端口。
- 分配轮询时间间隔。

注 要配置的过程取决于要配置的交换机。有关详细信息，请参见特定的交换机文档。

添加 Log Insight

发生 NSX 事件时，vRealize Log Insight 会动态收集 NSX 日志。但是，vRealize Network Insight 每 10 分钟从 NSX 收集数据。因此，在 vRealize Network Insight 中添加 vRealize Log Insight 可使您更快地获取事件信息，而不是等待事件信息。

在 vRealize Network Insight 与 vRealize Log Insight 集成中，vRealize Network Insight 使用 vRealize Log Insight 生成的警示。只要创建或修改安全组，NSX 的日志就会发送到 vRealize Log Insight，后者又发送警示。收到警示后，vRealize Network Insight 轮询在其上创建安全组的 NSX Manager，并提取所更改安全组的相应数据。当前，此集成仅支持与安全组 CRUD 相关的警示。

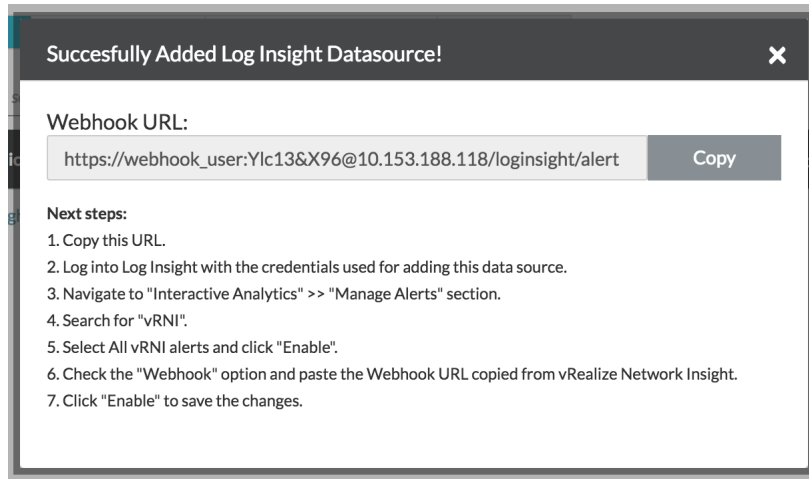
vRealize Network Insight 与 vRealize Log Insight 集成支持以下版本：

- VMware vRealize Log Insight 4.5 及更高版本

- vRealize Network Insight v3.8 及更高版本
- VMware NSX Manager v6.2 及更高版本

步骤

- 1 创建或重用具有 vRealize Log Insight API 访问权限的 vRealize Log Insight 用户。
- 2 在**安装和支持**页面上，单击**帐户和数据源**。
- 3 单击**添加源**。
- 4 在**日志服务器**下单击 **Log Insight**。
- 5 在**添加新的 Log Insight 服务器帐户或源**页面上，单击页面标题旁边的**说明**。将显示一个弹出窗口，其中提供了添加 Log Insight 数据源的必备条件以及在 vRealize Log Insight 上启用 Webhook URL



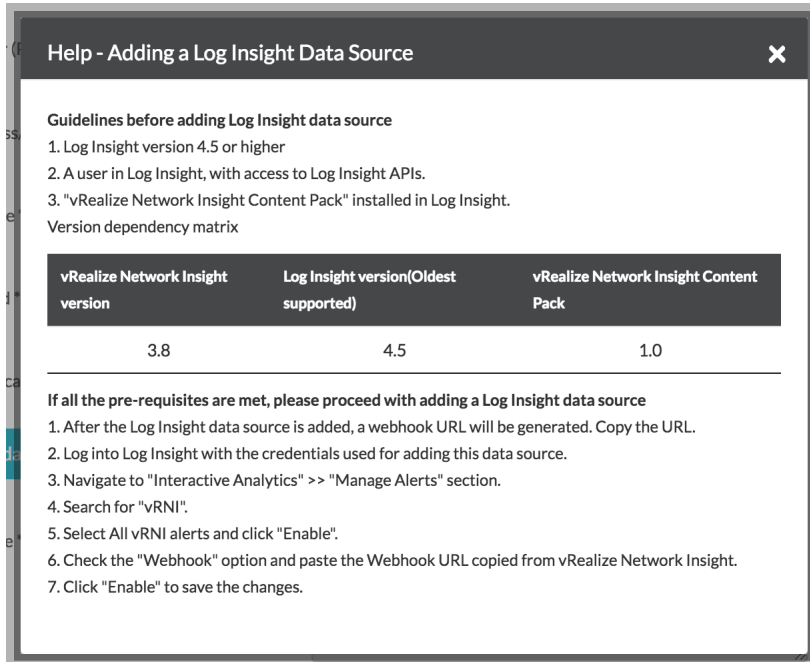
的说明。

注 在添加数据源后生成的 Webhook URL 在 vRealize Log Insight 中使用。

- 6 输入所需的详细信息。

名称	描述
收集器 (代理) 虚拟机	选择为数据收集过程部署的数据收集器的 IP 地址。
IP 地址/FQDN	输入数据源的 IP 地址或 FQDN。
用户名	输入要用于特定数据源的用户名。
密码	输入数据源的密码。
身份验证提供程序	为您提供的凭据选择相应的身份验证提供程序。

- 7 创建数据源后，将显示一个弹出窗口，该窗口将提供 Webhook URL 以及在 vRealize Log Insight 上启用此 URL 而必须执行的步骤。复制 Webhook URL。使用用于添加此数据源的凭据登录。在 vRealize Log Insight 应用程序中启用警示，然后配置此 Webhook URL。发送测试警示以确保集成成功。



注 vRealize Network Insight 中 vRealize Log Insight 数据源上显示的任何警示都将在一小时内解决。

添加 Infoblox

vRealize Network Insight 允许您将 Infoblox Grid 添加为 DNS 数据提供程序。

Infoblox DNS 提供了一个高级解决方案以管理和控制 DNS。它使用 Infoblox Grid 来确保 DNS 在整个网络中高度可用。来自 Infoblox 的 DNS 数据仅用于扩充源或目标 IP 地址与物理设备关联的流。

Infoblox DNS 数据与通过使用 CSV 导入的 DNS 数据共存。

如果在收集器上配置 Infoblox DNS 数据源，则也可以在同一收集器上配置其他数据源。对于 Infoblox，不需要专用的收集器。

注意事项

- 在当前版本中，vRealize Network Insight 仅支持 Infoblox 的单网格模式。
- 当前版本仅支持 A 记录。当前不支持共享 A 记录。
- 在当前版本中，DNS 扩充仅受标记为物理的 IP 地址支持。
- 如果单个物理 IP 地址有多个 FQDN，则将返回所有 FQDN。

步骤

- 1 在**设置**页面上，单击**帐户和数据源**。
- 2 单击**添加新源**。
- 3 单击 **DNS** 下的 **Infoblox**。
- 4 提供以下信息：

表 3-4.

属性	描述
Collector VM	从下拉菜单中选择收集器虚拟机。
IP Address/FQDN	输入 Infoblox Grid 的 IP 地址/FQDN。
Username	输入要用于特定数据源的用户名。
Password	输入密码。

- 5 单击**验证**。

注 确保您具有 API Privilege 以访问 Infoblox API。

- 6 为数据源输入**昵称**和**备注**（如果有），然后单击**提交**将 Infoblox DNS 数据源添加到环境。

添加 F5 BIG-IP

vRealize Network Insight 支持 F5 BIG-IP 的路由器和负载均衡器功能。支持虚拟机-虚拟机路径、高可用性、VRF、路由、路由器接口、交换机端口、端口通道、交换机端口衡量指标、VRF 仪表板、交换机仪表板和路由器仪表板等功能。要搜索 F5 BIG IP 实体，请使用查询字符串 F5 BIG-IP Data Source。

vRealize Network Insight 不支持虚拟机-虚拟机路径中的 LLDP 邻居或邻接设备。

要将 F5 BIG-IP 添加为数据源，请执行以下操作：

前提条件

- 用户必须具有：
 - 访问所有分区的 Guest 角色或只读权限。
 - REST API 的访问权限。
 - TMSH 终端的访问权限。
- 在设备上启用 SSH。

为 SSH 启用 password authentication，如下所示：

注

- 使用 root 或管理员角色特权来更改 SSHD 配置。
- 在 vRealize Network Insight 中添加 F5 BIG-IP 数据源时，请勿使用 root 用户特权。
- Root 用户没有 HTTP 访问权限。root 用户特权用于管理目的。

```
[root@bigip:Active] config # tmsh
root@bigip(Active) (/Common) (tmsh) # edit sys sshd

## Adding the following configuration ##

modify sshd {
    include "
    ChallengeResponseAuthentication no
    PasswordAuthentication yes"
}
#####
Save changes? (y/n/e) y
root@bigip(Active) (/Common) (tmsh) #
root@bigip(Active) (/Common) (tmsh) # save sys config

root@bigip(Active) (/Common) (tmsh) # show running-config sys sshd
sys sshd {
    include "
    ChallengeResponseAuthentication no
    PasswordAuthentication yes"
}
```

步骤

- 1 在“设置”页面上，单击**帐户和数据源**。
- 2 单击**添加源**。
- 3 在**路由器和交换机**下，选择 **F5 BIG-IP**。
- 4 提供以下信息：

属性	描述
收集器 (代理) 虚拟机	从下拉菜单中选择代理虚拟机。
IP 地址/FQDN	输入 IP 地址或 FQDN 详细信息。
Username	输入要用于此数据源的用户名。
Password	输入密码。

- 5 在文本框中输入信息后，单击**验证**。

6 如果为数据收集启用 SNMP，则选择 **SNMP** 版本。

- a 如果选择 2c，则输入关联的社区字符串。
- b 如果选择 3，则输入以下内容：

- Username
- Context Name
- Authentication Type

注 确保在 F5 BIG-IP UI 控制台上配置 SNMP。

- a 登录到 F5。
 - b 导航到**系统 > SNMP**。
 - c 转到 **SNMP > 代理 > 访问 (v1、v2c)**。
 - d 输入社区字符串。
 - e 输入源 IP 地址。
 - f 选择**只读**访问权限。
 - g 单击**完成**。
-

7 根据需要，提供**昵称**和**备注**。单击**提交**。

添加 ServiceNow

ServiceNow 配置管理数据库 (CMDB) 让您能够全面了解数据中心内的软件和硬件基础架构及其之间的关系，这有助于您管理清单。借助 ServiceNow 集成，vRealize Network Insight 可以发现 ServiceNow CMDB 中提供的应用程序，使您能够直接将其添加到 vRealize Network Insight 中。

CMDB 概念

CMDB 主要包括：

- **配置项**：系统中的一个实体或一个组件。例如，一台计算机、一个交换机、一项服务、一个应用程序、一台服务器或一个虚拟机。
- **关系**：配置项之间的链接或通信类型。例如，依赖于、运行于、交换数据。

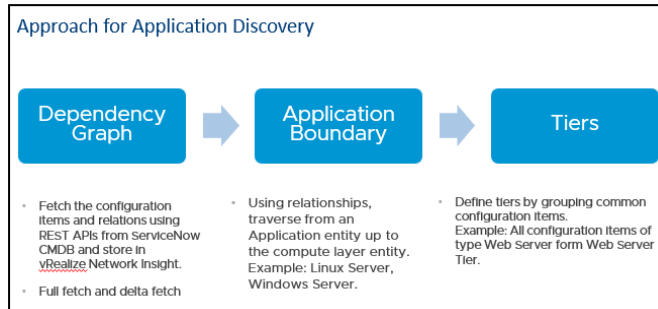
每个配置项都有一个定义的结构定义。

- **配置项类**：每个配置项都必须与一个定义其属性的类相关联。
- **关系类**：定义配置项之间的关系类型。

您可以扩展两个类以添加其他属性或自定义属性。

ServiceNow 支持应用程序服务，它是提供服务的一组互连应用程序和主机。ServiceNow 允许您通过使用 API 手动创建应用程序服务，或者可以通过服务映射自动发现该服务。所有这些应用程序均存储在 ServiceNow CMDB 中。

将 ServiceNow 数据源添加到 vRealize Network Insight 时，vRealize Network Insight 将从 ServiceNow CMDB 配置文件中提取配置项和关系。



默认情况下，vRealize Network Insight 会定期提取数据。

- 每 12 小时执行一次完整的数据提取，该操作会提取 CMDB 配置中定义的所有类记录。此外，添加或更新数据源时，也会执行完整的提取操作。
- 每 2 分钟执行一次增量提取，将提取 CMDB 配置中定义的所有新的、已修改和已删除的记录。vRealize Network Insight 大约需要 12 分钟才能在用户界面上反映这些详细信息。

注 vRealize Network Insight 仅在完整提取过程中提取类层次结构和关系类型。

限制的默认值

限制名称	描述	默认值	超出限制的影响
maxAppsPerDataSource	每个数据源的最大应用程序数。	5000	数据源停止提取数据，数据源和事件页面上显示错误，并且应用程序不会更新。
maxTiersPerApp	每个应用程序可以存储的最大层数。	150	层数减少到适合限制后，应用程序才会更新。
maxMembersPerApp	每个应用程序可以存储的最大成员数。	5000	成员数减少到适合限制后，应用程序才会更新。
maxGraphTraversalStackSize	图形遍历中使用的最大堆栈大小。	10000	不会创建应用程序，并出现异常 SizeLimitExceededException。
maxResponseAppCount	API 响应中可返回的最大应用程序数。	5000	仅返回适合此限制的应用程序数，并且 UI 显示错误。

添加 ServiceNow

您可以将 ServiceNow 作为数据源添加到 vRealize Network Insight 中，并提取应用程序和层详细信息。

前提条件

您必须具有管理员特权才能添加数据源。

步骤

- 1 在“设置”页面上，单击**帐户和数据源**。
- 2 单击**添加源**。

- 3 在 CMDB 下，选择 **ServiceNow**。
- 4 在“添加数据源”页面上，提供以下详细信息：

字段名称	描述
收集器 (代理) 虚拟机	ServiceNow 的主机 URL
IP 地址/FQDN	输入 IP 地址或 FQDN 详细信息。
用户名	输入要用于此数据源的用户名。
	注 您计划添加的用户必须是 ServiceNow 中的 管理员 或 只读管理员 。
密码	输入密码。

- 5 单击**验证**。
您会看到 Validation Successful 消息。
- 6 要添加自定义的 CMDB 配置，请执行以下操作：
 - a 选择**自定义 CMDB 配置**。
 - b 单击**下载**以下载默认配置文件。
 - c 更新文件属性。请参见**自定义 CMDB 配置**。
 - d 在“添加数据源”页面上，浏览以选择更新的 JSON 文件。
- 7 输入数据源的昵称，并添加任何描述备注。
- 8 单击**提交**。

后续步骤

添加 ServiceNow 数据源后，vRealize Network Insight 会发现 ServiceNow CMDB 中可用的应用程序，这些应用程序将添加到 vRealize Network Insight 中。有关详细信息，请参见[添加已发现的应用程序](#)。

默认 CMDB 配置文件

vRealize Network Insight 支持使用 JSON 格式的配置文件进行 ServiceNow 自定义。

```
{
  "fetchOnlyApprovedApplications": false,
  "nameBasedSearchForVm": false,
  "ignoreWorkloadCheck": false,
  "ciGroup": [
    {
      "name": "applicationClasses",
      "value": [
        "cldb_ci_service_discovered"
      ],
      "valueType": "CI_CLASS",
      "systemGenerated": true,
      "expandCIClass": true
    }
  ],
}
```



```

{
  "name": "relationshipTypeClasses",
  "value": [
    "*"
  ],
  "valueType": "CI_VALUE",
  "systemGenerated": true,
  "expandCIClass": false
},
{
  "name": "workloadRelationshipTypeClasses",
  "value": [
    "Hosted on::Hosts",
    "Instantiates::Instantiated by",
    "Runs on::Runs",
    "Virtualized by::Virtualizes"
  ],
  "valueType": "CI_VALUE",
  "systemGenerated": true,
  "expandCIClass": false
},
{
  "name": "workloadCIClasses",
  "value": [
    "cmdb_ci_computer",
    "cmdb_ci_vm_instance",
    "cmdb_ci_vmware_instance"
  ],
  "valueType": "CI_CLASS",
  "systemGenerated": true,
  "expandCIClass": true
},
{
  "name": "relationClasses",
  "value": [
    "cmdb_rel_ci"
  ],
  "valueType": "CI_CLASS",
  "systemGenerated": true,
  "expandCIClass": true
},
{
  "name": "ignoredCIClasses",
  "value": [
    "cmdb_ci_vcenter_server_obj"
  ],
  "valueType": "CI_VALUE",
  "systemGenerated": true,
  "expandCIClass": true
},
{
  "name": "ignoredTierCIClasses",
  "value": [
  ],
  "valueType": "CI_VALUE",

```

```

    "systemGenerated": true,
    "expandCIClass": true
  },
  {
    "name": "trackedCIClasses",
    "value": [
      "cmdb_ci_appl",
      "cmdb_ci_cluster",
      "cmdb_ci_cluster_node",
      "cmdb_ci_database",
      "cmdb_ci_lb_service",
      "cmdb_ci_spkg",
      "cmdb_ci_qualifier_manual_connection",
      "cmdb_ci_endpoint",
      "cmdb_ci_network_adapter",
      "cmdb_ci_translation_rule"
    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
  }
],
"traversalRule": [
  {
    "fromNode": [
      "applicationClasses"
    ],
    "toNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 5
  },
  {
    "fromNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "toNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 3
  }
],
"traversalStopRule": [
  {
    "fromNode": [
      "trackedCIClasses",

```

```

        "workloadCIClasses"
    ],
    "toNode": [
        "applicationClasses"
    ],
    "relationship": [
        "relationshipTypeClasses"
    ],
    "priority": 5
}
],
"associationRule": [
    {
        "fromNode": [
            "trackedCIClasses",
            "workloadCIClasses"
        ],
        "toNode": [
            "workloadCIClasses"
        ],
        "relationship": [
            "workloadRelationshipTypeClasses"
        ],
        "priority": 5
    }
]
}

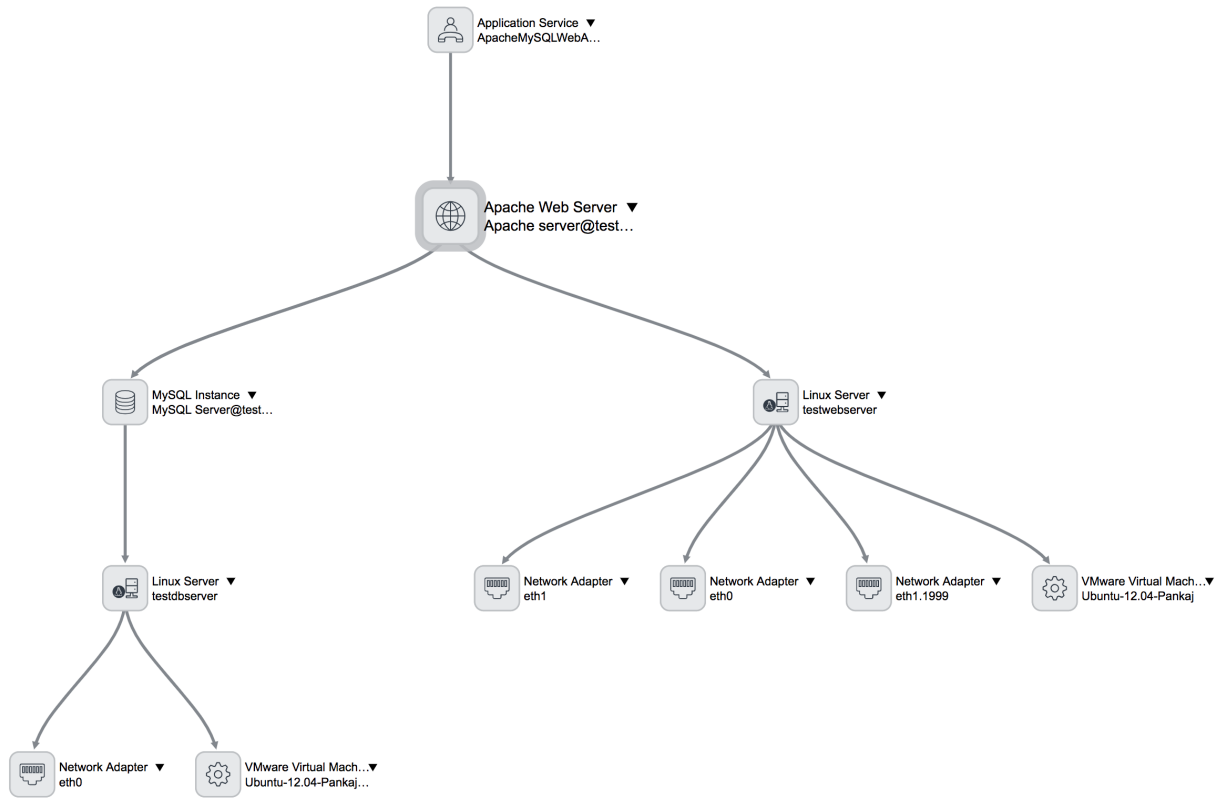
```

发生配置更改时，vRealize Network Insight 可能需要 30 分钟才能进行完整数据提取并重新计算所有应用程序。

示例：使用默认 CMDB 配置的 ServiceMap 和发现的应用程序示例

示例：vRealize Network Insight 上用于添加应用程序的更新页面

这使得 vRealize Network Insight 能够在 ServiceNow 中发现应用程序。



Modify Application



Application Name * ApacheMySQLWebApp Application Total: 2 VMs | 0 Physical IPs

▼ Tier Tier Total: 1 VMs | 0 Physical IPs

Name * ApacheMySQLWebApp.apache_web_server

Virtual Machines / IP Addresses * VM Names ▼ 'Ubuntu-12.04-Pankaj' 1 Vms

[Add another Condition](#)

▼ Tier Tier Total: 1 VMs | 0 Physical IPs

Name * ApacheMySQLWebApp.db_mysql_instance

Virtual Machines / IP Addresses * VM Names ▼ 'Ubuntu-12.04-Dark-Pankaj-1' 1 Vms

[Add another Condition](#)

[Add Tier](#)

☐ Analyze Flows

Save
Cancel

自定义 CMDB 配置

为了支持各种自定义，ServiceNow 和 vRealize Network Insight 集成支持通用配置。CMDB 配置必须采用 JSON 格式。

配置包括：

- 配置项
- 配置项之间的关系
- 依赖关系图遍历规则。

您可以根据您的实现方式自定义 CMDB 配置。

注 更改配置时，将执行完整提取并重新计算所有应用程序。因此，此过程可能需要至少 30 分钟，才能在“已发现的应用程序”仪表板上显示结果。

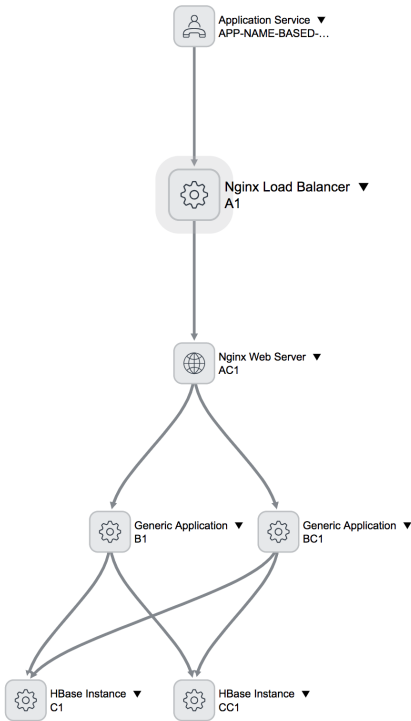
字段名称	描述
fetchOnlyApprovedApplications	允许布尔值仅从 ServiceNow 提取已批准的应用程序。默认情况下，其值设置为 False 。
nameBasedSearchForVm	<p>允许布尔值指示当 vRealize Network Insight 中不存在 ServiceNow 虚拟机时是否使用虚拟机名称创建自定义虚拟机搜索条件。如果将值设置为 True，则会创建自定义虚拟机名称条件，并在 vRealize Network Insight 中检测到相应虚拟机时反映计数，而不会重新计算应用程序。</p> <p>在不使用服务映射的情况下手动创建依赖关系图或服务映射时，可以使用此字段。默认情况下，其值设置为 False。</p>
ignoreWorkloadCheck	<p>允许布尔值指示是否将实体添加到层，即使关联的工作负载实体不存在也是如此。</p> <p>在不使用服务映射的情况下手动创建依赖关系图或服务映射时，以及在工作负载层之前未定义关系时，可以使用此字段。默认情况下，其值设置为 False。</p>
ciGroup	<p>定义要从 ServiceNow 提取的配置项和关系。此字段允许以下属性：</p> <ul style="list-style-type: none"> ■ Name: 配置项组的名称 ■ Value: 属于此组的 ServiceNow 类名称的列表。 ■ ValueType: 允许 CI_CLASS（要提取的类名称）和 CI_VALUE。 <ul style="list-style-type: none"> ■ CI_CLASS - 要提取的类。 ■ CI_VALUE <p>注 vRealize Network Insight 始终提取 applicationClasses、workloadCIClasses、trackedCIClasses、workloadCIClasses 和 relationClasses。</p> <ul style="list-style-type: none"> ■ systemGenerated: 允许布尔值指示该类是用户定义的类还是默认类。 ■ expandCIClass - 允许布尔字段指示是否提取 Value 中列出的配置项类的子类。
Rules for graph traversal	<p>支持三种类型的遍历规则：</p> <ul style="list-style-type: none"> ■ traversalRule: 所有允许的或有效的遍历。 ■ traversalStopRule: 不允许的遍历。 <p>注 traversalStopRule 中的规则比 traversalRule 中的规则具有更高的优先级。</p> <ul style="list-style-type: none"> ■ associationRule: 与实体关联的工作负载允许使用的遍历。 <p>规则的属性：</p> <ul style="list-style-type: none"> ■ fromNode: 作为遍历源的 ciGroup 列表。 ■ toNode: 作为遍历目标的 ciGroup 列表。 ■ relationship: 在一种类型的遍历中具有关系的 ciGroup 列表。 ■ priority: 如果 ciGroup 与两个规则匹配，则会根据 priority 设置 ciGroup 的规则。优先级数越大，优先级值越高。
applicationClasses	<p>列出图遍历的所有入口点配置项类。这些类表示在 CMDB 中用作应用程序类的配置项类型。</p> <p>默认配置使用 cmdb_ci_service_discovered 类。此类表示由 ServiceNow 的 ServiceMapping 功能创建的应用程序。</p>

字段名称	描述
<code>workloadCiClasses</code>	<p>列出托管基于软件的服务或操作系统（如 Linux Server、Windows Server）的所有配置项。例如虚拟机、AWS 实例、物理服务器。</p> <p>通常，工作负载配置项放置在依赖关系图的末尾。不会为此组中提到的配置项类创建层。</p> <p>默认配置包含以下配置项类：</p> <ul style="list-style-type: none"> ■ <code>cmdb_ci_computer</code>: 表示所有计算相关的配置项。这是所有 Linux 和 Windows Server 的超级类。 ■ <code>cmdb_ci_vm_instance</code>: 表示虚拟计算实体，如虚拟机和 AWS 实例。 ■ <code>cmdb_ci_vmware_instance</code>: 表示 VMware 虚拟机。
<code>trackedCiClasses</code>	<p>列出可以作为依赖关系图一部分但不是 <code>applicationClass</code> 或 <code>workloadCiClass</code> 的所有配置项。此组中的配置项是图完成从 <code>applicationClasses</code> 到 <code>workloadCiClasses</code> 所必需的。</p> <p>vRealize Network Insight 会为 <code>trackedCiClasses</code> 中提及的所有类创建层，除非在 <code>ignoredTierCiClasses</code> 下提到了该类。</p>
<code>relationshipTypeClasses</code>	<p>列出由关系配置项类或关系类型表示的所有相关配置项。</p> <p>默认配置使用 * 提取所有关系类型。</p>
<code>workloadRelationshipTypeClasses:</code>	<p>列出通常表示与工作负载实体的关系的关系类型。以下是 ServiceNow 中默认支持的关系：</p> <ul style="list-style-type: none"> ■ <code>Hosted on::Hosts</code> ■ <code>Instantiates::Instantiated by</code> ■ <code>Runs on::Runs</code> ■ <code>Virtualized by::Virtualizes</code>
<code>ignoredCiClasses</code>	<p>列出 vRealize Network Insight 从 ServiceNow CMDB 中提取时必须忽略的所有配置项。</p> <p>当提取超类时，要忽略不必要的子类，此字段非常有用。</p> <p>默认情况下，<code>cmdb_ci_vcenter_server_obj</code> 在 <code>ignoredCiClasses</code> 下列出，因为应用程序发现不需要 vCenter Server。</p>
<code>ignoredTierCiClasses</code>	<p>列出不得为其创建层的所有配置项。</p>

发现不含工作负载关系的应用程序的示例

下面是一个自定义的 CMDB 配置文件，其中定义了 nameBasedSearchForVm 以发现应用程序，其中 cmdb_ci_service_discovered 类是入口点，并且未定义工作负载关系。

拓扑



自定义的 CMDB 配置文件

```
{
  "fetchOnlyApprovedApplications": false,
  "nameBasedSearchForVm": true,
  "ignoreWorkloadCheck": true,
  "ciGroup": [
    {
      "name": "applicationClasses",
      "value": [
        "cmdb_ci_service_discovered"
      ],
      "valueType": "CI_CLASS",
      "systemGenerated": true,
      "expandCIClass": true
    },
    {
      "name": "relationshipTypeClasses",
      "value": [
        "*"
      ],
      "valueType": "CI_VALUE",
      "systemGenerated": true,
      "expandCIClass": false
    }
  ]
}
```



```

    },
    {
      "name": "workloadRelationshipTypeClasses",
      "value": [
        "Hosted on::Hosts",
        "Instantiates::Instantiated by",
        "Runs on::Runs",
        "Virtualized by::Virtualizes"
      ],
      "valueType": "CI_VALUE",
      "systemGenerated": true,
      "expandCIClass": false
    },
    {
      "name": "workloadCIClasses",
      "value": [
        "cmdb_ci_computer",
        "cmdb_ci_vm_instance",
        "cmdb_ci_vmware_instance"
      ],
      "valueType": "CI_CLASS",
      "systemGenerated": true,
      "expandCIClass": true
    },
    {
      "name": "relationClasses",
      "value": [
        "cmdb_rel_ci"
      ],
      "valueType": "CI_CLASS",
      "systemGenerated": true,
      "expandCIClass": true
    },
    {
      "name": "ignoredCIClasses",
      "value": [
        "cmdb_ci_vcenter_server_obj"
      ],
      "valueType": "CI_VALUE",
      "systemGenerated": true,
      "expandCIClass": true
    },
    {
      "name": "ignoredTierCIClasses",
      "value": [
        "cmdb_ci_qualifier_manual_connection",
        "cmdb_ci_endpoint"
      ],
      "valueType": "CI_VALUE",
      "systemGenerated": true,
      "expandCIClass": true
    },
    {
      "name": "trackedCIClasses",
      "value": [

```

```

        "cmdb_ci_appl",
        "cmdb_ci_cluster",
        "cmdb_ci_cluster_node",
        "cmdb_ci_database",
        "cmdb_ci_lb_service",
        "cmdb_ci_spkg",
        "cmdb_ci_qualifier_manual_connection",
        "cmdb_ci_endpoint",
        "cmdb_ci_network_adapter",
        "cmdb_ci_translation_rule"
    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
}
],
"traversalRule": [
{
    "fromNode": [
        "applicationClasses"
    ],
    "toNode": [
        "trackedCIClasses",
        "workloadCIClasses"
    ],
    "relationship": [
        "relationshipTypeClasses"
    ],
    "priority": 5
},
{
    "fromNode": [
        "trackedCIClasses",
        "workloadCIClasses"
    ],
    "toNode": [
        "trackedCIClasses",
        "workloadCIClasses"
    ],
    "relationship": [
        "relationshipTypeClasses"
    ],
    "priority": 3
}
],
"traversalStopRule": [
{
    "fromNode": [
        "trackedCIClasses",
        "workloadCIClasses"
    ],
    "toNode": [
        "applicationClasses"
    ],
    "relationship": [

```

```

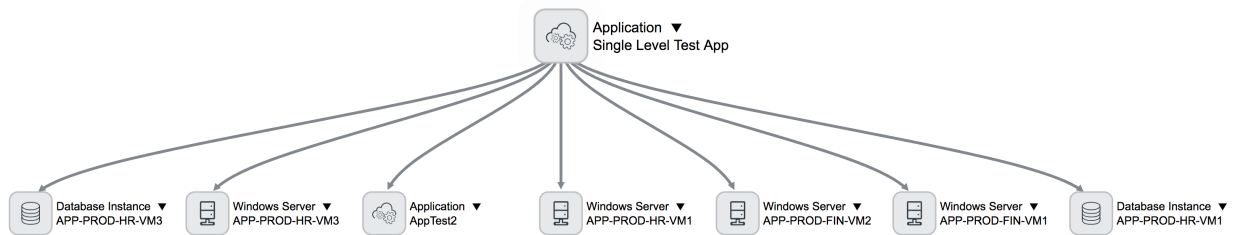
    "relationshipTypeClasses"
  ],
  "priority": 5
}
],
"associationRule": [
  {
    "fromNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "toNode": [
      "workloadCIClasses"
    ],
    "relationship": [
      "workloadRelationshipTypeClasses"
    ],
    "priority": 5
  }
]
}

```

发现单级应用程序的示例

下面是一个自定义的 CMDB 配置文件，其中定义了 `nameBasedSearchForVm` 以发现单级应用程序，其中 `cmdb_ci_service_discovered` 类是入口点，并且未定义工作负载关系。

拓扑



自定义的 CMDB 配置文件

```

{
  "fetchOnlyApprovedApplications": false,
  "nameBasedSearchForVm": true,
  "ignoreWorkloadCheck": true,
  "ciGroup": [
    {
      "name": "applicationClasses",
      "value": [
        "cmdb_ci_appl"
      ],
      "valueType": "CI_CLASS",
      "systemGenerated": true,
      "expandCIClass": false
    }
  ],
}

```

```

{
  "name": "relationshipTypeClasses",
  "value": [
    "*"
  ],
  "valueType": "CI_VALUE",
  "systemGenerated": true,
  "expandCIClass": false
},
{
  "name": "workloadRelationshipTypeClasses",
  "value": [
    "Hosted on::Hosts",
    "Instantiates::Instantiated by",
    "Runs on::Runs",
    "Virtualized by::Virtualizes"
  ],
  "valueType": "CI_VALUE",
  "systemGenerated": true,
  "expandCIClass": false
},
{
  "name": "workloadCIClasses",
  "value": [
    "cmdb_ci_computer",
    "cmdb_ci_vm_instance",
    "cmdb_ci_vmware_instance"
  ],
  "valueType": "CI_CLASS",
  "systemGenerated": true,
  "expandCIClass": true
},
{
  "name": "relationClasses",
  "value": [
    "cmdb_rel_ci"
  ],
  "valueType": "CI_CLASS",
  "systemGenerated": true,
  "expandCIClass": true
},
{
  "name": "ignoredCIClasses",
  "value": [
    "cmdb_ci_vcenter_server_obj"
  ],
  "valueType": "CI_VALUE",
  "systemGenerated": true,
  "expandCIClass": true
},
{
  "name": "ignoredTierCIClasses",
  "value": [
    "cmdb_ci_qualifier_manual_connection",
    "cmdb_ci_endpoint"
  ]
}

```

```

    ],
    "valueType": "CI_VALUE",
    "systemGenerated": true,
    "expandCIClass": true
  },
  {
    "name": "trackedCIClasses",
    "value": [
      "cmdb_ci_appl",
      "cmdb_ci_cluster",
      "cmdb_ci_cluster_node",
      "cmdb_ci_database",
      "cmdb_ci_lb_service",
      "cmdb_ci_spkg",
      "cmdb_ci_qualifier_manual_connection",
      "cmdb_ci_endpoint",
      "cmdb_ci_network_adapter",
      "cmdb_ci_translation_rule"
    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
  }
],
"traversalRule": [
  {
    "fromNode": [
      "applicationClasses"
    ],
    "toNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 5
  },
  {
    "fromNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "toNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 3
  }
],
"traversalStopRule": [
  {

```

```

    "fromNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "toNode": [
      "applicationClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 5
  }
],
"associationRule": [
  {
    "fromNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "toNode": [
      "workloadCIClasses"
    ],
    "relationship": [
      "workloadRelationshipTypeClasses"
    ],
    "priority": 5
  }
]
}

```

添加新的通用路由器或交换机

如果 vRealize Network Insight 不支持要添加的路由器或交换机，则可以通过上载设备配置文件将不支持的路由器或交换机添加为通用路由器或交换机。vRealize Network Insight 使用设备配置文件中的信息来提供对路由器或交换机的见解。在 vRealize Network Insight 中上载设备配置文件后，您无法修改已上载的设备配置文件的信息。

前提条件

使用 vRealize Network Insight 提供的 SDK，采用 .zip 格式创建设备配置文件。设备配置文件包含有关路由器接口、路由、交换机端口、VRF、交换机设备信息等实体的信息。要创建设备配置文件，请参见 <https://github.com/vmware/network-insight-sdk-generic-datasources>。

步骤

- 1 在“设置”页面上，单击**帐户和数据源**。
- 2 单击**添加源**。
- 3 在“路由器和交换机”下，单击**通用路由器和交换机**。

- 4 在**添加新的通用路由器/交换机**页面上，修改所需的信息。

选项	操作
收集器虚拟机	从下拉菜单中选择一个收集器虚拟机。
设备配置文件	选择并上载使用 SDK 创建的配置文件 (.zip)。
IP 地址/FQDN	输入 IP 地址或 FQDN 详细信息。

- 5 单击**验证**。
- 6 在**昵称**文本框中，输入要添加的交换机或路由器的昵称。
- 7 （可选）在**备注**文本框中，您可以根据需要添加备注。
- 8 单击**提交**。

编辑通用路由器或交换机

在 vRealize Network Insight 中，您可以通过上载新的配置文件来修改现有通用路由器或交换机的配置。

前提条件

使用 vRealize Network Insight 提供的 SDK，采用 .zip 格式创建设备配置文件。设备配置文件包含有关实体的信息，例如路由器接口、路由、交换机端口、VRF、交换机设备信息等。要创建设备配置文件，请参见 <https://github.com/vmware/network-insight-sdk-generic-datasources>。

步骤

- 1 在“设置”页面上，单击**帐户和数据源**。
- 2 单击要编辑的通用路由器或交换机数据源旁边的**编辑数据源**图标。
- 3 单击**替换文件**并上载新的设备配置文件。
- 4 （可选）要查看上载的设备配置文件，请单击**上载历史记录**。
您可以查看、下载和删除最近上载的五个设备配置文件。
- 5 单击**验证**。
- 6 （可选）在**昵称**文本框中，更改昵称。
- 7 单击**提交**。

从 vRealize Network Insight 中删除数据源

4

如果不需要查看数据源中的数据，或者数据源未在使用中，则可以从 vRealize Network Insight 中删除该数据源。

注 如果您的环境中不再有任何数据源可用，则必须从 vRealize Network Insight 中删除该数据源。

步骤

- 1 登录到 vRealize Network Insight Web 控制台。
- 2 转到 **设置 > 帐户和数据源**。
- 3 单击要删除的数据源旁边的 **删除数据源** 图标。
vRealize Network Insight 将提示您确认删除。
- 4 单击 **是**。

注 从系统中移除数据源后，两小时或更长时间后才能添加相同的数据提供程序。

迁移数据源

5

如果代理虚拟机已关闭或者已删除，则可以添加新代理虚拟机，并将数据源从旧代理虚拟机迁移到新代理虚拟机。

要迁移数据源，请执行以下操作：

步骤

- 1 在**安装和支持**页面中的**收集器 (代理) 虚拟机**部分下，单击编辑图标。
如果代理虚拟机已关闭，则可以在同一部分下看到错误消息，指出代理虚拟机不可用。
- 2 在**编辑收集器 (代理) 虚拟机**页面中，可以将昵称分配给代理虚拟机。
- 3 “编辑收集器 (代理)” 页面列出了添加到代理的所有数据源。要迁移数据源，请为特定的数据源单击**迁移**。
- 4 此时将显示“编辑帐户或源”页面。确保填写以下信息：

表 5-1.

字段	描述
收集器 (代理) 虚拟机	必须向其迁移数据源的新代理虚拟机的名称
IP 地址	数据源的预填 IP/FQDN 地址
用户名	数据源的用户名
密码	数据源的密码

- 5 单击**验证**。单击**提交**。然后将在旧代理虚拟机中删除该数据源，并将其添加到新代理虚拟机。
- 6 迁移成功后，在**帐户和数据源**页面的**已启用**列中将看到数据源的新代理虚拟机。

注

- 如果要将 vCenter 迁移到另一个代理虚拟机，请确保将对应的 NSX Manager 也迁移到同一代理虚拟机。
- 将 NSX Manager 迁移到另一个代理虚拟机时，子级数据提供程序（如 NSX Controller 和 NSX Edge）也会迁移到新代理虚拟机。

配置 vRealize Network Insight 设置

6

您可以从 vRealize Network Insight 设置页面配置 的各个方面。要访问设置页面，请单击配置文件 > 设置。

本章讨论了以下主题：

- 查看系统运行状况
- 配置数据保留时间间隔
- 配置 IP 属性和子网
- 配置事件和通知
- 配置身份与访问管理
- 配置日志
- 配置邮件服务器
- 配置 SNMP 陷阱目标
- 管理许可证
- 配置自动刷新时间间隔
- 配置用户会话超时
- 添加 Google Maps API 密钥
- 查看审核日志
- 加入或退出客户体验提升计划
- 查看安装的运行状况
- 启用支持通道
- 管理磁盘利用率
- 查看节点详细信息
- 创建支持包
- 了解收集器和平台负载的容量

查看系统运行状况

在 vRealize Network Insight 中，可以查看系统的运行状况。系统运行状况由进程滞后、索引器滞后和网格使用率确定。如果所有这些参数都处于绿色状态，则说明系统运行状况良好。如果这三个参数中的任何一个处于红色状态，则说明系统运行状况不佳。

步骤

- ◆ 在**设置**页面上，单击**安装和支持**。

在**安装和支持**页面中，会看到**系统运行状况**部分。

注 如果系统运行状况处于不良状态的时间超过六小时，则必须与 vRealize Network Insight 支持部门联系。

配置数据保留时间间隔

在 vRealize Network Insight 中，可以指定要保留数据的时间。

注 vRealize Network Insight 仅支持在企业许可证上进行可配置的数据管理。在高级许可证版本中，数据保留默认为 1 个月。

数据分为以下几类：

表 6-1.

类别	最小值	最大值
事件	1 个月	13 个月
实体和配置数据	1 个月	3 个月
衡量指标	1 个月	13 个月
流	不适用	1 个月
杂项数据	不适用	100 GB 的额外磁盘空间

注 对于所有类别，最小值是默认值。

可以为每个类别配置和控制不同的策略。可以根据您的需要配置策略。

要配置数据管理，请执行以下操作：

- 1 在主页的右上角，单击 ，然后单击**设置**。
- 2 在**设置**部分中，单击**数据管理**。
- 3 首次登录时，此页面显示默认数据。
- 4 有关数据如何占用磁盘的详细信息，请单击信息图标。

- 5 单击**更改策略**以更改各种数据类别的数据保留期。进行更改后，信息将记录在数据库中。
- 6 单击**提交**。

注 低分辨率衡量指标的保留期比高分辨率衡量指标的长。

配置 IP 属性和子网

在 vRealize Network Insight 中，您可以配置不同的 IP 属性，以便更好地进行安全性规划和识别。

导入 DNS 映射文件

要为物理设备之间的流提供信息，可以导入 DNS 映射文件。DNS 映射文件的支持格式为 Bind 和 CSV 文件格式。请确保已将这些文件放置在单个 ZIP 文件中。

注 vRealize Network Insight 不支持受密码保护的 ZIP 文件。

步骤

- 1 在**设置**页面中，单击 **IP 属性和子网**。
- 2 单击**物理 IP 和 DNS 映射**。
- 3 单击**上载并替换**以上载 DNS 映射文件。选择并上载文件后，单击**验证**。验证后，将显示 DNS 记录数。

上载并替换操作将移除任何现有的 DNS 映射，并将其替换为正在导入的映射。DNS 映射文件包含以下三个字段：

- 主机名称
- IP 地址
- 域名

配置子网与 VLAN 之间的映射

可以定义子网与 VLAN 之间的映射。

可以将此映射用于以下操作：

- 通过添加源和目标子网以及与流关联的第 2 层网络，扩充有关从物理到物理流了解的 IP 实体的信息。
- 基于物理地址的子网和 VLAN 规划网络拓扑。

步骤

- 1 在**设置**页面中，单击 **IP 属性和子网**。
- 2 单击**物理 IP 和 DNS 映射**。

- 3 在**设置**页面的 **IP 属性和子网**下，单击**物理子网和 VLAN**。

此页面列出所有子网和关联的 VLAN ID。

- 4 单击**添加**以添加子网和 VLAN 信息。

- 5 定义映射信息后，只能编辑与子网关联的 VLAN ID。不能更改为与 VLAN Id 关联的子网 CIDR。要编辑与 VLAN ID 关联的子网，请删除要编辑的子网，然后创建具有所需值的子网 VLAN 映射。

更新子网-VLAN 映射信息时，将为指定的 VLAN ID 创建新的 VLAN，子网信息将与此 VLAN 关联。

- 6 要删除子网-VLAN ID 映射，请单击删除图标。

注 创建子网和 VLAN 映射后，所有 VLAN 创建、更新和删除操作都不会立即发生。传播更改以及创建或修改对应的 VLAN 需要一些时间。

配置东西向 IP

在 RFC1918 标准范围内的 IP 被视为专用 IP。在 RFC1918 之外的 IP 被视为 Internet IP。但是，用户可以指定他们希望在标记流和微分段时视为非 Internet IP 的东西向 IP（数据中心公用 IP），即使它们在 RFC1918 定义的专用 IP 地址范围之外，也是如此。


指定要视为非 Internet IP 的公用 IP

- 1 在主页的右上角，单击“配置文件”图标，然后单击**设置**。
- 2 在“设置”部分中，单击**东西向 IP**。
- 3 在“IP 地址”框中，输入将被视为非 Internet IP 的特定 IP、IP 范围或子网。
- 4 单击**保存**。成功保存后，将显示“IP 地址已保存”确认消息。

配置南北向 IP

RFC1918 空间中的 IP 分类为南北向 IP。用户可以在标记流和微分段时指定其南北向 IP。

要指定南北向 IP，请执行以下操作：

- 1 在主页的右上角，单击“配置文件”图标 ，然后单击**设置**。
- 2 在“设置”部分中，单击**南北向 IP**。
- 3 在“IP 地址”框中，输入特定的 IP、IP 范围或子网。
- 4 单击**保存**。成功保存后，将显示“IP 地址已保存”确认消息。

配置事件和通知

在 vRealize Network Insight 中，您可以配置各种类型的事件和通知。每当系统满足预设规则时，vRealize Network Insight 都会创建一个事件。

在**设置**页面上，单击**事件**以查看各种类型的事件：

- **系统事件**

- 用户定义的事件
- 平台运行状况事件

查看和编辑系统事件

事件由系统或用户定义。系统事件是预定义的事件。

系统事件在**系统事件**页面中的**设置**下列出。为每个事件指定了以下字段。可以基于您的要求在除了“事件”列外的所有以下列中筛选信息。

表 6-2.

列	描述
事件	此字段指定事件的名称。
严重性	此字段指定事件的严重性。可以将其设置为以下值： <ul style="list-style-type: none"> ■ 严重 ■ 中等 ■ 警告 ■ 信息
类型	此字段指定事件表示 问题 还是 更改 。 注 类型为 问题 的所有事件都将记录到 syslog 中。
实体	此字段指定将事件配置为包括或排除用于生成事件的实体。默认情况下，值为 all 。
通知	此字段指定发送的通知类型。通知可以通过电子邮件和/或 SNMP 陷阱发送。 注 您必须为所有关键系统定义的事件启用通知。要获取所有关键系统事件的列表，请按严重性对系统事件进行排序。
已启用	如果已启用事件，则选择此选项。

将鼠标悬停到每个事件上时，可以查看**详细信息**。通过单击此选项，可以查看该事件的说明、事件标记和实体类型。

可以对系统事件执行以下任务：

- 编辑事件
- 执行批量编辑
- 为特定实体禁用事件

严重系统事件列表

本部分提供了严重系统事件的列表。要接收有关严重系统事件的通知，您必须为每个严重事件启用通知。

有关编辑事件的详细信息，请参见“编辑系统事件”。

名称	实体类型
AWS 限制: 每个安全组的入站规则数	AWS 防火墙规则
AWS 限制: 每个安全组的出站规则数	AWS 防火墙规则
AWS 限制: 每个 AWS VPC 的安全组数	AWS 安全组
AWS 限制: 每个网络接口的安全组数	AWS 安全组
AWS 限制: 每个区域的安全组数	AWS 安全组
ECMP 群集中的所有 NSX Edge 当前都已关闭	VMware Edge 设备
两个 NSX Edge HA 虚拟机处于活动状态	VMware Edge 设备
Check Point 网关 SIC 状态未处于通信状态	Check Point 安全管理器
在主机上未找到 Check Point 服务虚拟机	Check Point 安全管理器
关键 NSX 系统事件	-
无法从 NSX Edge 或外部路由器访问 DLR 网络	VRF
没有为一个或多个逻辑交换机建立主机控制层面到控制器的连接	主机
无法访问具有基础架构虚拟机的主机	主机
主机的 VTEP 计数与群集不匹配	群集
未找到服务节点的 IP	-
未在 NSX Manager 与主机之间建立消息总线和/或控制层面连接	模块
找到多个与服务节点 IP 对应的网卡	-
NSX Edge 虚拟机未处于活动/自身状态	VMware Edge 设备
在主机上未找到用于 Check Point 的 NSX 结构层代理	主机
在主机上未找到 NSX 结构层代理	主机
NSX Manager 到 Edge 虚拟机通信失败	VRF
未在主机上检测到 NSX VIB 或主机模块	模块
NSX 基础架构虚拟机未打开电源	虚拟机
NSX 管理服务未运行	-
NSX-T Edge 节点未连接快照器	NSX-T 传输节点
NSX-T Edge 节点未连接管理器	NSX-T 传输节点
在就绪主机上找不到 VTEP	主机
一个或多个 BGP 邻居未处于已建立状态	VMware Edge 设备
Palo Alto Panorama 未在 NSX Manager 中注册	PAN Manager

名称	实体类型
在主机上未找到 Palo Alto 服务虚拟机	PAN Manager
池成员已关闭	池成员
池为空	-
池已关闭	-
Check Point 和 NSX Manager 之间的服务虚拟机状态不匹配	Check Point 安全管理器
Panorama 和 NSX Manager 之间的服务虚拟机状态不匹配	PAN Manager
与池成员关联的虚拟机已关闭	-
已禁用负载均衡器的虚拟服务器	虚拟服务器
VeloCloud Edge 事务性 QOE 已降级	VeloCloud Edge
VeloCloud Edge 视频 QOE 已降级	VeloCloud Edge
VeloCloud Edge 不正常	VeloCloud Edge
VeloCloud 链路事务性 QOE 已降级	VeloCloud Edge
VeloCloud 链路视频 QOE 已降级	VeloCloud Edge
VeloCloud 链路语音 QOE 已降级	VeloCloud Edge
VeloCloud 链路不正常	VeloCloud 链路
VeloCloud Edge 不正常	VeloCloud Edge
VeloCloud 链路不正常	VeloCloud 链路
应用程序数据包丢失超过阈值	SD-WAN Edge 应用程序
VeloCloud 链路上游数据包丢失超过阈值	VeloCloud 链路
VeloCloud 链路下游数据包丢失超过阈值。	VeloCloud 链路

编辑系统事件

您可以编辑系统事件，并定义首选系统事件的通知。

步骤

- 1 单击特定事件的**已启用**列旁边的编辑图标。
- 2 根据需要添加或移除事件标记。
- 3 更改严重性。

4 如果要为所选实体启用或禁用该事件，选择“包括实体”/“排除实体”。

- 要创建包含规则，请执行以下操作：
 - a 选择**包含列表**。
 - b 在**条件**下指定要为事件包括的实体。
- 要创建排除规则，请执行以下操作：
 - a 选择**排除列表**。
 - b 在**条件**下指定要为事件排除的实体。

注

- 可以在包含和排除列表中创建多个规则。
 - 选择 NSX Manager 时，可以在这两个列表中添加例外。如果希望包含或排除规则保留特定实体的例外，则可以定义例外。
 - 也可以通过编写自己的查询以包括或排除实体来指定 Custom Search。
-

5 选择**启用通知**以配置何时必须发送通知。

- 要设置电子邮件服务器，请单击[配置邮件服务器](#)。
 - 要设置 SNMP 服务器，请单击[配置 SNMP 陷阱目标陷阱](#)。
-

注 如果您已配置，这些选项将不可用。

6 执行下列步骤：

- 对于电子邮件通知，指定希望接收电子邮件的电子邮件地址和频率。
 - 对于 SNMP 通知，选择将 **SNMP 陷阱发送到 IP-address**。
- 您可以单击**更改**以修改 SNMP 配置。

7 单击**提交**。

对事件执行批量编辑

- 1 在**系统事件**页面中，选择多个事件时，选项**启用**、**禁用**和**编辑**将显示在列表上方。
- 2 单击**编辑**。
- 3 在**编辑**页面中，具有以下选项：
 - **替代现有值**：在此选项中，仅覆盖您编辑的字段。
 - **添加到现有**：在此选项中，可以添加到现有值，如电子邮件地址和事件标记。
- 4 单击**提交**。

禁用事件

- 1 可以在主页上的**未解决的问题**小组件中选择事件。也可以在搜索栏中输入**问题**，然后从列表中选择事件。
- 2 选择特定事件，然后单击**存档**。
- 3 选择**将来禁用此类型的所有事件**，然后选择一个实体或所有实体。
- 4 单击**保存**。

注 在严重性、标记或包含/排除规则中进行的更改会在将来的事件中得到反映。现有事件继续显示旧配置。

事件限制

本部分提供了各种系统定义的事件的限制。

分布式防火墙规则被前面的规则事件限制屏蔽

此事件存在以下限制：

- 仅 NSX-V 分布式防火墙规则支持此事件。不支持其他防火墙供应商。
- 当前支持以下防火墙规则属性以进行屏蔽计算：
 - 源
 - 目标
 - 应用对象
 - 服务协议和端口范围
 - 数据包类型
 - 第 7 层应用程序 ID
- 不支持具有源或目标反转的规则。
- 禁用的规则将被忽略。
- 不支持安全组直接或间接地在“源” / “目标”或“应用对象”中包含已排除成员的规则。
- “源”、“目标”和“应用对象”属性的屏蔽计算基于成员 IPSet 的静态成员资格和 IP 范围重叠。不考虑安全组的动态成员资格进行屏蔽。

编辑用户定义的事件

用户定义的事件基于搜索。

所有用户定义的事件均在**用户定义的事件**页面上的**设置**下列出。为每个事件指定了以下字段。

表 6-3.

字段	描述
名称 (搜索条件)	此字段指定事件的名称和事件的搜索条件。
严重性	此字段指定警示的严重性。可以将其设置为以下值： <ul style="list-style-type: none"> ■ 严重 ■ 中等 ■ 警告 ■ 信息
类型	此字段指定事件是表示出现问题还是发生更改。
通知时间	此字段指定必须发送通知的时间。
创建者	此字段指定创建事件的人员。
已启用	如果已启用事件，则选择此选项。

可以编辑或删除事件。编辑它时，可以指定电子邮件地址和电子邮件通知的频率。

配置用户定义的事件

您可以通过搜索创建用户定义的事件。

步骤

- 1 单击搜索结果窗口中的创建通知图标。
此时将打开“配置用户定义的事件”页面。
- 2 为事件输入唯一的名称。
- 3 选中相应的复选框将事件标记为问题，并选择严重性。
- 4 输入唯一的搜索条件。
- 5 选择要接收通知的条件。
- 6 将通知频率选择为**立即**或**作为每日摘要**。
- 7 指定电子邮件地址。
- 8 要配置 SNMP 服务器，单击**配置 SNMP 陷阱**。
如果已配置 SNMP 服务器，则选择将 **SNMP 陷阱**发送到 *IP-address*。
您可以单击**更改**以修改 SNMP 配置。
- 9 单击**保存**。

查看平台运行状况事件

“平台运行状况事件”页面是一站式页面，可查看提供有关系统整体运行状况的详细信息的所有事件。这些事件可能发生在基础架构中的数据源或节点上。您也可以通过搜索查看这些事件。

表 6-4.

字段	描述
事件	此字段指定事件的名称。
严重性	此字段指定事件的严重性。不能更改事件的严重性。
类型	此字段指定事件是表示出现问题还是发生更改。
通知	此字段指定发送的通知类型。通知可以通过电子邮件和/或 SNMP 陷阱发送。

通知

基于搜索的通知

基于搜索的通知可分为以下几类：

- 基于系统的通知
- 用户定义的通知

基于系统的通知参数是预定义的，并在激活通知警示时以邮件形式发送通知。用户定义的通知由用户根据其要求进行设置。可以根据搜索查询创建电子邮件通知。运行搜索后，将在“结果”页面上显示**创建通知**选项。对于每个搜索，可以：

- 选择要接收通知的条件。
- 定义要接收通知的频率。
- 输入每个通知的电子邮件收件人（默认情况下，您的电子邮件 ID 显示在收件人列表中；您也可以添加多个电子邮件 ID）。

对于用户定义的搜索：

- 必须为基于搜索的通知分配名称。
- 必须为标记为问题的基于搜索的事件选择严重性。
- 用户定义的事件由搜索条件唯一标识。
- 可以将通知频率指定为**立即**或**作为每日摘要**。

可以从**设置 > 基于搜索的通知**页面管理通知。在**基于搜索的通知**页面上，可以查看现有的通知，对其进行编辑，将其激活或取消激活，也可以删除不需要的通知。

配置事件通知

通知以电子邮件的形式发送。

要设置通知，您必须先配置邮件服务器。要了解如何配置邮件服务器，请参见[配置邮件服务器](#)。

指定要发送电子邮件通知的事件

用户可以指定要为其发送邮件通知的事件。

指定事件

- 1 在**设置**页面上，单击**基于搜索的通知**，或者仅使用“搜索”框搜索任何信息。
- 2 在“基于搜索的通知”页面上，单击**创建通知**图标。将显示通知对话框。
- 3 在**接收通知时间**框中，选择要为其发送通知的事件。
- 4 在**通知**框中，选择发送通知的频率。
- 5 如果不希望出现该事件，则选中**将其标记为问题**复选框。
- 6 输入要向其发送通知的电子邮件地址，然后单击**保存**。

注 要验证通知邮件是否已正确设置，请单击**发送测试电子邮件**。

事件通知

vRealize Network Insight 包含一个预定义的系统事件（系统问题和系统更改）的列表，您可以每隔四个小时接收一次自动电子邮件通知，并对此进行修改。

可以在**设置 > 系统通知**页面上查看通知列表。

如果您尚未为事件配置任何电子邮件或 **SNMP** 通知，则会在主页上看到一条警示消息，提醒并允许您定义通知。您可以单击警示消息中的**启用通知**，以便直接导航到“系统事件”页面并订阅首选事件的通知。

要禁用提醒，请选择**不再显示此消息**选项。不会为该特定用户显示警示消息。要稍后定义通知，请导航到**设置 > 事件**。

将问题存档

将问题存档

- 1 单击“全部显示”链接（如果事件有多个实例）以显示事件的所有实例。
- 2 将鼠标悬停在要存档的事件实例上以显示一组图标，然后单击“存档”图标。
- 3 在事件特定的对话框中
 - a 如果要仅将此事件存档，则从“将要存档”列表中选择“此事件”。
 - b 如果要将同一类型的所有事件存档在系统中，则从“将要存档”列表中选择此类型的所有事件。
- 4 单击**保存**。

查看所有已存档的事件

- 1 在主页上，在“搜索”框中键入事件，然后按 **Enter**。将显示事件列表。

- 2 在左侧窗格的“已存档”面中，选中“True”复选框（在下面的屏幕快照中突出显示）。

在此处可以查看所有已存档的事件。

还原已存档事件

- 1 在已存档事件上，单击“已存档”图标。（请参见上一部分“查看已存档事件”以了解如何转到“已存档事件”页面）。
- 2 在事件特定的对话框中
 - a 如果要仅还原此事件，则从“将要从存档还原”列表中选择“此事件”。
 - b 如果要还原所有类似类型的事件，则从“将要从存档还原”列表中选择此类型的所有事件。
 - c 单击“保存”以完成还原。

禁用事件

用户可以有选择地禁用事件以及阻止将来发送通知。

禁用事件通知

方法 1

- 1 在事件上，单击**全部显示**链接（如果事件有多个实例）以显示该事件的所有实例。
- 2 将鼠标悬停在要禁用其通知的事件的实例上。这将显示一组图标，单击“存档”图标。
- 3 在“事件特定”对话框中，选中**将来禁用此类型的所有事件**复选框，然后单击**保存**。

方法 2

- 1 在主页的右上角，单击**配置文件**图标，然后单击**设置**。
- 2 在**设置**部分中，单击**事件通知**以查看所有已启用和已禁用事件的列表。
- 3 在要禁用的已启用事件上，在**已启用**列中，单击相应滑块的左侧空白。
- 4 在**确认操作**对话框中，单击**是**。

配置事件通知服务

用户可以为不同事件启用客户通知

设置通知服务

- 1 在“设置”上，转到“事件通知”，然后单击与要为其启用电子邮件通知和 **SNMP** 的问题相对应的（编辑）图标。
- 2 在“编辑系统通知”对话框中，输入要向其发送电子邮件通知的电子邮件地址。在“电子邮件频率”框中，选择要接收通知的时间频率。
- 3 选中“为此事件启用 **SNMP** 陷阱”复选框，以设置 **SNMP** 通知。
- 4 单击**保存**。
- 5 成功启用后，将显示相应的邮件和 **SNMP** 图标（在下面的屏幕快照中突出显示）。

配置身份与访问管理

在 vRealize Network Insight 中，您可以创建用户或者配置 LDAP 用户和 VMware Identity Manager 用户的访问权限。您还可以为用户分配不同的角色。

配置 LDAP

在 vRealize Network Insight 中，您可以配置 LDAP 用户的访问权限。

vRealize Network Insight 支持以下两种类型的用户：

- 在 vRealize Network Insight 平台虚拟机上创建的用户
- LDAP 用户

要允许 LDAP 用户登录到 vRealize Network Insight，请在 vRealize Network Insight 平台中配置 LDAP 服务，如下所示：

启用基于 LDAP 的用户身份验证

- 1 在**设置**页面上，单击**身份与访问管理 > LDAP**。
- 2 单击**配置**。
- 3 在**配置 LDAP** 页面上，在相应的框中键入适当的域、LDAP 主机 URL 和 LDAP 凭据。请参见下表以了解各个字段的说明。

表 6-5.

字段	描述
域	这通常是用户电子邮件地址在“@”符号之后的最后一部分。示例：对于以 johndoe@example.com 登录的用户，此字段为 example.com
LDAP 主机 URL	可以指定多个用逗号分隔的 LDAP 主机 URL。
用户名	具有使用所提供设置进行登录所需权限的用户。
密码	用户的密码。

可以配置一个组，并为该组的成员提供角色。要启用此功能，请选择**基于组的访问控制**。

- a 在**基本 DN** 下，键入基本 DN，即服务器开始搜索用户的位置。
- b 在**组 DN** 下，添加组。
- c 对于每个组，从下拉菜单中选择用户的角色，即作为成员或管理员。如果为特定组选择管理员角色，则该组的所有成员都具有管理员特权。同样，如果为特定组选择成员角色，则该组的所有成员都具有成员特权。如果未选择此选项，则使用组设置分配特权。但是，不属于您已添加组的其他有效 LDAP 用户可以登录到产品。
- d 单击**添加更多**以在包含列表中添加组。

要仅允许访问所添加的 LDAP 组中的用户（直接或继承的成员资格），请选中**只能访问上述组的成员**复选框。

4 单击**提交**以配置 LDAP。

LDAP 配置成功后，登录屏幕上会显示一个新的下拉菜单，用户可以选择是希望在本地上登录还是使用其 LDAP 凭据进行登录。

LDAP 凭据未保存在任何位置。

有关组和继承的注意事项

- 对于在“组 DN”下添加的组，其子组也可以使用 LDAP 凭据进行登录。
- 角色分配不考虑继承。例如，如果用户必须是管理员，则应向该用户所属的直接组分配管理员角色。属于子组的用户将不具有管理员角色。
- 假定将管理员角色分配给组，并且要使该组中的某特定用户不具有管理员角色，请执行以下步骤：
 - a 在**设置**页面上，单击**用户管理**。
 - b 在 **LDAP 用户** 选项卡下，可以看到为该特定用户分配的角色，还可以看到该角色从组继承。
 - c 单击编辑图标。在**角色**下，从该用户的下拉菜单中选择**成员**。这样就可以将角色直接分配给用户。
 - d 单击**保存更改**。
 - e 输入密码以进行确认。单击**授权**。
- 假定您希望用户从其所属的组继承角色，请执行以下步骤：
 - a 在**设置**页面上，单击**用户管理**。
 - b 在“LDAP 用户”选项卡下，可以看到为该特定用户分配的角色，还可以看到该角色直接分配给用户。
 - c 单击删除图标以删除该 LDAP 用户。
 - d 该特定用户登录时，默认情况下用户会从父组继承角色。
- 用户登录时，如果某人更改了该用户所属组的角色，则只有在该用户注销后新角色才生效。
- 假定有一些 LDAP 用户在升级之前已登录。升级后，这些 LDAP 用户具有直接角色且不从组继承。
- 假定某用户属于多个组。例如，某用户属于组 A、组 B 和组 C。如果为组 A 分配了管理员角色，为组 B 和组 C 分配了成员角色，则该用户将继承管理员角色。

配置 VMware Identity Manager (vIDM)

管理员可以授权 VMware Identity Manager 用户根据其角色访问 vRealize Network Insight 功能。

前提条件

将 vRealize Network Insight 作为 OAuth 客户端注册到 VMware Identity Manager 主机。有关详细信息，请参见 [VMware Workspace ONE Access 文档](#)。

步骤

- 1 登录到 vRealize Network Insight 并单击**设置**。
- 2 在“身份与访问管理”下，选择 **vIDM**。
- 3 提供以下信息。

参数	描述
VMware Identity Manager 设备	VMware Identity Manager 主机的完全限定域名 (FQDN)。
OAuth 客户端 ID	在将 vRealize Network Insight 注册到 VMware Identity Manager 主机时创建的 ID。
OAuth 客户端密钥	在将 vRealize Network Insight 注册到 VMware Identity Manager 主机时创建的密钥。
SHA-256 指纹	这是可选字段。VMware Identity Manager 主机的证书指纹。有关详细信息，请参见 从 VMware Identity Manager 主机获取证书指纹 。

- 4 单击**提交**。
配置后，您会看到 VMware Identity Manager 设备和已配置的客户端详细信息。
- 5 单击切换按钮以启用或禁用 VMware Identity Manager。如果禁用，则无法在 vRealize Network Insight 中使用 VMware Identity Manager 身份验证。

从 VMware Identity Manager 主机获取证书指纹

对于 SSL 证书验证，您可以从 VMware Identity Manager 主机获取 SHA-256 指纹。

步骤

- 1 要获取 SSL/TLS 证书，请运行以下命令：

```
openssl s_client -connect <FQDN of vIDM host>:443
```

将服务器证书（从 -----BEGIN CERTIFICATE----- 到 -----END CERTIFICATE-----）复制到 cert.pem 文件中，然后保存该文件。

- 2 要获取指纹，请运行以下命令。

```
openssl x509 -fingerprint -noout -sha256 -in cert.pem
```

结果

您会看到以下格式的指纹：

SHA256

```
Fingerprint=3D:E8:4C:CD:19:D6:AD:23:30:86:E4:A1:72:D5:22:08:F9:72:6D:D3:E7:6E:99:32:C8:C7:3D:F8:E2:91:91:AE
```

后续步骤

复制指纹并将其粘贴到“配置 VMware Identity Manager”页面。

配置用户管理

在 vRealize Network Insight 中，您可以为用户添加、管理和分配角色。

您可以为用户分配成员角色或管理员角色。

管理员拥有对 vRealize Network Insight 设置的完全访问权限。管理员可以添加数据源、添加用户、管理用户、配置 SNMP 和邮件服务器等。成员用户拥有对 vRealize Network Insight 设置的有限访问权限。在**设置**页面中，成员用户可以查看和编辑系统和平台运行状况事件、查看用户定义的事件、访问属性和应用程序发现模板、访问我的首选项以及查看和复制服务标记。

添加新用户

- 1 在**设置**页面中，单击**身份与访问管理 > 本地用户 > 添加新用户**，然后在表单中提供所需的信息。

该表单包含以下文本框：

属性	描述
名称	输入用户的名称。
电子邮件 (登录 ID)	输入电子邮件或登录 ID（如果有）。
角色	从下拉列表中选择角色。
密码	输入密码。
重新输入新密码	重新输入密码以进行确认。

- 2 单击**添加用户**以保存用户信息。

分配管理员角色

可以将管理员角色分配给任何 LDAP 用户。

即使该特定用户未登录，仍可以将管理员角色分配给该用户。要分配管理员角色，请执行以下操作：

- 1 在**设置**页面中，单击**身份与访问管理 > LDAP 用户 > 分配管理员角色**。
- 2 提供要为其分配管理员角色的用户的登录 ID。
- 3 单击**添加用户**。
- 4 添加用户后，可以在“LDAP 用户”选项卡中查看登录 ID。
- 5 要更改角色，请单击“LDAP 用户”选项卡中登录 ID 旁边的编辑图标。

从 VMware Identity Manager 导入用户

您可以导入 VMware Identity Manager 用户帐户以允许他们使用 vRealize Network Insight 并为其分配角色。

步骤

- 1 在 vRealize Network Insight “设置”页面上，展开**身份与访问管理**。

- 2 单击**用户管理**，然后选择 **VIDM** 选项卡。
- 3 提供所需的详细信息。

字段名称	描述
域名	输入要导入的 VMware Identity Manager 域名。
搜索用户/组	输入搜索字符串，然后从自动完成列表中选择用户帐户。您可以选择单个用户，也可以选择一个用户组。如果选择一个组，则该组中的所有成员都可以访问 vRealize Network Insight。
角色	将 成员 或 管理员 角色分配给用户帐户。

- 4 单击**添加用户**。

注

- 如果选择了一个组，则该组中的所有成员都将获得相同的角色。如果要为组中的特定用户分配不同的角色，则必须单独添加该用户，并分配所需的角色。

例如，要将**管理员**角色仅分配给 *Mygroup* 中的 *user1*:

- 添加 *Mygroup* 并分配**成员**角色，
- 添加 *user1* 并分配**管理员**角色。

分配给用户的角色会直接覆盖作为组成员分配给用户的角色。

- 如果用户属于具有不同角色的多个组，则会将最高特权角色分配给该用户。

例如，如果用户属于具有**管理员**角色的 *Group A*，同时还属于具有**成员**角色的 *Group B* 和 *Group C*，则用户将继承**管理员**角色。

结果

现在，此 VMware Identity Manager 用户或组成员可以登录到 vRealize Network Insight，并根据分配的角色使用这些功能。

配置日志

在 vRealize Network Insight 中，您可以查看和配置不同类型的日志。

查看和导出审核日志

审核日志捕获在系统中执行的管理操作。它们是常规的 CRUD 操作以及登录和注销事件。将记录通过 UI、CLI 或 API 执行的管理操作。

审核日志从 API、UI 和 CLI 捕获操作。

功能

- 审核日志功能始终处于打开状态。
- vRealize Network Insight 在审核日志中支持 UTC 格式。
- 审核日志与 syslog 集成在一起。可以将 syslog 收集器配置为收集所有审核日志。

- 可以在 CSV 文件中导出所有审核日志数据。

设置 Syslog 配置

可以使用 **Syslog 配置** 页面为 vRealize Network Insight 配置远程 syslog 服务器。

虽然每个代理服务器有可能具有不同的远程 syslog 服务器，但是群集中的所有平台服务器都使用同一个远程 syslog 服务器。

在当前版本中，vRealize Network Insight 问题事件和平台/代理服务器 syslog 将发送到远程 syslog 服务器。

当前，vRealize Network Insight 仅对 vRealize Network Insight 服务器和远程 syslog 服务器之间的通信支持 UDP。因此，请确保您的远程 syslog 服务器已配置为接受通过 UDP 的 syslog 流量。

要配置 syslog，请执行以下操作：

- 1 在**设置**页面中，单击 **Syslog 配置**。**Syslog 配置** 页面将列出配置的 syslog 服务器及其到虚拟设备的映射。如果您是首次访问此页面，则默认情况下禁用 syslog，且不会在此页面上显示服务器列表。
- 2 要添加 syslog 服务器，请执行以下操作：
 - a 单击**添加 Syslog 服务器**。
 - b 输入服务器的 IP 地址、昵称和端口号。用于 UDP 的标准端口号为 514。
 - c 要测试配置，请单击**发送测试日志**。
 - d 单击**提交**。
 - e 如果这是您添加的第一个服务器，则在页面顶部启用 syslog。
- 3 要将服务器映射到平台和代理，请执行以下操作：
 - a 单击**编辑映射**。
 - b 为所有平台和代理服务器选择该 syslog 服务器。
 - c 如果不希望在任何代理服务器或平台上启用 syslog，请选择**无服务器**选项。
 - d 单击**提交**。

注 进行更改后，可能需要几分钟才能使这些更改生效。

配置邮件服务器

在 vRealize Network Insight 中，您可以配置邮件服务器以通过邮件接收事件通知。

要配置邮件服务器，请执行以下操作：

- 1 在主页的右上角，单击**配置文件**图标，然后单击**设置**。
- 2 单击**邮件服务器**。
- 3 选中“SMTP 服务器”复选框。

- 在框中输入相应的值。

表 6-6.

字段	描述
发件人电子邮件	发件人的电子邮件地址。
SMTP 主机名/IP 地址	SMTP 服务器的主机名或 IP 地址。
加密	以下加密选项是可用的：“无”、“TLS”和“SSL”。
SMTP 端口号	SMTP 服务器的端口号（默认为 25）。

注 要使用 Gmail 服务器作为电子邮件服务器，需要 Google 支持中列出的其他配置设置。

（可选）要增强安全性，请选中“身份验证”复选框，然后输入用户名和密码。

注 要验证通知邮件是否已正确设置，请单击**发送测试电子邮件**。

- 单击**提交**以完成配置。

配置 SNMP 陷阱目标

在 vRealize Network Insight 中，您可以配置简单网络管理协议 (SNMP) 陷阱以接收邮件通知。产品支持以下 v2c 和 v3 版本的 SNMP：

- 在主页的右上角，单击“配置文件”图标，然后单击**设置**。
- 选择 **SNMP 陷阱目标**。
- 在“SNMP 陷阱目标”页面的“版本”框中，选择“SNMPv2c”或“SNMPv3”协议。

注 SNMPv2c 协议不需要身份验证。SNMPv3 协议支持身份验证。

- 在“目标 IP 地址/FQDN”框中，输入 SNMP 代理的 IP 地址，或输入完全限定域名 (FQDN)。
- 在“目标端口”框中，输入 **162**。
- 如果选择 SNMPv2c 协议，则在“社区字符串”框中输入**公用**。如果选择 SNMPv3 协议，则在“用户名”框中输入在 SNMP 代理中创建的用户名。

对于 SNMPv3，还需要执行以下操作：

- 选中**使用身份验证**复选框。
- 选择身份验证协议，然后输入在 SNMP 代理中为特定用户设置的密码。（可选）在“隐私协议”和“隐私短语”框中，分别选择隐私协议和隐私短语。

要验证配置是否已正确完成，请单击**测试 SNMP 陷阱**，然后查明陷阱是否已发送到 SNMP 代理。

- 单击**提交**。

管理许可证

VMware 遵循 vRealize Network Insight 许可的诚信制度，这意味着出现任何违反许可证计数的行为，系统都会在用户界面上显示一条警告消息，但不会限制您使用可用功能。

在以下情况下，您会在 UI 的所有页面上看到许可证警告消息：

- 超出插槽 (CPU) 许可证的许可证使用量。
必须添加其他许可证才能支持您的要求。
- 混用许可证类型
 - 添加了高级许可证和企业级许可证。
从高级版本升级到企业版后，必须手动删除高级许可证（**设置 > 许可证和使用情况**）。确保您有足够数量的企业级许可证，以便使用企业功能。
 - 添加了一个插槽许可证和一个核心许可证。
根据您的要求，删除其中一个许可证类型。

许可证使用情况计算

vRealize Network Insight 许可证使用情况是根据以下比率计算的。

对象	描述	每个插槽许可证允许的对象计数
VMware vSphere CPU	内部部署主机的 CPU 插槽总数	1
VMware Cloud on AWS 主机	VMware Cloud on AWS 主机总数	0.5
AWS vCPU	AWS 实例的 vCPU 总数	16
非 VMware 端点	非 VMware 流报告功能（例如，来自物理交换机的 NetFlow）专门报告的流中显示的非 Internet 和非 VMware 端点的总数	15
Kubernetes POD	Kubernetes POD 总数	12

注 vRealize Network Insight 还会在计算许可证使用情况期间考虑禁用的数据源。如果希望 vRealize Network Insight 在计数期间忽略这些数据源，请删除这些数据源。

SD-WAN 许可证

要在 vRealize Network Insight 中将 VMware SD-WAN 添加为数据源并查看 VMware SD-WAN 部署，必须添加 VMware SD-WAN 许可证。可以将 VMware SD-WAN 许可证添加为独立许可证，也可以将其与企业许可证一起使用。但是，不能将 VMware SD-WAN 许可证与高级许可证一起使用。可以使用多个 VMware SD-WAN 许可证密钥支持不同带宽的 Edge。

使用 VMware SD-WAN 许可证，除了 VMware SD-WAN 数据源之外，还可以添加不带 IPFIX、交换机和路由器以及 Infoblox 的 vCenter。

添加并更改许可证

此页面显示许可证使用情况详细信息，并允许您添加许可证。vRealize Network Insight 支持添加多个许可证。

添加许可证

要添加许可证，请执行以下操作：

- 1 在“许可证和使用情况”页面上，单击**添加许可证**。
- 2 为**新许可证密钥**字段提供许可证密钥。
- 3 单击**验证**。
您将看到许可证类型、许可证可用的套接字或核心计数以及到期详细信息。
- 4 单击**激活**。
- 5 可以在页面中看到许可证列表。
- 6 也可以通过单击“过期”列旁边的删除图标来删除许可证。如果许可证属于企业版，且它是系统中保留的最后一个企业版，则在删除该企业级许可证之前，请确保已删除 AWS 帐户。

更改许可证

如果评估许可证过期，则登录到产品时，会显示一条消息，指出许可证已过期，需要续订许可证。使用以下步骤更改许可证。

要更改许可证，请执行以下操作：

- 1 单击“过期”消息中包含的链接以转到“更改许可证”页面。或者，在**设置**中，单击**许可证和使用情况**，然后单击**更改许可证**。
- 2 在**更改许可证**页面的**新许可证密钥**中，输入从 VMware 收到的新许可证密钥。
- 3 单击**验证**。
- 4 单击**激活**。

注 评估许可证到期后，数据提供程序将被禁用并且会停止收集数据。续订许可证后，必须从 UI 中再次启用数据提供程序才能启动数据收集。

配置自动刷新时间间隔

在 vRealize Network Insight 中，您可以为实体页面和看板配置自动刷新时间间隔。

vRealize Network Insight 为实体仪表板和看板提供了自动刷新功能。仪表板按标题栏中指定的每 n 分钟时间间隔自动刷新一次。

您可以指定希望所有仪表板执行自动刷新的时间间隔。在指定的时间间隔（n 分钟）后，仪表板上所有打开的小组件将自动重新加载。

注

- 您无法更改特定仪表板的自动刷新时间间隔。
- 如果在时间轴滑块中选择过去的时间间隔，则会暂停自动刷新。

如果特定仪表板不需要自动刷新，则可以暂停自动刷新。在标题栏上，将**暂停**设置为**打开**。将**暂停**设置为**关闭**后，自动刷新计数器将重置。

如果您正在查看看板，并且其他用户正在对其进行更改（例如更改看板的布局），则自动刷新功能不仅更新内容，还会刷新整个看板。仅当您与其他用户之间存在共享和协作时，才会发生此问题。

步骤

- 1 在**设置**页面上，单击**我的首选项**。或者在相应的仪表板上，单击标题栏中“自动刷新”旁边的**修改**。
- 2 单击**编辑**以更改自动刷新的时间间隔。从下拉菜单中选择时间间隔。单击**保存**。
- 3 要禁用自动刷新选项，从下拉菜单中选择**已禁用**。如果选择此选项，则会禁止所有仪表板自动刷新。

配置用户会话超时

默认情况下，用户会话超时设置为 15 分钟。您可以根据自己的偏好修改此值。

步骤

- 1 在**设置**页面上，单击**系统配置**。

注 系统配置选项卡仅对 admin user 可见。

- 2 单击编辑图标以更改用户会话超时的首选项。
- 3 拖动滑块栏以设置会话的超时值。该值的范围为从 15 分钟到 24 小时。
- 4 也可以在上次修改字段中查看有关修改超时值的人员和时间的详细信息。
- 5 单击**提交**。将显示成功消息，确认更新的会话持续时间将从下次登录时生效。

注 只有在您先注销再重新登录后，用户会话超时的新值才会生效。

添加 Google Maps API 密钥

要获取 SD-WAN 部署的地图视图，必须在 vRealize Network Insight 中添加 Google Maps API 密钥。

前提条件

确保以下事项：

- 您是 Google Cloud Platform 的成员，并在您的帐户中启用计费。

- 您具有 Google Maps API 密钥。要获取 API 密钥，请参见 Google Maps Platform 文档中的“获取 API 密钥”过程。
- 您已对 API 密钥施加限制以防止任何误用。要了解更多信息，请参见 Google Maps Platform 文档中的“限制 API 密钥”。

步骤

- 1 在**设置**页面上，单击**系统配置**。
- 2 在 **Google Maps API 密钥** 中，输入 API 密钥，然后单击**保存**。

查看审核日志

审核日志捕获在系统中执行的管理操作。它们是常规的 CRUD 操作以及登录和注销事件。审核日志从 API、UI 和 CLI 捕获操作。

- 审核日志功能始终处于打开状态。
- vRealize Network Insight 在审核日志中支持 UTC 格式。
- 审核日志与 syslog 集成在一起。可以将 syslog 收集器配置为收集所有审核日志。
- 可以在 CSV 文件中导出所有审核日志数据。

步骤

- 1 在**设置**页面上，单击**日志**下的**审核日志**。
- 2 在**审核日志**页面上将显示以下详细信息：

信息	描述
Date & Time	执行实际操作的时间戳。
IP Address	从其建立连接的客户端（如 CLI 或浏览器）的 IP 地址。
User Name	正在执行操作的用户。
Object Type	正在对其执行操作的对象。
Operation	用户对对象执行的不同操作。
Object Identifier	对其执行操作的特定对象的唯一标识符。
Response	操作成功或失败的指示器
Details	已更改的设置的详细信息，如昵称或属性。

- 3 要在用户通过浏览器或 CLI 登录时允许收集信息，请启用**允许收集个人身份信息**。默认情况下禁用此选项。

注 如果禁用此选项，则 IP Address 和 User Name 列为空。

- 4 单击**导出为 CSV**以 CSV 格式导出审核日志数据。

加入或退出客户体验提升计划

本产品加入了 VMware 客户体验提升计划 (CEIP)。CEIP 将向 VMware 提供相关信息，以帮助 VMware 改进产品和服务、解决问题、并向您建议如何以最佳方式部署和使用我们的产品。作为 CEIP 的一部分，VMware 会定期收集与贵组织所持有的 VMware 许可证密钥相关的使用 VMware 产品和服务的技术信息。此信息不会识别个人身份。

有关通过 CEIP 收集的数据的详细信息以及 VMware 使用这些数据的目的在“信任与保证中心”中进行了介绍，网址为：<https://www.vmware.com/solutions/trustvmware/ceip.html>。

您可以加入或退出 vRealize Network Insight 的客户体验提升计划 (CEIP)。

- 1 在关于页面中的“客户体验提升计划”下，单击**修改**。
- 2 将弹出 CEIP 窗口。要加入 CEIP，请选中**启用**。此操作将激活 CEIP 并将数据发送到 <https://vmware.com>。
- 3 要退出 CEIP，请取消选中**启用**。
- 4 单击**提交**。

查看安装的运行状况

运行状况指示器在**安装和支持**页面上的**概览**部分中可用。

如果出现以下任一故障事件，则**运行状况**指示器将变为红色：

- 如果代理停止收集流数据
- 如果由于某种原因（例如，磁盘空间不足）平台停止处理数据
- 如果搜索索引器滞后，导致搜索结果过期

整体运行状况指示器显示异常数量，红灯亮起。单击有关整体运行状况的问题数时，将列出各个异常及其详细信息。正常运行时，运行状况指示器发出绿光。

注 vRealize Network Insight 有时可能无法检测到不同步的系统时钟。如果时钟与 NTP 不同步，某些服务可能会变得不正常或停止工作。

启用支持通道

支持通道允许 VMware 远程连接到 SSL 安全连接上的平台和收集器虚拟机，以便进行高级故障排除或调试。



要请求高级支持，请在**安装和支持**页面的**概览**部分中切换**支持隧道**选项。

注 请确保允许到端口 443 上 support2.ni.vmware.com 的流量。

管理磁盘利用率

如果平台或收集器的磁盘利用率很高，则会触发事件以警告用户。此外，还提供了需要另外添加多少磁盘空间的建议。可以在平台或收集器仪表板中查看事件。警示也会显示在**安装和支持**页面的对应收集器或平台部分中。

Platform VMs

IP Address (Name)	Last Activity	Status
 Critical: Disk Utilization is high 		<p>Disk utilization is at 85%. The Platform might run out of disk in 2 days. Add 100 GB more disk space to avoid any service interruption.</p>

可以通过执行以下步骤将磁盘添加到节点：

注 不要扩展现有的硬盘。

步骤

- 1 使用足够的特权通过 Web 客户端登录到 vCenter。
- 2 右键单击节点，然后单击**编辑设置**。
- 3 根据警示中提供的建议添加硬盘。

vRealize Network Insight 需要几分钟的时间检测设备并将其添加到 /var 分区。

查看节点详细信息

可以查看平台或收集器中每个节点的详细信息。

步骤

- 1 要查看特定平台节点的详细信息，请单击在**安装和支持**页面上**平台虚拟机**下列出的其名称。
此时将显示“NI 平台”仪表板。
- 2 要查看特定收集器节点的详细信息，请单击**安装和支持**页面上**收集器 (代理) 虚拟机**下列出的相应名称。
此时将显示“NI 收集器”仪表板。

创建支持包

您可以创建一个支持包，用于收集诊断信息，例如产品特定的日志、设置的配置文件。当您提出支持请求时，VMware 技术支持将使用此信息对您的设置问题进行故障排除。

步骤

- 1 在“设置”页面上，单击**安装和支持**。
- 2 单击**创建支持包**。
- 3 选择要为其创建支持包的平台虚拟机和收集器虚拟机。
要选择所有虚拟机，请单击平台虚拟机和收集器虚拟机表标题中的复选框。
- 4 单击**创建**。
- 5 单击**是**以确认创建新的支持包。

vRealize Network Insight 需要一些时间才能完成支持包的创建。

结果

将创建一个新的支持包，并显示日期和时间。要启动支持包的下载，请单击相应虚拟机旁边的**下载**链接。

注

- 在中型系统上创建支持包可能需要超过十五分钟的时间。
- 一个给定时间只能存在两个支持包。因此，在创建新的支持包时，如果已有两个支持包，则会删除较旧的支持包。

后续步骤

将支持包附加到您的服务请求，以便 VMware 访问详细信息。

了解收集器和平台负载的容量

vRealize Network Insight 提供收集器节点和平台的近似容量和负载信息。基于限制的此信息可帮助您稍后防止性能和体验问题。

了解容量

有以下两种容量：

- **虚拟机容量：**它定义为节点或设置可以处理的已发现虚拟机的数量。
- **流容量：**它定义为节点或设置可以处理的流的数量。

容量定义如下：

- **具有一个或多个代理节点的单个平台：**代理节点或平台的容量是它可以处理但不会降低性能的已发现虚拟机的数量。

- **群集设置：**群集设置中平台的容量是所有平台节点的所有容量的聚合，而代理节点的容量在单个节点级别上进行考虑。

访问容量信息

可以在[安装和支持](#)页面上查看**虚拟机容量**和**流容量**。

对于“收集器 (代理) 虚拟机”下列出的每个收集器节点，仅提供虚拟机容量信息。

注 在整个部署期间从数据源发现的虚拟机数量超过系统和/或收集器的容量时，将不允许您触发升级。

要查看数据源的已发现虚拟机，请执行以下操作：

- 1 在**帐户和数据源**页面中，可以查看已添加且当前处于活动状态的特定数据源的已发现虚拟机的数量。仅当数据源为 vCenter 或 AWS 源时，此列才具有值。

注 已发现虚拟机的计数包括占位符和模板虚拟机。因此，它可以不同于产品中的虚拟机计数。

创建和扩展群集

7

本章讨论了以下主题：

- 创建群集
- 扩展群集

创建群集

可以从[安装和支持](#)页面创建群集。

必备条件

需要至少两个其他平台。应部署其他平台虚拟机并打开其电源。

创建群集

- 1 对于平台虚拟机，单击**创建群集**。
- 2 在**创建群集**页面上，输入以下信息：
 - **IP 地址**：输入要添加的新平台的 IP 地址。
 - **密码**：输入平台虚拟机的支持用户密码。如果尚未更改密码，则参阅《vRealize Network Insight 安装指南》中的“默认登录凭据”部分了解密码。
- 3 要继续添加更多的平台，请单击**添加更多**，然后输入 IP 地址和支持用户密码。
- 4 单击**提交**。单击**是**。
- 5 创建群集后，用户需要再次登录到产品。

注

- 仅当平台采用大型块时，才会启用**创建群集**选项。所有平台都应采用大型块以创建群集。
 - 在单个节点上启用遥测可在所有节点上启用遥测。
 - 要扩展群集，请参阅《vRealize Network Insight 安装指南》中的“扩展群集”部分。
-

扩展群集

创建群集后，您可以通过向其添加更多平台节点来扩展群集。

注 您只能从平台 1 (P1) 节点执行扩展群集操作。

步骤

- 1 在**安装和支持**页面上，为**平台虚拟机**单击**扩展群集**。
- 2 在“扩展群集”页面上列出了已属于群集的虚拟机的 IP 地址。要将一个或多个节点添加到现有群集，请提供节点的 IP 地址和支持用户密码。

注

- 当前，vRealize Network Insight 支持现有群集中的 10 个节点。达到限制后，就会禁用**添加更多**按钮。
 - 请确保所有新节点均未置备且可通过 SSH 进行访问。
 - 在开始扩展群集之前，请确保已制作现有平台虚拟机的备份。
-

- 3 单击**提交**。
将显示分步进度。
- 4 群集扩展链接完成后，将显示一条指示成功的消息。
正在进行群集扩展时，应用程序不能用于任何其他操作。

查看实体详细信息

8

实体页面提供了数据中心中存在的实体的综合外观。此信息涵盖的范围可以从显示与数据中心的其他实体关系的详细拓扑到有关特定实体的详细衡量指标。

每个实体页面都是小组件的集合，且每个小组件都显示与实体相关的特定信息。同时提供实时信息和历史信息，还提供实体的衡量指标和属性的完整列表。

如果要查看有关实体的详细信息，请单击页面右上角的 **配置文件 > 帮助**。

时间轴

时间轴为您提供以下信息：

- 数据中心在过去某个特定时间的状态。
- 在选定时间范围内检测到的事件的鸟瞰视图。

选择要查看的时间轴的时间范围。

要查看特定的时间轴，请通过使用**时间范围**选项来选择时间范围。

属性小组件

属性小组件在两列布局中显示重要属性。某些属性看板项也可能仅显示单个属性值。属性插针的示例是**虚拟机属性**插针。**虚拟机属性**插针显示虚拟机的属性，如操作系统、IP 地址、默认网关、逻辑交换机、CPU、内存、电源状态等。

本章讨论了以下主题：

- [查看 vRealize Network Insight 系统（NI 系统）详细信息](#)
- [查看平台虚拟机详细信息](#)
- [查看收集器虚拟机详细信息](#)
- [查看 VMware vCenter 数据源详细信息](#)
- [查看 PCI 合规性详细信息](#)
- [Object Missing](#)
- [查看负载均衡器详细信息](#)
- [查看虚拟机详细信息](#)

- [查看 NSX Manager 详细信息](#)
- [查看虚拟服务器详细信息](#)
- [查看池成员详细信息](#)
- [查看 Microsoft Azure 详细信息](#)
- [查看 VeloCloud 企业详细信息](#)
- [查看 SD-WAN 和 Edge SD-WAN 应用程序详细信息](#)
- [查看“流洞察”详细信息](#)
- [查看微分段详细信息](#)
- [查看应用程序详细信息](#)
- [分析 - 异常值检测](#)
- [分析：静态和动态阈值](#)

查看 vRealize Network Insight 系统（NI 系统）详细信息

“vRealize Network Insight 系统”页面（“NI 系统”页面）提供与系统相关的所有信息的快照。要访问“vRealize Network Insight 系统”页面，请执行以下操作：

- 在[安装和支持](#)页面上，单击**概览**旁边的[查看详细信息](#)。此时将显示“NI 系统”页面。
- 提供 NI-System 作为搜索查询以查看“vRealize Network Insight 系统”页面。

“NI 系统”页面分为以下三个部分：

- **概览**：此部分包含有关主要属性、数据源、未解决的问题以及与系统相关的所有更改和问题的信息。通过单击每个数据源，可查看其详细信息。
- **事件**：此部分列出系统、数据源、平台和收集器中的所有问题和更改。
- **平台和收集器**：此部分列出与系统关联的所有平台和收集器。要查看有关任何平台或收集器的更多详细信息，请单击它。

查看平台虚拟机详细信息

平台虚拟机页面提供特定平台节点的属性、更改和问题的快照。

在**平台虚拟机**页面中，您可以查看：

- 有关所选平台节点的重要信息，如名称、IP 地址、CPU 内核数、内存、上次升级时间和版本。
- 与平台关联的未决问题。
- 与所选平台节点相关的事件的列表。
- 衡量指标（如 CPU 使用情况、内存使用情况和数据磁盘使用情况）的图形表示。

查看收集器虚拟机详细信息

收集器虚拟机页面提供特定收集器节点的属性、更改和问题的快照。

在**收集器虚拟机**页面中，您可以查看：

- 有关所选平台节点的重要信息，如名称、IP 地址、CPU 内核数、内存、上次升级时间和版本。
- 与收集器相关的未决问题数以及问题详细信息。
- 与数据源相关的未决问题数以及问题详细信息。
- 过去七天内数据源中发生的更改的列表。
- 收集器中可用的数据源和 NetFlow 报告器的详细信息。对于每个 NetFlow 报告器，显示流数。对于数据源，显示流数和发现的虚拟机。
- 衡量指标（如 CPU 使用情况、内存使用情况和数据磁盘使用情况）的图形表示。

查看 VMware vCenter 数据源详细信息

VMware vCenter 数据源页面提供特定数据源的属性、更改和问题的快照。

在“VMware vCenter 数据源”页面中，您会看到：

- 有关选定 VMware vCenter 数据源的重要信息，例如 IP 地址 / FQDN、收集器名称、已启用、已发现的虚拟机数、IPFIX 已启用状态等。
- 与数据源关联的所有未决问题。
- 过去七天内特定数据源中遇到的所有更改和问题。

查看 PCI 合规性详细信息

PCI 合规性页面仅适用于企业级许可证用户。

访问 PCI 合规性

- 1 在主页左侧的导航面板中，选择**安全性 > PCI 合规性**。
- 2 此时将显示 **PCI 合规性**窗口。选择所需的范围、相应实体以及需要数据的持续时间。单击**评估**。
- 3 此时将显示 **PCI 合规性**页面。

PCI 合规性页面详细信息

PCI 合规性页面有助于仅在 NSX 环境中根据 PCI 要求评估合规性。在仪表板中的第一个插针下会显示这些要求。仪表板中提供用于评估这些要求的数据的其余看板项如下所示：

- **网络流图**：显示数据流、防火墙、连接以及与网络关联的其他详细信息。
- **流**：列出在网络流图中查看的流。

- 基于目标端口的明文协议流：在特定端口上流动的流量采用明文形式。此插针将基于特定的目标端口显示明文协议流。
- 范围内的虚拟机：显示在查询中所选择范围内的虚拟机。此插针显示该范围内虚拟机的出站规则、入站规则和安全组。
- 虚拟机的安全组：列出虚拟机的安全组。
- 虚拟机计数 (按安全组)：通过单击此插针中的“计数”，可以查看安全组中的虚拟机列表。
- 虚拟机计数 (按安全标记)：通过单击此插针中的“计数”，可以查看具有安全标记的虚拟机列表。
- 应用于内部流量的防火墙规则：可以查看所选范围内的虚拟机之间流量的防火墙规则。
- 应用于入站流量的防火墙规则：可以查看从范围外的虚拟机传输至所选范围内虚拟机的流量的防火墙规则。
- 应用于出站流量的防火墙规则：可以查看从所选范围内的虚拟机传输至范围外虚拟机的流量的防火墙规则。
- 安全标记成员资格更改：在此插针中显示与安全标记的成员资格相关的更改。
- 安全组成员资格更改：在此插针中显示与安全组成员资格相关的更改。
- 防火墙规则更改：在此插针中列出与任何防火墙规则相关的更改。

注 如果 NSX 具有嵌套安全组，则 PCI 合规性的范围应扩展到安全组之外。

导出为 PDF

在 vRealize Network Insight 中，可以在“PCI 合规性”仪表板上创建信息并导出为 PDF 报告。

步骤

- 1 在“PCI 合规性”仪表板中，单击页面右上角的**导出为 PDF**。此时将显示“导出为 PDF”窗口。
- 2 “导出为 PDF”窗口列出了“PCI 合规性”仪表板上可用的所有小组件及其相应属性。选择要导出的小组件和属性。

注

- 必须至少选择一个属性。
 - 可以选择的最大属性数为 20。
 - 可以导出的列表视图中的最大条目数为 100。
 - 某些小组件不允许选择属性。在这种情况下，请仅指定条目数。
-

3 提供 PDF 报告的标题。

注

- 标题允许的最大字符数为 200。
- 可以在报告中生成的最大页数为 50。

4 单击预览。可看到完整报告的预览。

5 单击导出 PDF。

Object Missing

This object is not available in the repository.

查看负载均衡器详细信息

负载均衡器页面汇总了在负载均衡器上创建的虚拟服务器和池的所有信息。

您可以查看

- 负载均衡器上的虚拟服务器列表及其问题
- 负载均衡器上的池列表及其关联问题
- 与负载均衡器关联的事件
- 不同目标 IP 上的流列表、计数及其网络流量。

注 不会针对 NSX-V 负载均衡器捕获流信息。

- 负载均衡器的属性，提供供应商、类型、序列号、虚拟服务器、池等信息。

查看虚拟机详细信息

您可以使用“虚拟机”页面获取 vRealize Network Insight 中可用虚拟机的详细概览。

在“虚拟机”页面中，您会看到以下部分：

区域	详细信息
概览	<p>您可以查看</p> <ul style="list-style-type: none"> ■ 虚拟机详细信息。 ■ 拓扑信息。 ■ 各种配置参数 ■ 安全性相关参数。 ■ 虚拟机到 Internet 路径。
邻居	<p>您可以查看</p> <ul style="list-style-type: none"> ■ 与邻居虚拟机比较的各种衡量指标属性的图形视图 ■ 属于同一主机的虚拟机列表。

区域	详细信息
事件	您可以查看与所选虚拟机相关的事件列表。
流	您可以查看源自或尝试访问允许和拒绝防火墙操作的选定虚拟机的流列表。
衡量指标	<p>您可以查看</p> <ul style="list-style-type: none"> ■ 与所选虚拟机相关的衡量指标信息。 ■ 有关 ToR 路径中端口的网络使用情况的信息。 ■ 有关所有衡量指标属性的信息。 ■ 输入 - 输出衡量指标信息。 ■ 虚拟磁盘空间。 ■ 数据存储性能 <p>注 如果虚拟机托管在 vSAN 数据存储上，则无法查看该虚拟机的数据存储衡量指标。</p> <ul style="list-style-type: none"> ■ 虚拟基础架构延迟详细信息。 <p>注 要查看虚拟基础架构延迟，必须打开收集器上的端口 1991，才能从 ESXi 主机接收延迟时间数据。</p>

查看 NSX Manager 详细信息

可以使用 **NSX Manager** 页面详细浏览 vRealize Network Insight 中可用的 NSX Manager。

如何访问 NSX Manager 页面

要访问此页面，请搜索 NSX Manager where SDDC Type = 'VMC'，然后在搜索结果列表中，单击要查看的 **NSX Manager** 页面。

概览

在 **NSX Manager** 页面中，您会看到以下部分：

表 8-1.

区域	详细信息
概览	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ NSX 策略实体概览详细信息。 ■ 过去 24 小时内修改的实体。 ■ 前几个流 (按规则)。 ■ 路由器列表。 <p>注 NSX 策略实体概览小组件中显示的实体数和过去 24 小时内的实体数小组件中显示的实体数可能有所不同。如果删除过去 24 小时内发现的某些实体，则过去 24 小时内的实体数小组件中显示的实体数可能大于 NSX 策略实体概览小组件中显示的实体数。</p>
通信最多者	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 环境中通信最多的实体。
网络流量和事件	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 网络流量和警示概览详细信息。 ■ 事件列表。

查看虚拟服务器详细信息

“虚拟服务器”页面包括虚拟服务器衡量指标以及问题和更改事件。

您可以查看

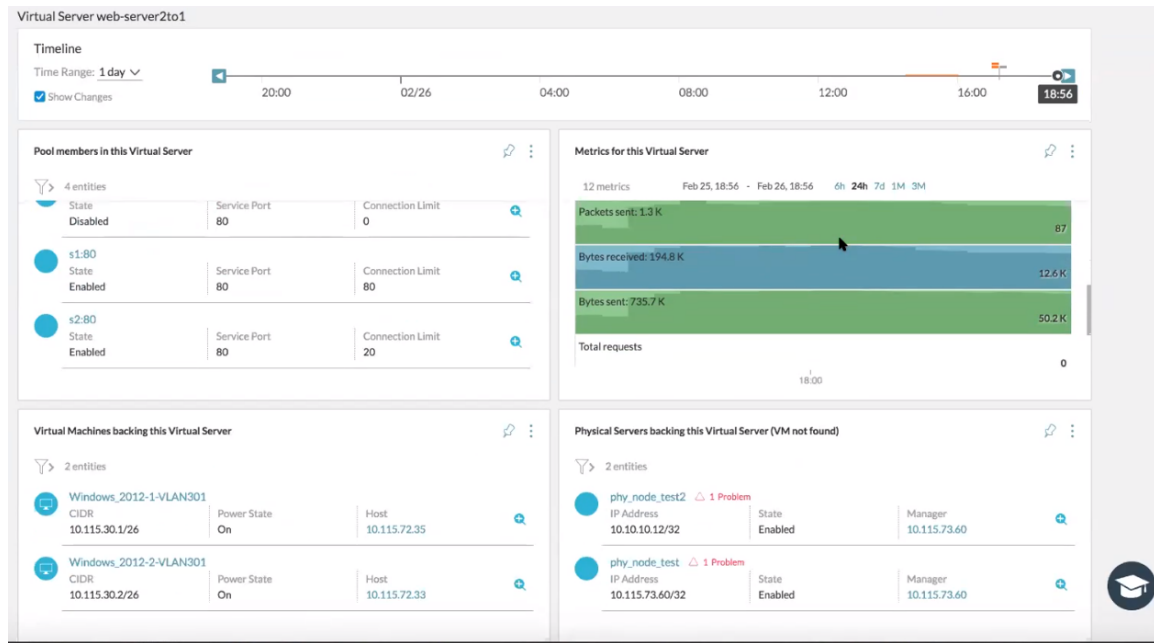
- 虚拟服务器中所有池成员的列表及其详细信息以及任何问题的警示。
- 虚拟机列表
- 物理服务器列表
- 与虚拟服务器关联的问题事件列表
- 与虚拟服务器相关的衡量指标列表，如
 - 连接数（计数、持续时间）
 - 网络衡量指标（接收或发送的数据包数和字节数）
 - CPU 使用情况

注 有关受支持的 NSX-V 负载平衡器衡量指标的列表，请参见受支持的 NSX-V 衡量指标。

- 此虚拟服务器所用池成员的前几个流。

注 不会针对 NSX-V 负载平衡器捕获流信息。

- 提供负载平衡器 IP 地址、网络流量、服务端口相关信息的虚拟服务器属性。



要查看与负载均衡器关联的拓扑路径，可以使用以下查询：client VM name to Virtual server IP。如果不同服务端口上有多个虚拟服务器，您会在“选择目标虚拟机”下看到该列表。您可以从列表中选择一个服务器，然后单击**显示路径**以查看虚拟机到虚拟服务器路径。

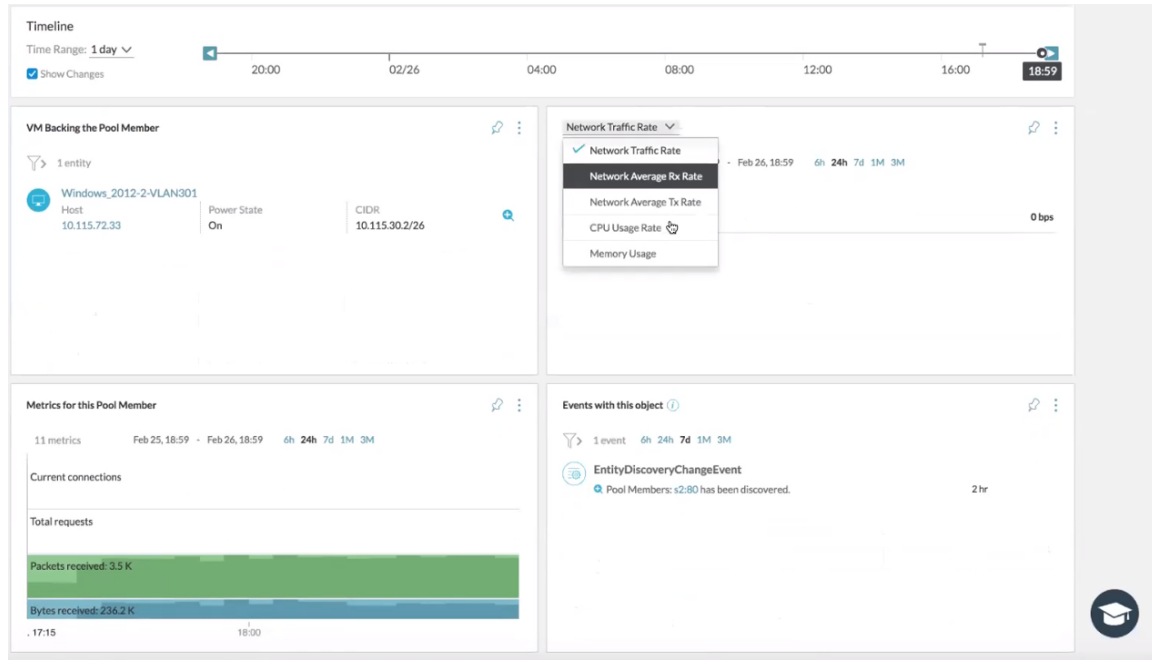
您可以单击虚拟机路径拓扑上的虚拟服务器，以查看虚拟服务器窗口中的一组虚拟机。单击**查看路径**可查看虚拟服务器到选定虚拟机的路径。

查看池成员详细信息

“池成员”页面提供了有关池成员、衡量指标以及与池成员关联的事件的见解。

您可以查看：

- 虚拟机列表以及有关虚拟机的其他详细信息。
- 允许您将池成员的衡量指标与虚拟机的衡量指标进行比较。例如，内存和 CPU 使用情况，网络流量。
- 与池成员相关的衡量指标列表，如
 - 连接（计数、持续时间、使用期限）
 - 网络衡量指标（接收或发送的数据包数和字节数）
 - CPU 使用情况
- 池成员属性，提供有关负载均衡器、节点、状态和服务端口的信息。



查看 Microsoft Azure 详细信息

可以在 vRealize Network Insight 中使用 **Microsoft Azure** 页面快速浏览 Azure 环境详细信息。

如何访问

要访问此页面，请搜索 **Azure**。或者，在主页的**操作与故障排除**部分中，单击 **Microsoft Azure** 图标。

概览

在此页面中，您将看到：

- 订阅列表
- 虚拟机列表
- 网络接口、虚拟网络、子网、路由表和路由列表
- 网络安全组、应用程序安全组和 NSG 规则列表。

您还可以单击此页面上的实体，查看有关特定实体的更详细见解。

除了 **Microsoft Azure** 页面以外，您还可以查看有关以下 Azure 实体的见解：

表 8-2. Azure 实体详细信息

实体名称	描述
Azure 应用程序安全组	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 属性、事件、关联虚拟机和过去 24 小时内的关联虚拟机的列表。 ■ 入站 NSG 规则和出站 NSG 规则的列表。 ■ 允许的流、拒绝的流、过去 24 小时内的流列表。
Azure 数据源	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 属性、事件和衡量指标的列表。
Azure NSG 规则	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 属性、事件和衡量指标的列表。
Azure 网络接口	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 属性、事件和衡量指标的列表。
Azure 网络安全组	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 属性、事件、网卡和子网的列表。 ■ 出站规则和入站规则的列表。 ■ 允许的流、拒绝的流、过去 24 小时内的流列表。
Azure 路由	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 属性、事件和衡量指标的列表。
Azure 路由表	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 属性、事件和衡量指标的列表。
Azure 子网	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 属性、事件、虚拟机、网卡和自定义路由的列表。 ■ NSG 规则列表。
Azure 订阅	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 属性和事件列表。 ■ 虚拟机列表。 ■ 网卡、虚拟网络和路由表列表 ■ 网络安全组、应用程序安全组和 NSG 规则列表。
Azure 虚拟机	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 属性、事件、网卡、关联的应用程序安全组 (ASG) 的列表。 ■ 入站 NSG 规则和出站 NSG 规则的列表。 ■ 允许的流和拒绝的流列表。
Azure 虚拟网络	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 属性、事件、虚拟机、过去 24 小时内创建的虚拟机、关联的 ASG、过去 24 小时内关联的 ASG、子网和路由表的列表。 ■ 允许的流、拒绝的流和过去 24 小时内的流列表。

查看 VeloCloud 企业详细信息

可以在 vRealize Network Insight 中查看 **VeloCloud 企业** 页面，快速了解 VMware SD-WAN 部署。

访问 VeloCloud 企业页面

要访问此页面，请搜索 **VeloCloud 企业**。或者，在主页的**操作与故障排除**部分中，单击 **VeloCloud 企业** 图标。

概览

在此页面中，您会看到以下部分：

区域	详细信息
概览	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ VMware SD-WAN 部署摘要，其中包括事件图表、Edge 数量、Hub、网关、链路、Edge 到 Edge 流、Internet 流和应用程序。您还可以查看这些实体的运行状况条件。 ■ VMware SD-WAN 部署的地图视图和 Edge 上的应用程序列表。 <p>注 要获取地图视图，必须在 vRealize Network Insight 中添加 Google Maps API 密钥。有关详细信息，请参见添加 Google Maps API 密钥。如果不添加 Google Maps API 密钥，则只能查看 Edge 的列表视图。</p>
事件	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 各种事件的列表。
分析	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 各种流量分布列表，如按应用程序、Edge、Edge 对、流路径、流量类型、链路策略和路由类型的流量分布。
可用性	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 可用 Edge/Hub 以及不可用 Edge/Hub 列表。
衡量指标	<p>您可以查看：</p> <ul style="list-style-type: none"> ■ 基于 Edge 流量、Edge 数据包、Edge QoE、应用程序流量、应用程序数据包、链接数据包、链路延迟、链路吞吐量 and 链路 QoE 的各种衡量指标。您可以单击加号 (+) 图标以获取更多详细信息。

您还可以单击此页面上的实体，查看有关特定实体的更详细见解。

除了 **VeloCloud 企业** 页面以外，您还可以查看有关以下 VMware SD-WAN 实体的见解：

表 8-3. VMware SD-WAN 实体详细信息

实体名称	描述
VeloCloud 群集	您可以查看： <ul style="list-style-type: none"> ■ 属性列表。
VeloCloud 数据源	您可以查看： <ul style="list-style-type: none"> ■ 属性、未决问题及过去 7 天内发生的更改和问题列表。
VeloCloud Edge	您可以查看： <ul style="list-style-type: none"> ■ 有关 VMware SD-WAN Edge 的详细信息。有关更多详细信息，请参见查看 VeloCloud Edge 详细信息。
VeloCloud 网关	您可以查看： <ul style="list-style-type: none"> ■ 属性和 Edge 列表。
VeloCloud 第 2 层网络	您可以查看： <ul style="list-style-type: none"> ■ 属性和事件列表。
VeloCloud 链路	您可以查看： <ul style="list-style-type: none"> ■ 属性和事件列表。 ■ 有关 QoE、数据包、正常运行时间、延迟和吞吐量的衡量指标。
VeloCloud 配置文件	您可以查看： <ul style="list-style-type: none"> ■ 属性和 Edge 列表。
VeloCloud 分段	您可以查看： <ul style="list-style-type: none"> ■ 属性列表。

查看 VeloCloud Edge 详细信息

可以在 vRealize Network Insight 中使用 **VeloCloud Edge** 页面快速了解 VMware SD-WAN Edge。

如何访问

要访问此页面，请搜索 **VeloCloud Edge**，然后单击任意搜索结果。

概览

在此页面中，您会看到以下部分：

区域	详细信息
概览	您可以查看： <ul style="list-style-type: none"> ■ VMware SD-WAN Edge 的摘要，如事件图表、正常运行时间详细信息、应用程序数、分段、链路、第 2 层网络、LAN 接口和 WAN 接口。 ■ VMware SD-WAN Edge 拓扑。 ■ Edge QoE 和链路 QoE 列表
事件	您可以查看： <ul style="list-style-type: none"> ■ 各种事件的列表。

区域	详细信息
流	您可以查看： <ul style="list-style-type: none"> ■ 流列表。
分析	您可以查看： <ul style="list-style-type: none"> ■ 各种流量分布列表，如按应用程序和优先级、流路径、流量类型、链路策略和路由类型的流量分布。
衡量指标	您可以查看： <ul style="list-style-type: none"> ■ 基于 Edge 流量、Edge 数据包、应用程序流量、应用程序数据包、链接数据包、链路延迟和链路吞吐量的各种衡量指标。您可以单击加号 (+) 图标以获取更多详细信息。

您还可以单击此页面上的实体，查看有关特定实体的更详细见解。

查看 SD-WAN 和 Edge SD-WAN 应用程序详细信息

可以在 vRealize Network Insight 中使用 **SD-WAN 应用程序** 和 **Edge SD-WAN 应用程序** 页面快速了解 SD-WAN 应用程序和 Edge SD-WAN 应用程序。

概览

在此页面中，您会看到以下部分：

表 8-4. SD-WAN 应用程序

区域	详细信息
概览	您可以查看： <ul style="list-style-type: none"> ■ Edge、事件、流量、数据包和流列表。
分析	您可以查看： <ul style="list-style-type: none"> ■ 流量（按 Edge）和流量（按客户端）列表。

您还可以单击此页面上的实体，查看有关特定实体的更详细见解。

除了 **SD-WAN 应用程序** 页面以外，您还可以查看有关 **Edge SD-WAN 应用程序** 实体的以下见解：

- 属性、事件和衡量指标列表。

注 vRealize Network Insight 支持每个 VMware SD-WAN Edge 最多 2 个分段和最多 20000 个第 3 层域。

查看“流洞察”详细信息

通过**流洞察**页面，可深入了解数据中心、设备和流。它是基于上下文的页面，因为该页面基于您选择的实体、流和时间范围执行分析。

要访问“流洞察”页面，请执行以下操作：

- 1 在左侧导航窗格中，单击**分析 > 流洞察**。

2 选择**范围**和**持续时间**。

3 单击**分析**。

或者，您也可以搜索**流**，然后在搜索结果页面中单击**流洞察**。

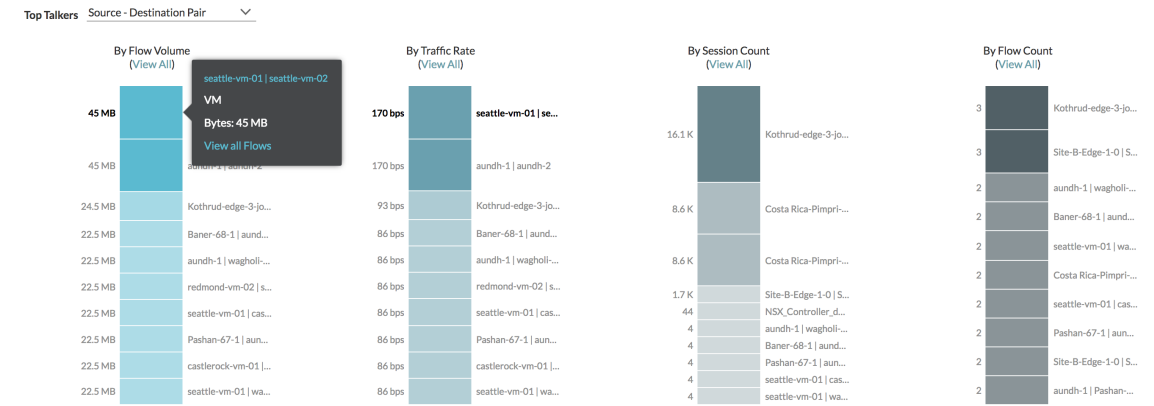
“流分析”仪表板中的各个部分如下：

- 通信最多者
- 新增内容
- 网络性能
- 离群者

通信最多者

此部分可帮助您识别哪些实体在您的环境中通信最多。可以选择不同类型的实体，如源-目标对、虚拟机、群集、L2 网络、子网。此小组件列出了所选择实体类别中的前 10 个通信最多者。它有助于客户规划网络优化。此小组件中用条表示的衡量指标如下所示：

- 按流量：指示流量。
- 按流速：指示流量的速率。
- 按会话计数：指示会话的数量。
- 按流计数：指示流的数量



注

- 如果某虚拟机在一个或多个衡量指标中出现，则在一个条中指向该虚拟机时，该虚拟机也会在其他条中突出显示。
- 单击衡量指标条中的虚拟机时，将显示传入此虚拟机的流的完整列表。
- 在“通信最多者”列表中选择虚拟机作为实体时，将显示与此虚拟机相关的所有流，而不管它是源还是目标。如果在列表中选择“源虚拟机”，则仅考虑传出此虚拟机的流。
- 如果正在考虑物理流，则可以选择“源 IP”或“目标 IP”。
- 选择源-目标对并指向衡量指标条后，如果单击工具提示中的链接，则会显示相应的仪表板。例如，对于源-目标对中的虚拟机，将显示虚拟机-虚拟机路径仪表板。
- 对于流组视图、流实体投影或流组查询，看不到**流分析**按钮。

新增内容

此部分有助于跟踪数据中心中选定时间范围内发现的服务和实体。此部分中的小组件如下所示：

- 访问 Internet 的新虚拟机：列出访问 Internet 的新虚拟机。
- 已访问的新 Internet 服务：列出在环境中发现的新 Internet 服务。
- 已访问的新内部服务：列出从 Internet 端点发现和访问的新 Intranet 服务。
- 已访问的新内部/E-W 服务：列出由数据中心内的计算机公开和访问的服务
- 具有已阻止流的新服务：列出具有已阻止流的服务。此部分仅针对 IPFIX 进行填充。
- 生效的新防火墙规则：列出已生效的新防火墙规则。此部分仅针对 IPFIX 进行填充。

网络性能

在此部分中，您可以根据所选条件查找并可视化各种范围的 TCP 往返时间 (RTT) 值的异常流。

注 vRealize Network Insight 仅显示过去 24 小时内以 5 分钟粒度为间隔的平均 TCP RTT 衡量指标。

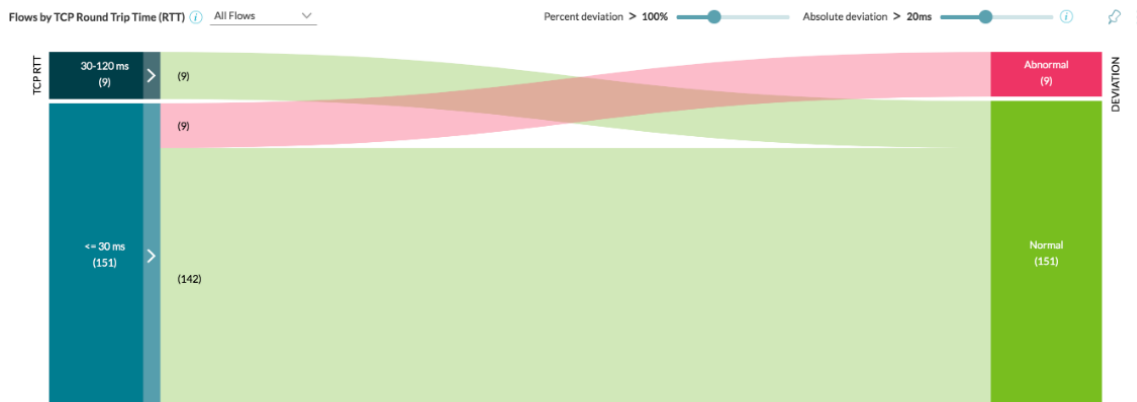
如果流偏差百分比为 100%，绝对偏差为 20 毫秒 (ms)，则 vRealize Network Insight 会将该流视为异常流。

在可视化中，左侧显示 TCP RTT 的不同范围，右侧显示正常和异常偏差范围。根据百分比偏差和绝对偏差的值，流从左侧 (TCP RTT) 连接到右侧 (DEVIATION)。您可以分析以下类型的流：

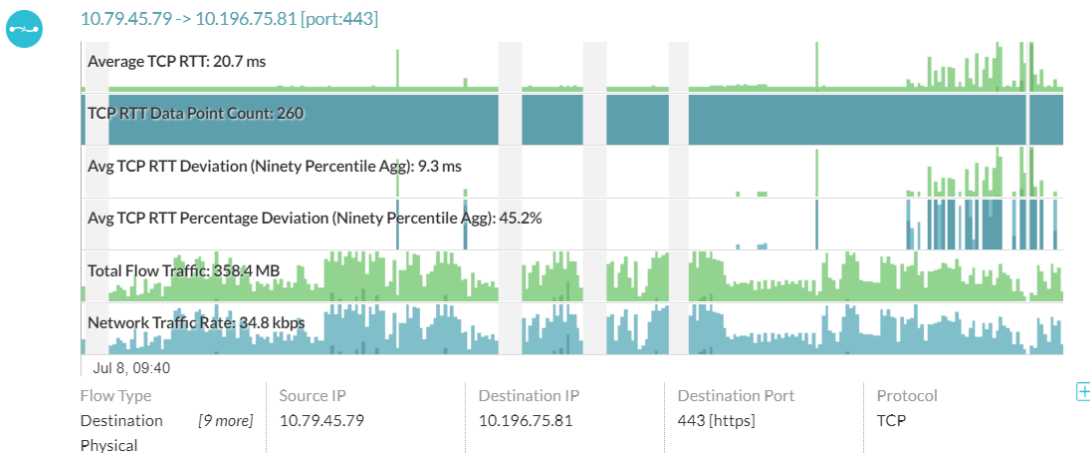
- 主机间
- 主机内部
- Internet
- 所有流

您还可以根据要求更改百分比偏差和绝对偏差。

在下面的示例中，有两个不同范围的 TCP RTT，一个小于等于 30 毫秒，另一个是 30-120 毫秒。您可以发现，总共有 151 个流在小于等于 30 毫秒 TCP RTT 范围内。在 151 个流中，9 个流显示为异常流。



要深入了解 TCP RTT 分布信息和流计数，请单击可视化中的彩色线条。在下面的示例中，您可以看到有关 TCP RTT 分布信息和流计数的详细信息：

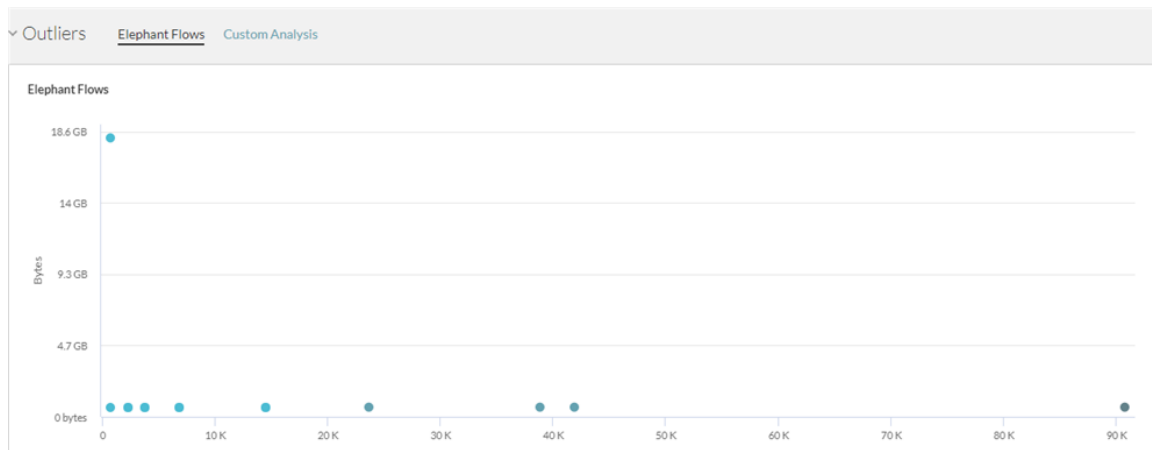


离群者

此部分有助于跟踪和分析相关数据。它包含以下部分：

- **大型流：**此部分有助于识别哪些流的会话计数少而吞吐量高，哪些流的会话计数多而吞吐量小。通常，会话计数多而吞吐量小的流也称为小型流。分析基于字节数与会话数之比。图形中的每个点都表示多个流。指向一个点时，可以看到流列表。要查看特定流的详细信息，请在列表中单击该流。
- **自定义分析：**在此部分中，可以在所选的两个维度上查看流数据。这有助于分析数据以通过各种方式查找离群者。

注 此部分中表示的衡量指标是近似值，而不是准确值。



查看微分段详细信息

可以基于 VLAN/VXLAN、安全组、应用程序、层、文件夹、子网、集群、虚拟机 (VM)、端口、安全标记、安全组和 IPSet 等实体选择相应的范围并对其进行分段，从而对流进行分析。

微分段页面提供了拓扑图的分析详细信息。此页面包含以下部分：

- **微分段：**此小组件提供拓扑规划图。可以选择组和流的类型。根据输入内容，可以查看对应的拓扑规划图。
- **流量分布：**此小组件提供流量分布的详细信息（以字节为单位）。
- **排名靠前的端口 (按字节)：**此小组件列出记录最高流量的前 100 个端口。提供了流计数和流体积的衡量指标。通过单击对应于特定端口的流计数，可以查看该端口的流。

要访问微分段页面，请执行以下操作：

步骤

- 1 在主页左侧的导航面板上，单击 **安全性 > 规划安全性**。

- 2 选择要规划和分析的范围、子范围和持续时间。单击**分析**。

此时将显示微分段页面。

注 环形视图可显示最多 600 个节点和 6000 个 Edge。如果超出限制，您将看到要分析的微分段过多。请选择其他实体或微分段标准 (Too many micro-segments to analyse. Please select a different entity or micro-segmentation criteria) 错误。

查看应用程序详细信息

应用程序是层的集合。应用程序中的每个层都是基于用户定义的筛选标准的虚拟机和物理 IP 集合。通过这些应用程序，可以创建一组层，并可视化同一应用程序的层之间以及应用程序之间的流量或流。

您可以通过三种方式创建应用程序或将应用程序添加到 vRealize Network Insight 中：

- 手动创建应用程序
- 公共 API
- 应用程序发现

通过“应用程序”页面可完整查看 vRealize Network Insight 中的单个应用程序。这样，您可以对问题进行故障排除，还可以查看分析。

- 概览
 - 应用程序拓扑
 - 层概览
 - 应用程序中的虚拟机列表
 - 应用程序依赖或使用的物理 IP
 - 共享服务数
 - 此特定应用程序与之通信的应用程序
 - 与应用程序相关的事件
 - 应用程序虚拟机管理器
- 过去 24 小时内的新增内容
 - 入站和出站流量计数
 - 丢弃的流
 - 新成员和不受保护的成员
 - 外部访问的服务
 - 通过 Internet 访问的服务
 - 已用应用程序端口

- 流量流或流分析
 - 通信最多者
 - 前几个应用程序流（按规则）
- 微分段
 - 实体之间的上下文流，可提供不同流类型的数据，例如根据 NSX DFW 的所有允许的流、丢弃的流、受保护的流和不受保护的流。
 - 应用程序的新增功能
- 衡量指标
 - 表示网络速率、CPU、内存和磁盘信息的虚拟机衡量指标信息。
 - Kubernetes 衡量指标

分析 - 异常值检测

vRealize Network Insight 基于与通过虚拟机和物理 IP 地址定义的流关联的衡量指标提供异常值检测。这些虚拟机/IP 应具有类似的流量模式，以便将特定虚拟机/IP 分类为离群者是有价值的。例如，属于应用程序同一层的虚拟机通常对应用程序执行相同的功能，例如，SQL 数据库的虚拟机为 Web 应用程序的请求提供服务。对于这些类型的虚拟机，接收到的请求数、发出的流量、会话计数等将经历一系列相似变化。

在 vRealize Network Insight 中，通过异常值检测，可以检测到流量模式截然不同于组中其他虚拟机/IP 的特定虚拟机。例如，如果虚拟机在发送或接收比组中其余虚拟机高得多/低得多的流量。可能原因是错误地配置了负载均衡器、存在 DDOS 攻击等。vRealize Network Insight 将此类虚拟机/IP 分类为异常值。通过查看这些离群者，用户可以轻松了解此意外行为并采取相应操作。

如何检测离群虚拟机

步骤

- 1 在边栏上，单击**分析**。单击**离群者**。
- 2 单击**添加**以添加配置。

3 在分析/配置页面中，为配置提供以下详细信息：

表 8-5.

字段	描述
名称	配置的名称
范围	<p>定义需要对其执行分析的虚拟机和 IP 的组的名称。可以选择“应用程序层”或“安全组”作为范围。</p> <p>如果选择“应用程序层”，请分别提供应用程序和层的名称。为层定义的虚拟机和物理 IP 的数量显示在层名称的旁边。</p> <p>如果选择安全组，则提供安全组的名称。</p> <p>注 目前，一层中的虚拟机和物理 IP 的数量限制为 200。选择虚拟机和物理 IP 的数量小于此限制的层或安全组。范围还应至少包含 3 个虚拟机/物理 IP。</p> <p>通过单击查看微分段，可以查看所选配置的微分段。</p>
检测类型	当前，vRealize Network Insight 支持在系统中检测异常值。
衡量指标	<p>检测基于此流衡量指标。可以选择以下选项：</p> <ul style="list-style-type: none"> ■ 字节数 ■ 数据包数 ■ 会话数 ■ 流速
流量方向	可以选择 出站 、 入站 或 二者 作为流量方向。如果选择 二者 ，则可以在配置预览中指定“入站”或“出站”。
流量类型	可以根据要求选择 Internet 、 东西向 或“全部”。
目标端口	<p>可以选择在所选范围内发现的流上检测到的所有端口，也可以手动输入您选择的目标端口。如果选择所有端口，则显示目标端口数。如果选择手动输入端口，然后在自动完成文本框中输入端口，则分析将仅限于这些端口</p> <p>注 目前，端口数限制为 20。</p>
敏感度	可以衡量所需的检测和报告的敏感度。默认值为 中等 。
预览	<p>此部分基于您提供的输入和参数提供特定配置的预览。如果之前选择“二者”作为“流量方向”，则指定端口和流量方向。</p> <p>您将能够在图形中识别离群虚拟机。</p>

注

- 通过评估过去 24 小时内可用的数据，检测离群者。
- 您需要连续的 IPFIX 数据流才能检测离群者。

4 单击**提交**以创建分析配置。

5 应用程序创建后，便会显示在“分析配置”页面的应用程序列表视图中。单击该特定应用程序以查看与其关联的仪表板。

分析：静态和动态阈值

通过 vRealize Network Insight，可以基于实体行为中的偏差来设置和配置阈值以及接收警示。可以配置以下两种类型的阈值：

- **静态阈值：**如果特定的衡量指标值高于或低于配置的值，则会生成基于静态阈值的警示。
- **动态阈值：**如果阈值由系统基于历史数据分析确定，则违反此阈值的情况下会生成警示。在生成任何警示前，对数据进行为期 7 天的分析。创建基准的过程仅限于 21 天的历史数据，为新衡量指标值创建基准时不考虑较旧的衡量指标值。

违反阈值后，立即生成警示。企业级许可证用户可以在主页的**当前状态**部分中查看阈值冲突数。要查看事件详细信息，请单击“阈值冲突数”。如果系统中不存在阈值配置，则**当前状态**部分会显示 **+配置** 链接。您可以单击 **+配置** 链接以配置阈值。

配置阈值和警示

您可以添加阈值配置，并获取已配置阈值的警示。

要配置与分析关联的阈值和警示，请执行以下操作：

步骤

- 1 在主页的左侧导航面板中，单击**分析 > 阈值 > 添加**。
- 2 在**阈值 - 添加配置**页面的**名称**文本框中，输入配置的唯一名称。
- 3 从**范围**下拉菜单中，选择一个范围，然后在**选择条件**文本框中，输入一个条件。
范围下拉菜单包含**虚拟机**、**流**和**应用程序**实体。范围基于搜索查询系统。您可以根据您的要求，利用可用的建议创建查询。
- 4 在**条件**部分中，设置一个条件以创建警示。
根据您的设置的条件，系统会决定是否违反了阈值。

- 5 默认衡量指标为 `network traffic rate`。选择实体的分组和要检查其阈值的值。可以通过聚合一组实体中的数据来设置累积衡量指标的阈值。

a 要配置静态阈值，请从列表中选择以下任一阈值条件：

- 超过阈值
- 下降到低于
- 超出范围

为 `network traffic rate` 或 `total traffic` 或者任何其他衡量指标输入 Upper Bound 或 Lower Bound（如果存在范围）时，请确保为该特定文本框输入指定衡量指标中的值。以下转换值供您参考：

- 1 Kbps= 1000 bps
- 1 Mbps= 1000 kbps
- 1 Gbps = 1000 mbps
- 1 KB=1024 B
- 1 MB=1024 KB
- 1 GB = 1024 MB

b 要配置动态阈值，选择**偏离过去的行为**。基于您的报告要求选择敏感度。

Condition ⓘ

For metric `network traffic rate` aggregated over `virtual machine` when `any value` **deviates from past behavior**

Sensitivity `Medium (2.5 standard deviation)`

exceeds threshold

drops below

is outside range

✓ deviates from past behavior

设置阈值时，可以查看页面顶部的关联图形。粉红色条表示违反阈值的虚拟机或流。可以查看系统中违反阈值的实体和阈值内的实体的列表。

- 6 通过设置以下属性来配置通知或警示：

- 严重性
- 电子邮件频率
- 将通知电子邮件发送到：

注 如果在系统上已配置 SNMP 陷阱，则选择**发送 SNMP 陷阱**。

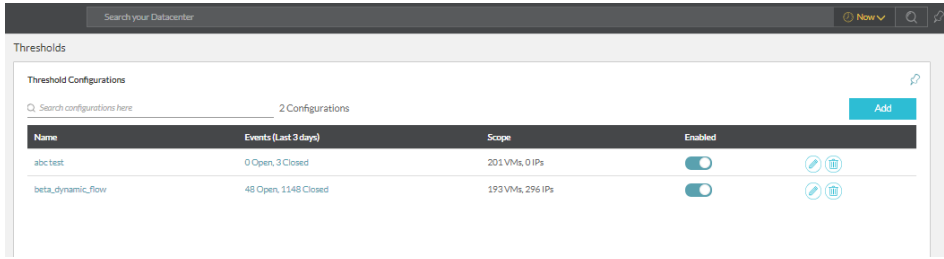
- 7 单击**提交**以创建阈值配置。

查看“阈值配置”页面

添加阈值配置后，就可以在**阈值配置**页面上查看其详细信息。

步骤

- 1 在左侧导航面板上，单击**分析**。单击**阈值**。

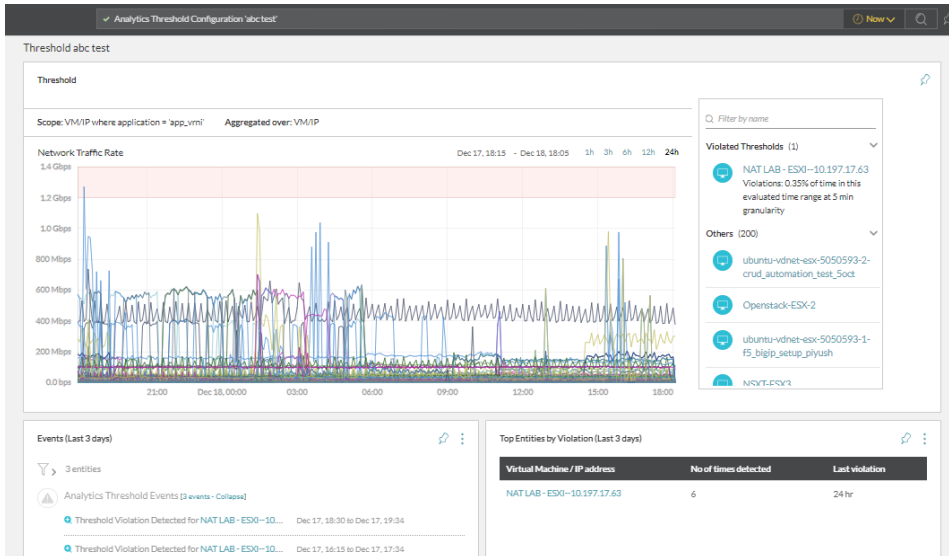


- 2 提供了有关阈值配置的以下详细信息：

- Name
- Events
- Scope

如果禁用该配置，则不会生成违反该特定阈值的警示。也可以在此页面上搜索任何特定的阈值配置。

- 3 单击列表中所需的阈值配置可查看该特定配置的仪表板。



可以在仪表板上查看以下小组件：

- 图形：阈值图可帮助您检测违反阈值的实体。
- 事件：此小组件提供过去三天内为已违反的阈值生成的事件列表。
- 排名靠前的实体 (按违反)：此小组件可让您了解在过去三天内导致偏差的排名靠前的实体。

查看实体拓扑

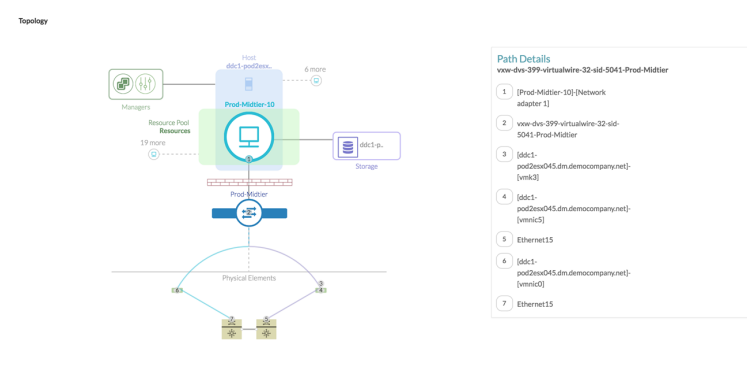
拓扑提供了实体的全面图形视图。

本章讨论了以下主题：

- 虚拟机拓扑
- 主机拓扑
- VXLAN 拓扑
- VLAN 拓扑
- NSX Manager 拓扑

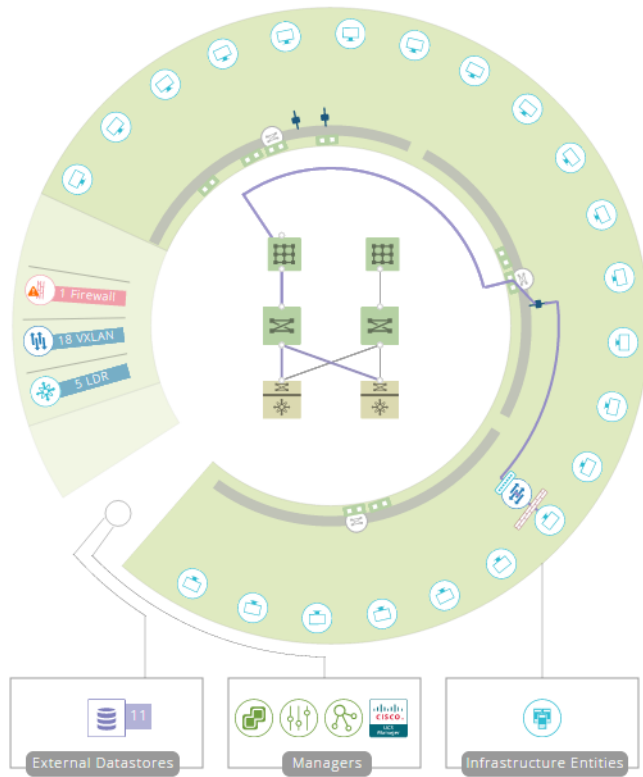
虚拟机拓扑

虚拟机拓扑提供与数据中心其余部分相关的单个虚拟机的综合视图。



主机拓扑

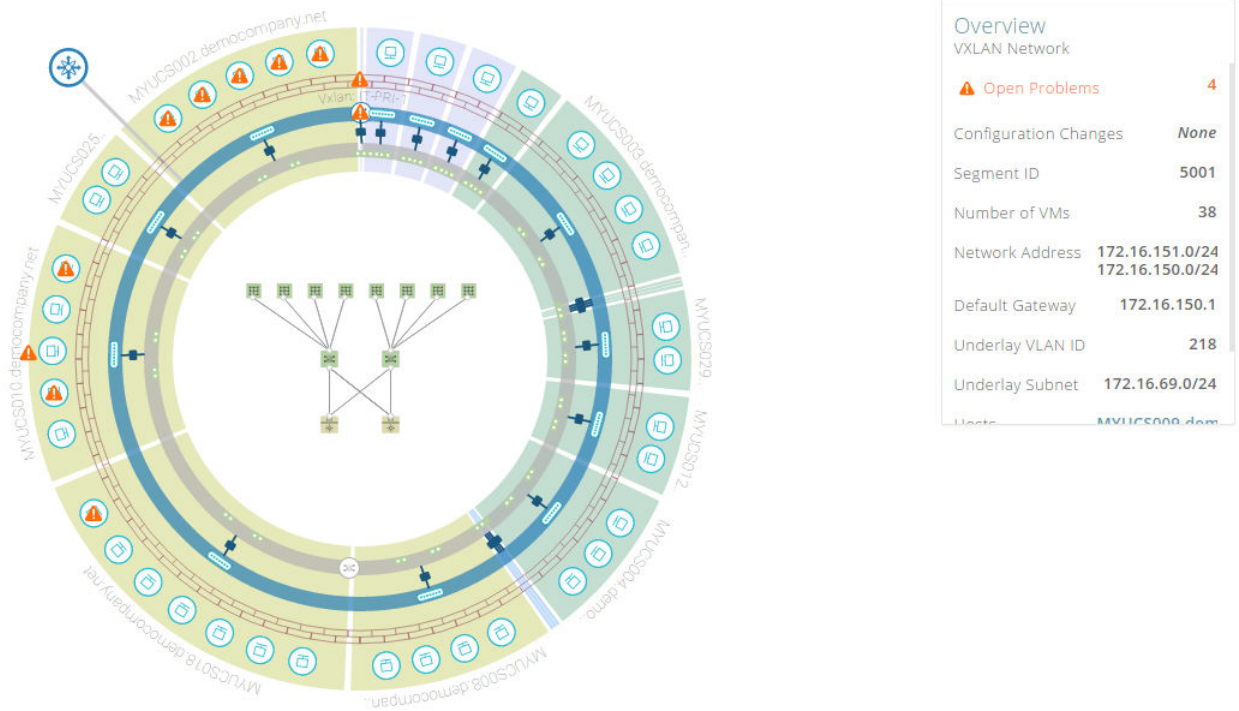
主机拓扑显示了特定主机的虚拟机如何连接到数据中心的虚拟和物理组件，以及主机本身如何与数据中心连接。



VXLAN 拓扑

虚拟可扩展局域网 (VXLAN) 覆盖网络连接技术是由 VMware 与主要网络连接供应商联合开发的行业标准。

VXLAN 拓扑是一种创新的可视化，它为您提供所选 VXLAN 的概览。下图说明组成可视化的各种组件：



注 虚拟组件和物理组件都可以通过此方式进行可视化。

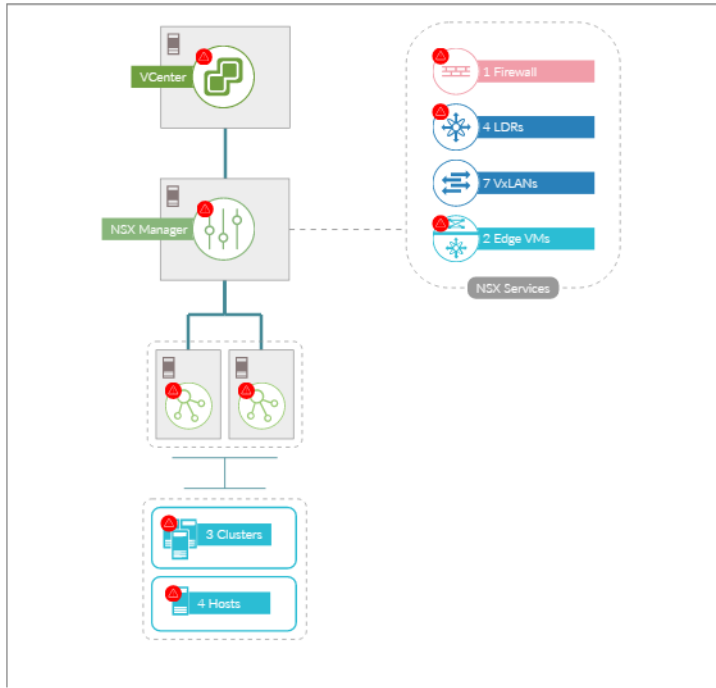
VLAN 拓扑

通过虚拟 LAN (VLAN)，单个物理 LAN 分段可进一步分段，以使端口组互相隔离，就好像它们位于不同物理分段上一样。

VLAN 拓扑的构建方式与 VXLAN 拓扑类似。

NSX Manager 拓扑

NSX Manager 拓扑显示与 NSX Manager 关联的组件。



Edge 数据收集

每次添加 NSX 数据源时，都可以启用自动 Edge 数据收集。在以前的版本中，Edge 数据收集通过 NSX Central CLI 或 Edge-SSH 会话完成。从当前版本开始，Edge 数据收集通过 NSX Central CLI 完成。因此，不会在 NSX Manager 下创建 Edge 数据提供程序。

注 NSX 用户特权验证

添加 NSX 数据源并启用 Edge 填充时，会验证 NSX 用户特权。

假定用户在 NSX 6.3 中具有企业管理员特权，并且正在运行当前版本的 vRealize Network Insight，则会在 **VMware NSX Manager** 的帐户和数据源页面上显示 Insufficient Privileges 错误。显示该错误的原因是，用户必须是超级用户才能在 NSX 6.3 中运行 NSX Central CLI 命令。

表 9-1.

NSX 版本	用户
NSX 6.4 和更高版本	<ul style="list-style-type: none"> ■ 要将 NSX Manager 添加为数据源，您必须是超级用户、企业管理员、审核员或 NSX 安全管理员。 ■ 企业管理员、超级用户、NSX 安全管理员或审核员可以运行 vRealize Network Insight 所需的 NSX Central CLI 命令。 <p>注 NSX 网络管理员无法将 NSX Manager 添加为数据源。</p>
NSX 6.4 之前的 NSX 6.2 和更高版本	<ul style="list-style-type: none"> ■ 用户应该是管理员才能启用 Edge 数据填充。 ■ 审核员、超级用户或 NSX 安全管理员可以运行 vRealize Network Insight 所需的 NSX Central CLI 命令。 ■ 将 NSX Manager 添加为数据源时需要提供的用户凭据必须属于企业管理员或超级用户。

在 vRealize Network Insight 中查看 NSX 对象的审核信息

vRealize Network Insight 可以从 NSX-T Manager 和 NSX-V Manager 快速捕获 NSX 对象的审核信息。该信息包括创建或修改 NSX 对象的用户名、操作发生时间以及该对象上的操作详细信息。

如果已在 NSX-T Manager 或 NSX-V Manager 中启用审核日志，则 vRealize Network Insight 可以收集某些 NSX-T 和 NSX-V 对象的审核详细信息。

NSX-V

vRealize Network Insight 在三到五分钟内收集审核详细信息的 NSX-V 对象的列表。

- SecurityGroup
- SecurityGroupTranslation
- FirewallConfiguration
- FirewallStatus
- IPSet
- SecurityTag
- UniversalSecurityGroup
- UniversalSecurityGroupTranslation
- UniversalIPSet

将针对发现、属性更改和删除事件捕获有关 NSX-V 对象的审核详细信息：

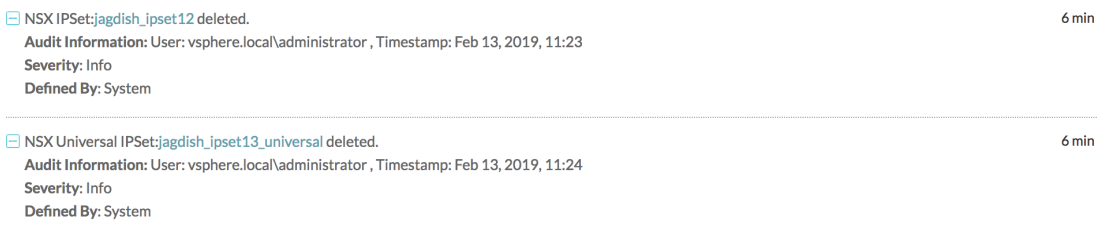
- Discovery



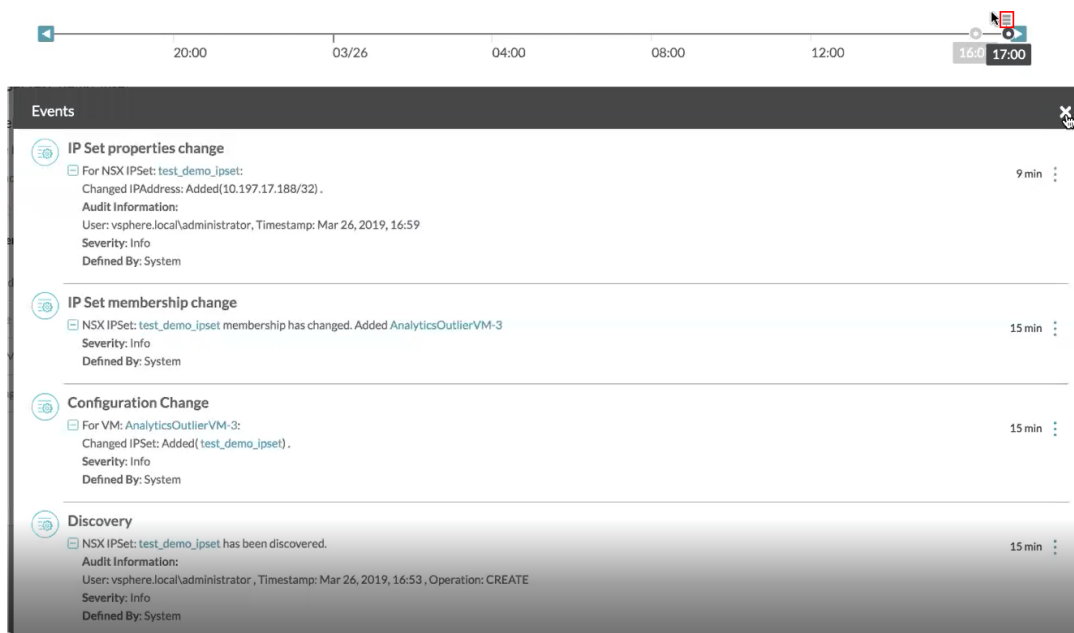
■ Properties Change



■ Delete



也可以在对象的时间轴上查看审核信息。



NSX-T

vRealize Network Insight 针对其收集审核详细信息的 NSX-T 对象的列表。

注 不显示 VMC 策略实体的审核信息。

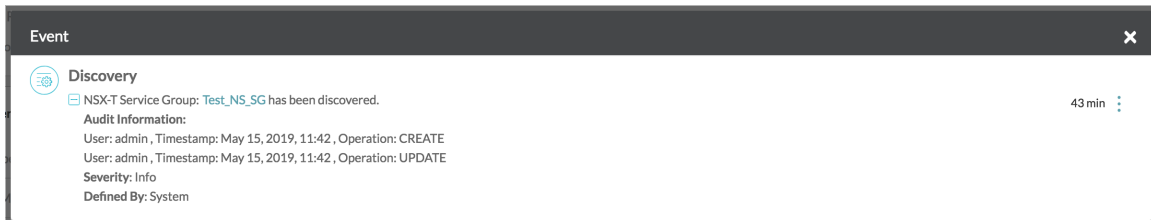
- NS 组
- NS 服务
- NS 服务组
- NS 防火墙规则

注 不显示 NSFirewallRule 的删除事件的审核信息。

- IPSet
- NSX 策略组
- NSX 策略防火墙规则

将针对发现、属性更改和删除事件捕获有关 NSX-T 对象的审核详细信息：

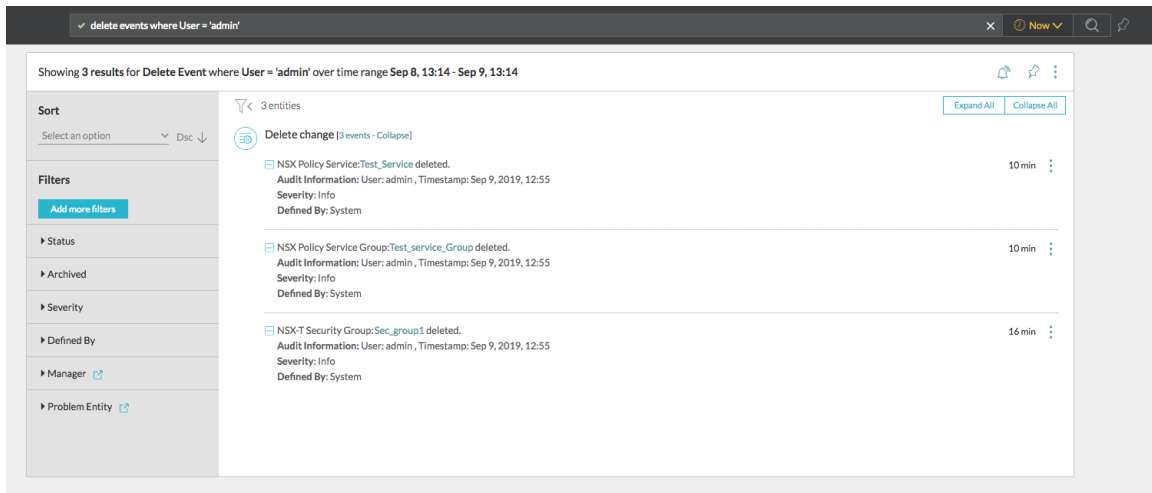
- Discovery



- Properties Change



- Delete



注 删除事件在实体仪表板上不显示。但是，可以搜索该事件以查看审核信息。

查看审核信息的查询示例

- `events where user = username`
- `discovery events where user = username`
- `delete events where user = username`
- `change events where user = username`

使用看板项

10

应用程序的所有部分均表示为看板项；看板项是可以保存和分组的基本单元，用于聚合您认为组合起来可以很有用的数据，以及将其与团队中的其他成员共享。可以插接搜索查询以及可用于实体的看板项。

要添加插针，请单击“插针”图标。所有已保存的看板项都显示在“看板”部分中，该部分可通过单击标题中的“看板”图标进行调用。

本章讨论了以下主题：

- 看板项
- 看板

看板项

每个实体页面上的信息会分为多个看板项。所有实体页面均由看板项组成，每个看板项都包含与实体相关的特定少量信息。

这些看板项具有以下功能：

- 可以使用“更多选项”()按钮最大化任何插针视图，还可以使用**帮助**选项查看有关插针的详细信息。
- 看板项还可以包含筛选器，以便可以深入了解看板项上显示的数据。
- 许多看板项还包含“导出为 CSV”选项，以便能以 CSV 格式导出看板项中存在的流数据。可以在显示的对话框中选择要导出的特定属性和 CSV 行数。

注 选择所有字段后，流数据的“导出到 CSV”功能需要 30 多分钟才能导出 180,000 个流。

插针类型

软件中可用的大多数插针可分为以下类别：

衡量指标插针

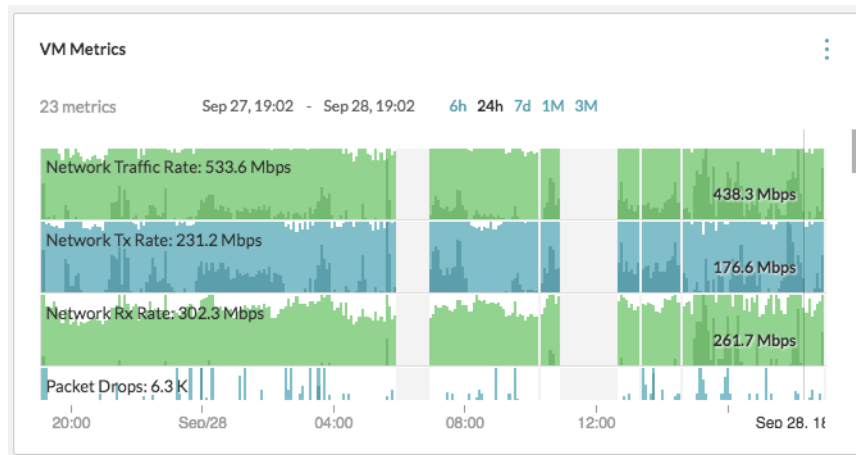
衡量指标插针显示与所选实体有关的重要衡量指标。

衡量指标插针使用立体图形来显示数据，方法是将每个图形划分为两个区段，并将较高的值相互换位。因此较高的值以较暗的颜色显示且更易于辨别。

可以从存在于插针标头的下拉菜单中选择要显示的特定衡量指标，并更改要显示的实体选择。

通过使用范围预设或在自定义日期/时间中输入，可以修改时间范围。

衡量指标插针的一个示例是虚拟机衡量指标插针。此插针显示虚拟机的网络流速、网络 Tx 率、网络 Rx 率和数据包丢弃数。



“实体列表视图” 插针

“实体列表视图” 插针显示按共同主题分组的实体列表。该列表显示每个实体的重要属性。

通过单击最右侧的放大图标，可以查看特定实体的更多属性。单击实体名称可转到实体页面。

与其他插针一样，筛选器图标包含可用于筛选列表的各种层面。条目列表视图插针的一个示例是“虚拟机邻居”插针。默认情况下，此插针显示同一主机上存在的虚拟机。也可以按安全组、VXLAN 和数据存储筛选虚拟机。

Metrics			
Key Metrics	Neighbor Benchmark	Neighbor Performance	VM Neighbors
Network Usage of Ports in Path to TOR	All Metrics	I/O Metrics	Virtual Disks
Datastore Performance			

VM Neighbors			Host: ddc1-pod2esx...
7 entities			
Prod-Midtier-14 CIDR 10.17.7.14/24	Def Gateway 10.17.7.254	Logical Switches Prod-Midtier	
Lab-Web-19-noip Logical Switches Lab-Web	CPUs 16	Memory (GB) 16	
Prod-Db-5 CIDR 10.17.8.10/24	Def Gateway 10.17.8.254	Logical Switches Prod-DB	

事件视图列表插针

“事件列表” 视图插针按时间顺序提供特定实体或实体组（可从插针标头的下拉列表中选择）的事件列表。

通过使用可用预设或在自定义日期/时间中输入，可以更改插针显示事件的时间（离现在）应有多远。通过单击筛选器图标，可以选择其他筛选器选项，如**事件状态**和**事件类型**。

在下图中，显示了与虚拟机 **Prod-db-vm21** 及其相关实体有关的事件。可以单击实体名称以查看其他相关实体中的事件。使用筛选器，可以基于事件的状态和类型对其进行筛选。事件可以是与实体相关的更改或问题。

Events VM: SITED-ESX-01

10 events Jan 24, 14:14 - Feb 23, 14:14 6h 24h 7d 1M 3M

- Configuration change [5 - Show all]**
For Host: 192.168.0.218: VMs has changed. Added 122, deleted 0. 4 days
- Discovery**
Virtual Machine: SITED-ESX-01 has been discovered. 4 days
- Delete change**
Virtual Machine: SITED-ESX-01 deleted. 8 days
- Configuration change [2 - Show all]**
For Virtual Machine: SITED-ESX-01: DVS has changed. Added VDS-Priv-Netw... 8 days

可以使用事件搜索查询来搜索事件。可以通过查询（如已打开的事件或已关闭的事件）来搜索已打开或已关闭的事件。还可以搜索具有相同修饰符的问题。

看板

可以从看板上的任何页面插接任何小组件，以便更轻松地了解访问和共享数据。

创建看板

PLAN

Micro Segments All Flows Application Applications VM All VMs

Open Problems 125 entities

- Test1**
Event Search: vmware vm returned 8530 results 3 days
- vms where Power State = 'POWEREDON'**
Event Search: vms where power state = 'poweredon' r... 3 days
- vms where Power State = 'POWEREDOFF'**
Event Search: vms where power state = 'poweredoff' r... 3 days
- Create Test Event - 0**

Pin Options

Search for pinboard

Recently Modified

- Default Pinboard
- testing
- New board 1

Create New Pinboard

246

- 1 单击要插接的小组件上的插针图标。

- 2 在弹出窗口中单击**创建新看板**。

注

- 如果尚未创建任何看板，则可以从**最近修改**列表中选择**默认看板**。

注 “默认看板”为初次使用的用户提供了典型看板的外观。这有助于用户熟悉看板的布局和功能。无法共享或删除默认看板。可以将看板项从默认看板复制到任何自定义看板。

- 可以在“最近修改”列表中看到的最大条目数为 15。
- 可以在所有用户之间创建的最大看板数为 500。

注 看板总数包括自定义看板、共享看板和默认看板。

- 每个看板的最大看板项数为 20。

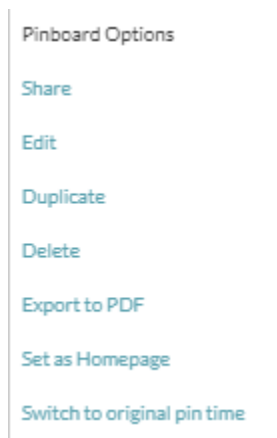
- 3 在**创建看板**窗口中，输入新看板的名称和描述。单击**创建并加为看板项**。

注

- 看板的名称在整个系统中必须是唯一的。
- 看板名称允许的最大字符数为 100。在看板的名称中只能使用字母、数字和空格。

- 4 此时将显示**已创建看板**消息。单击**立即共享**以立即共享看板。
- 5 要将小组件插接到现有的看板，请在**最近修改**下选择该看板，然后单击**插接**。此时将显示消息**您的插针已添加**，其中包含指向相应看板的链接。

访问看板选项



单击看板右上角的**更多选项**以访问**看板选项**。

注 仅当已创建看板或者已与具有**查看和编辑**权限的任何其他用户共享时，才能看到所有看板选项。任何其他用户只能看到**导出为 PDF**和**切换到原始插接时间**选项。

可以在看板上执行以下操作：

- 可以与任何其他现有 vRealize Network Insight 用户共享看板。


- 可以编辑看板和看板上插针的名称。
- 可以重新排列看板上的看板项。它们的立场保持不变。
- 单击**删除**可删除该特定看板。
- 单击**导出为 PDF** 可将看板上的信息导出为 PDF 报告。有关更多详细信息，请参见**导出为 PDF**。
- 要查看插针在插接时的数据，请单击**切换到原始插接时间**。通过此功能，可以查看每个插针在创建时的数据。

使用看板的时间轴滑块

vRealize Network Insight 在看板上支持时间轴滑块。要查看任何所需时间的看板数据，可以使用时间轴滑块。看板加载时，会加载当前时间（**现在**）的所有看板项。








查看看板库

如果您是管理员用户，则可以在看板库中看到**我的看板**选项卡和**所有看板**选项卡，如下图所示。如果您是成员用户，则可以在看板库中看到看板列表。

 Pinboards

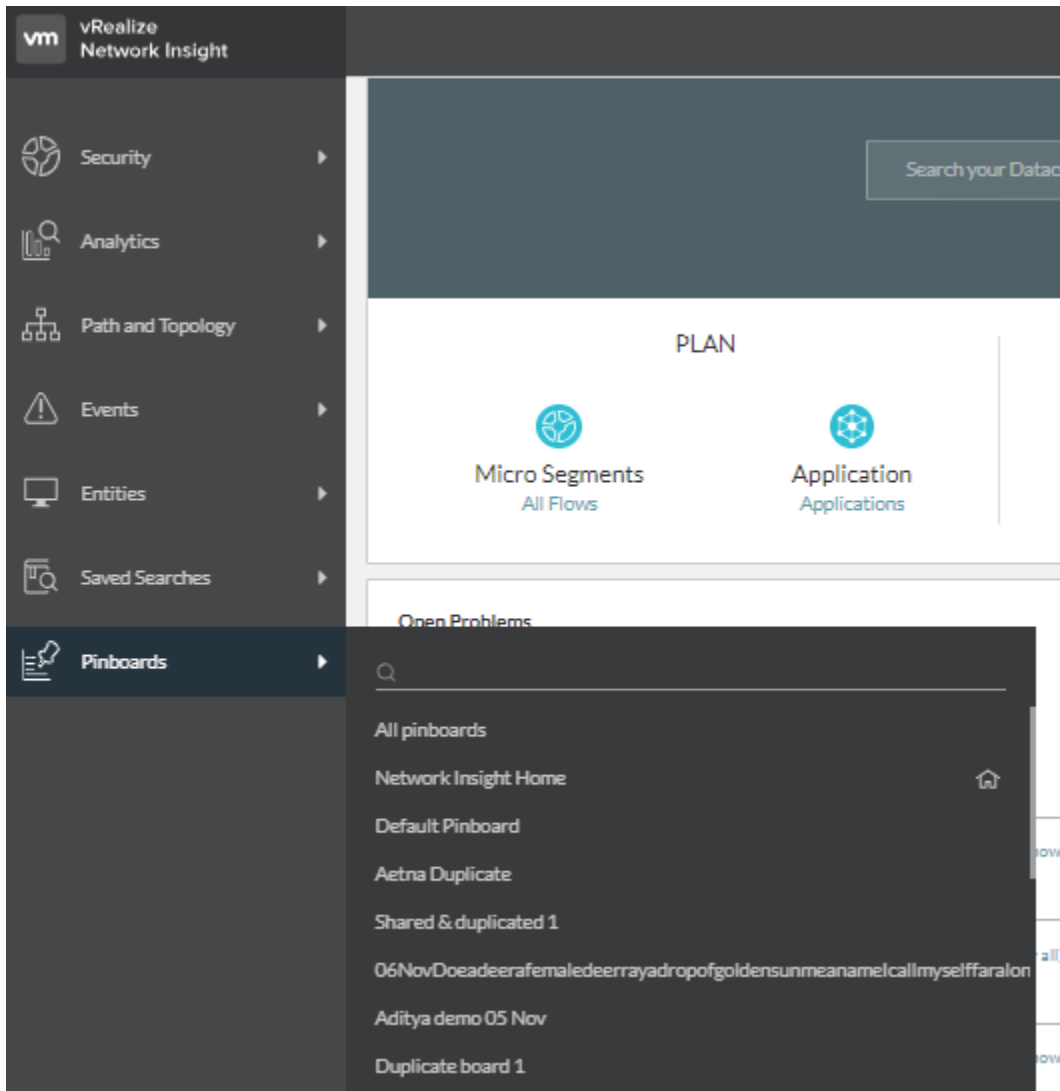
Search for pinboards

17 pinboards

Pinboard name	Last modified	Owner	Shared	Actions
Network Insight Home	--	--	--	
Default Pinboard	81 days	Guest 1	Not shared	
Aetna Duplicate	24 days	Guest 1	Not shared	  
Shared & duplicated 1	30 days	Guest 1	5 others	  

- 1 在主页的左侧导航栏上，单击**看板**。
- 2 单击**所有看板**以查看系统中的所有看板。
- 3 可以在导航栏中查看现有看板的列表。该列表具有与看板库中**我的看板**选项卡相同的项目。最后修改的看板显示在列表的顶部。单击要查看的看板。

注 创建看板后，需要一些时间它才会显示在此列表中。



4 也可以在库中搜索看板。

复制插针

- 1 单击小组件上的插针图标。
- 2 选择要向其复制插针的看板。
- 3 单击添加。

插接板的共享和协作

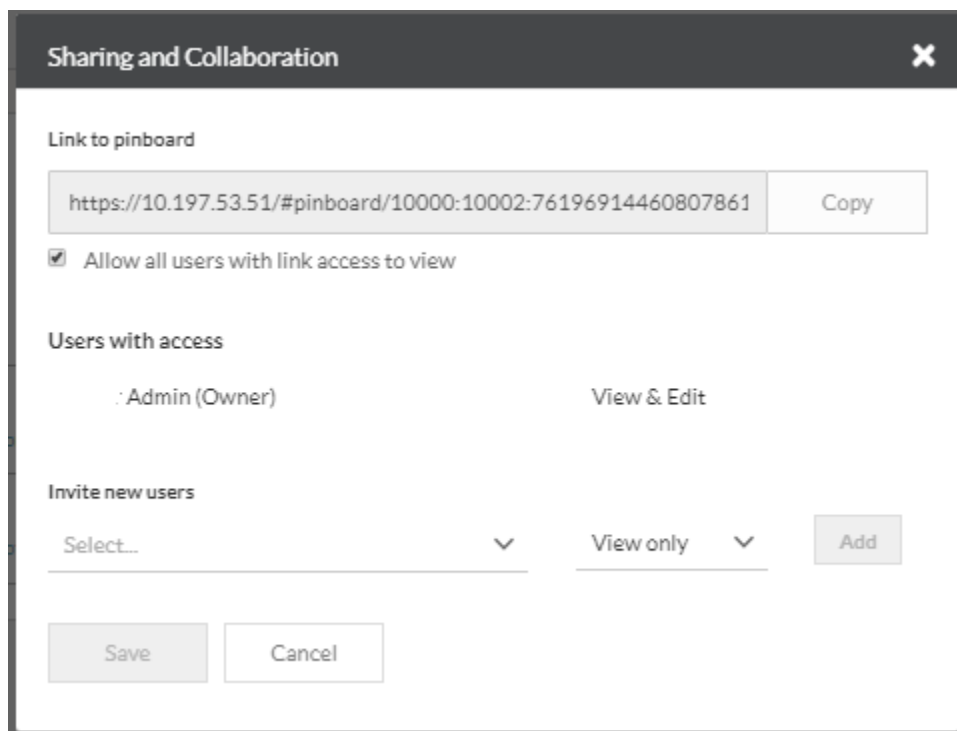
可以与其他用户共享您创建的插接板。管理员用户可以查看和删除任何插接板。以下是插接板的共享和协作功能：

如果已创建插接板，则不管您是管理员还是成员用户，都可以查看、编辑或删除它。

表 10-1.

插接板所有者	共享对象	特权	可能的操作
管理员	管理员	查看和编辑	查看、编辑、删除
	管理员	仅查看	查看、删除
	成员	View and Edit	查看、编辑
	成员	View only	查看
成员	管理员	View and Edit	查看、编辑、删除
	管理员	View only	查看、删除
	成员	View and Edit	查看、编辑
	成员	View only	查看

注 如果必须删除插接板，并且创建它的用户不可用，则管理员用户可以删除它。



要共享插接板，请执行以下操作：

步骤

- 1 在要共享的插接板上单击**更多选项**。
- 2 单击**共享**。
- 3 也可以通过单击**操作**下的共享图标，从**插接板库**共享插接板。

- 4 默认情况下，链接共享已启用。可以与已登录的任何用户共享插接板的链接。
- 5 可以添加要与其共享插接板的用户。可以为特定用户指定诸如 `view` 和 `view and edit` 之类的特权。

注 仅具有 `view` 特权的用户不能与其他任何用户共享插接板。

- 6 单击**保存**以保存您进行的共享和协作更改。
- 7 可以通过以下任一选项查看任何插接板的共享和协作信息。
 - 在**插接板库**中，可以在特定插接板的**已共享**列中查看共享信息。
 - 单击小组件上的插针图标。指向**最近修改**下列出的任何插接板，可查看有关所有者以及与其共享它的用户的详细信息。

将插接板设置为主页

可以将您选择的插接板设置为默认主页。

步骤

- 1 导航到要设置为主页的所需插接板。
- 2 单击**插接板选项**。单击**设置为主页**。

此特定插接板将设置为主页。

注 将插接板设置为主页后，就会禁用该插接板上的**设置为主页**选项。

- 3 在**我的首选项**页面的**设置**下，也可以将特定的插接板设置为默认主页。
- 4 如果要查看之前的主页，请单击左侧导航面板中**插接板**下的 **Network Insight 主页**。将弹出消息**是否要将 Network Insight 主页设置为主页？**。如果要恢复为默认主页，请单击**设置主页**。单击**关闭**以关闭消息。

注

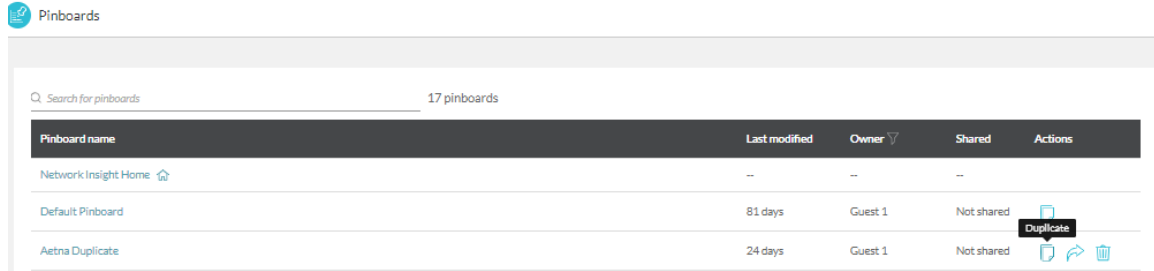
- 如果删除已设置为主页的插接板，则默认主页将重置为 **Network Insight 主页** 页面。如果您是要删除的插接板的所有者，则会弹出一条消息以确认删除。
 - 如果其他用户已将您创建的插接板设置为主页，则当您删除它时，将为该用户自动将主页恢复为 **Network Insight 主页**。
-

结果

复制插接板

步骤

- 1 对于插接板库的列表中的特定插接板，单击**操作**下的复制图标。



- 2 弹出窗口将出现，必须在其中输入插接板的名称。该描述与原始插接板的描述相同。单击**复制**。

注 插接板的名称是必需的。在输入名称之前，**复制**按钮不会启用。

- 3 如果尝试复制已共享的插接板，则可以选择保留源插接板用户和权限。如果要保留它们，则选择**保留源插接板用户和权限**。

注 如果要复制的插接板与具有只读访问权限的您共享，则看不到**保留源插接板用户和权限**选项。

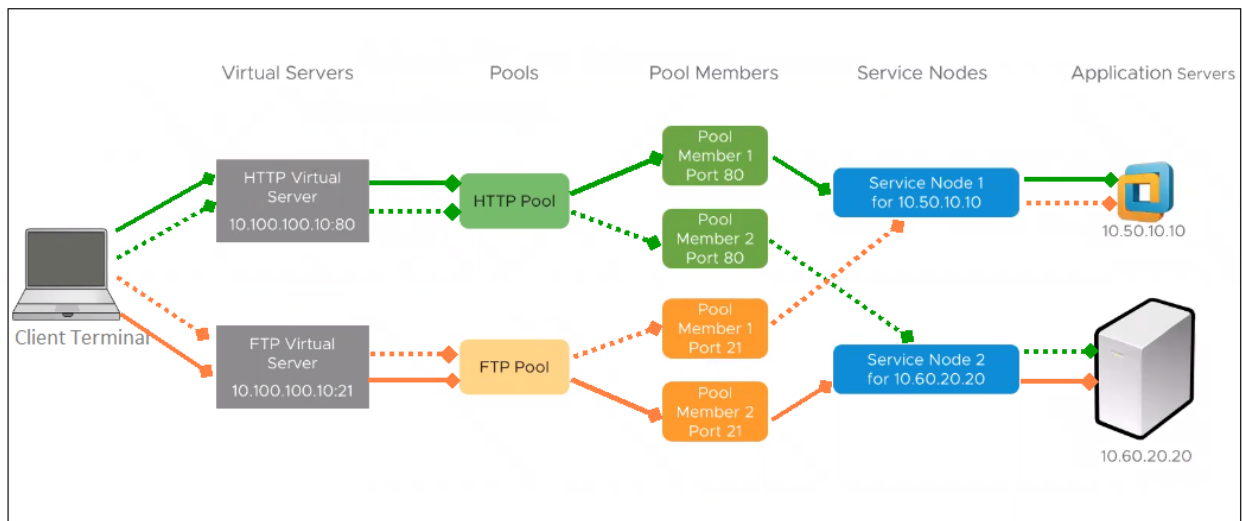
复制插接板的用户将成为新插接板的所有者。

F5 作为负载均衡器

11

为了支持和启用 F5 的负载均衡功能，已添加 vRealize Network Insight 所需的组件或实体。

F5 负载均衡器及其组件概览



- 应用程序服务器 - 托管应用程序的计算机。例如，如果您具有 Web 服务器，则您的服务器会在应用程序服务器（物理或虚拟服务器）上运行。
- 服务节点 - F5 将应用程序服务器表示为服务节点。因此，服务节点具有与应用程序服务器相同的 IP 地址或 FQDN。每个服务节点可以有多个应用程序。
- 池成员 - 逻辑实体。服务节点中的每个应用程序都由池成员表示，该池成员具有与服务节点相同的 IP 地址或 FQDN。要识别不同的应用程序，池成员会将端口号嵌入服务节点的 IP 地址中。
- 池 - 服务于一个应用程序的所有池成员分组为一个池。
- 虚拟服务器 - 应用程序的面向公众的 IP 地址。因此，要使用应用程序的客户端会连接到虚拟服务器 IP 地址（例如，10.100.100.10）和端口号（80 或 21）。
- 客户端终端 - 连接从客户端终端（即虚拟机）开始。

客户端请求连接到虚拟服务器，后者根据池确定池成员。然后，池成员将请求转发到应用程序服务器（虚拟机或物理服务器）。

注 单个应用程序服务器可以处理来自不同端口和不同服务节点的多个请求。

vRealize Network Insight 通过负载均衡功能支持提供其他优势：

- 用于确定应用程序服务器是物理服务器还是虚拟机。
- 允许您通过查看应用程序服务器（主机或虚拟机）信息（例如配置、性能和流）来轻松调试或解决问题。
- 在分布负载的应用程序中查看物理或虚拟网络连接组件。
- 针对环境中的任何问题发出警示，还有助于检测问题的原因。例如，由于服务节点虚拟机已关闭，应用程序没有响应。
- 提供端到端的流可见性。

本章讨论了以下主题：

- [NSX-V 作为负载均衡器](#)

NSX-V 作为负载均衡器

从 4.2 版本开始，vRealize Network Insight 支持并启用 NSX 的负载均衡功能。

以下是当前支持的衡量指标列表：

- 虚拟服务器
 - 接收的字节总数
 - 发送的字节总数
 - 当前会话数
 - 总会话数
- 池
 - 接收的字节总数
 - 发送的字节总数
 - 当前连接数
 - 最大连接数
 - 总连接数

当前，在 vRealize Network Insight 中，仅支持将虚拟机作为池成员。

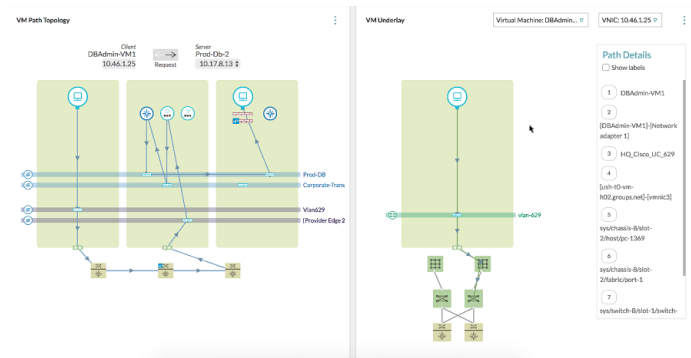
本章讨论了以下主题：

- 网络可见性
- 安全性

网络可见性

路径拓扑

路径拓扑绘制了环境中任何两个虚拟机之间存在的详细连接。



该拓扑同时涉及第 3 层和第 2 层组件。可以使用搜索查询 `vm_name_1` 到 `vm_name_2` 来查看此拓扑。如果路径存在，则虚拟机到虚拟机路径可视化将继续填充 `vm_name_1` 到 `vm_name_2` 之间存在的所有组件，还会绘制一条动画路径。如果路由器是物理路由器，则它们显示在边界外部。

在路径拓扑中，您会看到源和目标之间的虚拟机到虚拟机路径。如果未在虚拟机之间配置默认路径，则会显示一条错误消息，指示路径未定义或未找到路由器接口。

对于 Kubernetes，路径拓扑显示以下方案的路径：

- Kubernetes 服务到 Kubernetes 服务
- Kubernetes 服务到 Kubernetes Pod
- Kubernetes Pod 到 Kubernetes Pod

注 不支持涉及物理设备的路径。

通过负载均衡器的路径选项列出了在选定源和目标虚拟机的路径之间使用的所有负载均衡器。要查看通过特定负载均衡器的虚拟机之间的路径，请从列表中选择负载均衡器名称。如果将鼠标悬停在路径拓扑中的负载均衡器组件上，您将看到以下详细信息：

- 虚拟服务器名称
- 负载均衡器 IP 地址
- 端口号
- 负载均衡器算法
- 从负载均衡器中获取的默认网关。

您还可以查看路径拓扑中的路由组件。

如果将鼠标悬停在路径中涉及的任何路由器、Edge 或 LDR 上，则会显示完整的路由或 NAT 信息。

位于虚拟机路径拓扑右侧的“虚拟机底层”部分显示所涉及虚拟机的底层信息，及其到机架交换机顶部和所涉及端口的连接。对于 Kubernetes 实体，“虚拟机底层”显示 Pod 所在的虚拟机或 Kubernetes 节点信息。

在“虚拟机底层”部分中，如果选择**路径详细信息**下的**显示标签**，则对组件进行标记。在此部分中，顶部的下拉列表显示 Edge 上的端点虚拟机和活动虚拟机。对于每个 Edge 虚拟机，相邻的下拉列表会显示输入和输出接口 IP 地址。根据所选内容，将显示该特定接口的底层路径。

也可以使用拓扑图顶部的箭头反转路径方向。

通过拓扑图，可以更深入地了解有关虚拟机-虚拟机路径中所涉及端口的信息。在**路径详细信息**部分中，将显示实际端口通道的名称。

注 在物理正面没有第 2 层的完全可见性。如果数据包从一个交换机遍历到另一个交换机，则可能会涉及多个交换机。但拓扑不显示底层网络中的交换机。

AWS 虚拟机-虚拟机路径

AWS 的虚拟机-虚拟机路径提供内部部署虚拟机和 AWS EC2 实例之间的路径可见性。

当前，vRealize Network Insight 支持以下方案：

- **AWS VPC 内部虚拟机间路径：**此方案涉及特定 VPC 中同一子网或不同子网的虚拟机之间的通信。
- **通过对等连接的 AWS 对等 VPC 虚拟机间路径：**此方案涉及一个 VPC 的虚拟机与另一个 VPC 的虚拟机之间通过对等连接进行的通信。
- **AWS 虚拟机到 Internet：**VPC 中的虚拟机通过 Internet 网关与 Internet 进行通信。

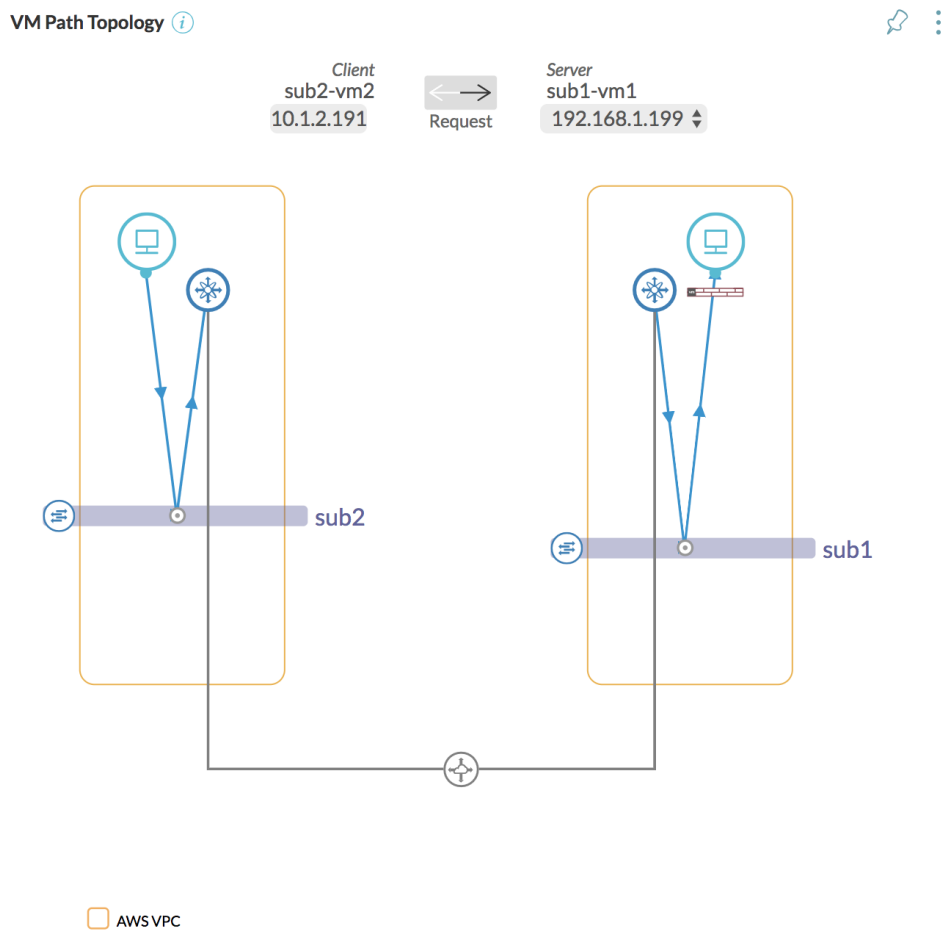
- 通过 AWS VPN 连接的 AWS 虚拟机到数据中心虚拟机：在此方案中，VPC 中的虚拟机通过 AWS VPN 连接与数据中心内的虚拟机进行通信。对于此方案，vRealize Network Insight 支持 SDDC 以及 NSX-V 和 NSX-T 数据中心。

注

- 仅当为 NSX-T 和 NSX-V Edge 路由器配置了公用 IP 地址时，NSX-T 和 NSX-V 数据中心的混合路径拓扑才起作用。
- vRealize Network Insight 不支持 AWS 的虚拟机底层拓扑。

注

通过对等连接的 AWS 对等 VPC 虚拟机间路径的 AWS 虚拟机-虚拟机路径示例如下：



可以通过在虚拟机-虚拟机路径中指向其图标来查看对等连接的属性。

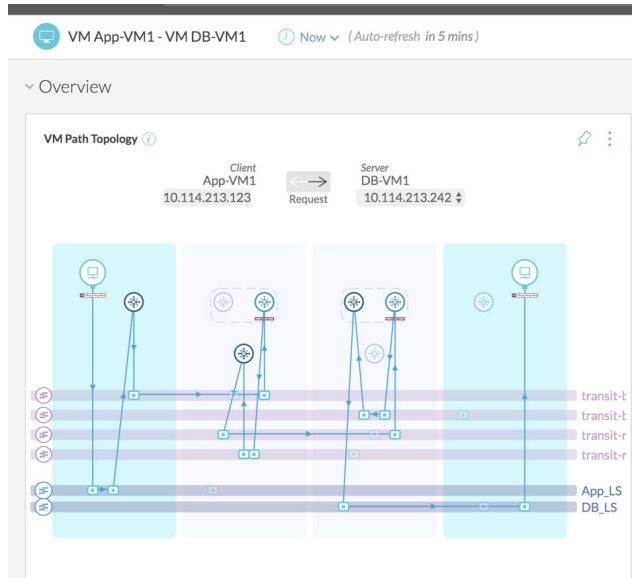
可以搜索与 AWS 虚拟机-虚拟机路径有关的以下实体：

- AWS Subnet
- AWS Route Table

- AWS Virtual Private Gateway
- AWS Internet Gateway
- AWS VPN Connection
- AWS VPC Peering Connection

NSX-T

NSX-T 的虚拟机-虚拟机路径示例如下所示：



蓝色表示主机节点，灰色表示 **Edge** 节点。屏幕右侧列出了虚拟机路径拓扑中使用的图标，以及“路径详细信息”下的标签。分布式路由器以相同的颜色显示，而与其所在的层无关。拓扑图中服务路由器的颜色会随关联层而变化。所有第 1 层组件都显示在同一级别，而所有第 0 层组件都显示在另一个不同的级别。在 NSX-T 中，Edge 防火墙用图进行描述。

要规划 NSX-T 网络的安全性，可以选择 **NSX-T Layer2 网络** 作为范围，并使用以下查询：

```
plan NSX-T Layer2 Network '<NAME_OF_NSX_T_LOGICAL_SEGMENT>'
```

通过执行以下步骤也可以获取相同的结果：

- 从导航侧栏中选择**安全性**。
- 从下拉菜单中选择 **NSX-T Layer2 网络** 作为范围。

注

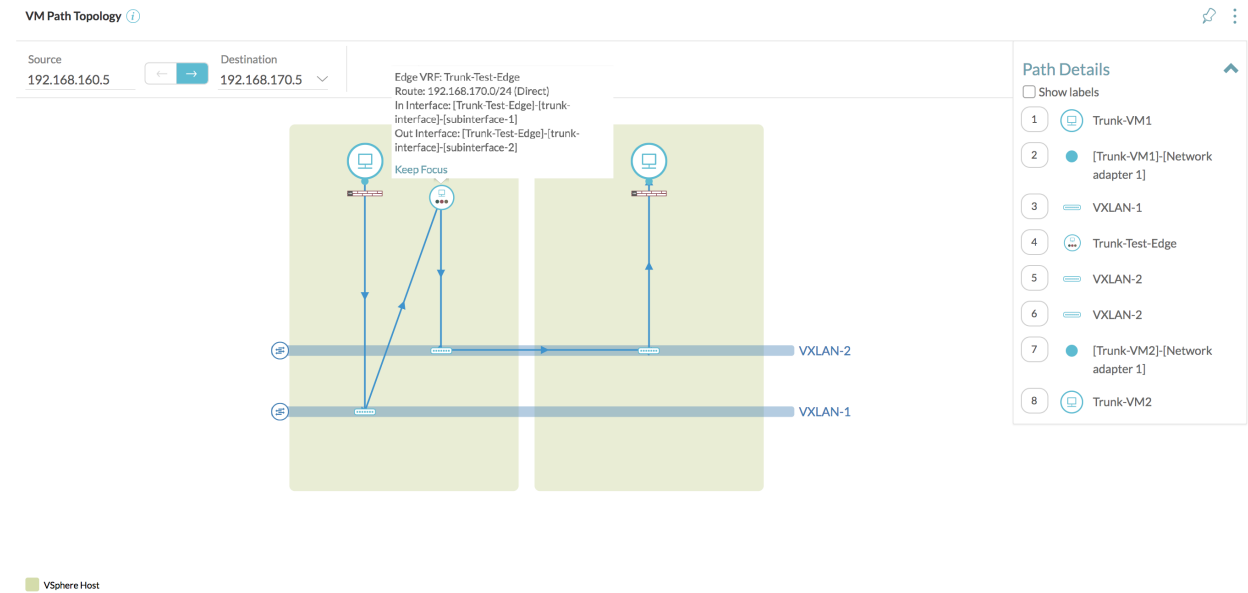
- 范围中提供了 NSX-T 相关实体，如 **NSX-T L2 网络** 和 **标记**。可以在规划、微分段和应用程序定义中使用这些 NSX-T 相关实体。
- 在**分组依据**下拉菜单中，**NSX-T 安全组**是安全标记的一部分，**逻辑分段**是 **VLAN/VXLAN** 的一部分。

NSX-V Edge 中继接口虚拟机-虚拟机路径

在 vRealize Network Insight 中，当 DVPG 连接到 NSX Edge 的中继 vNIC 并且子接口连接到 VLAN 或 VXLAN 时，您可以查看虚拟机-虚拟机路径和虚拟机到 Internet 路径。

以下是通过 NSX Edge 的虚拟机-虚拟机路径示例：

注 vRealize Network Insight 不支持 Edge 虚拟机中继接口的底层信息。



对 NSX-T 中 NAT 的支持

当前，vRealize Network Insight 在流和虚拟机到虚拟机路径中支持 SNAT、DNAT、反身规则。

要获取 NSX-T 中的所有 NAT 规则，请使用 NSX-T Edge NAT Rule 查询。要获取 NSX-V 和 NSX-T 中的所有 NAT 规则，请使用 NAT Rules 查询。

注意事项

- 对于具有已启用 NAT 服务的 NSX-T 逻辑路由器的虚拟机-虚拟机路径，vRealize Network Insight 不会为此类路径正确显示 NSX-T Edge 防火墙规则。
- 只有在 VMware NSX-T 层路由器的上行链路接口上配置的 NAT 规则才由虚拟机到虚拟机路径处理。如果在任何 NSX-T 层路由器上配置了 NAT，则连接到路由器的所有虚拟机都应该具有 NAT 规则，否则虚拟机到虚拟机路径和到 Internet 的路径不起作用。相反，它显示缺少规则的消息。
- vRealize Network Insight 支持嵌套的 NAT 层次结构。
- 仅支持基于 NSX-V 和 NSX-T 的 Edge。
- vRealize Network Insight 支持具有 NAT 定义的上行链路的 Edge 和层路由器。
- vRealize Network Insight 支持带有范围的 SNAT 规则。但是，DNAT 必须是目标和转换的 IP 地址之间的一对一映射（通过 NSX-V 的奇偶校验）。

■ vRealize Network Insight 不支持以下用例：

- a 在 NSX-T 中，可以在服务级别上应用 NAT 规则。例如，在 NSX-T 中，L4 端口集是一种服务类型，关联的协议可以是 TCP 或 UDP。因此，在虚拟机-虚拟机路径中，不支持服务级别详细信息。
- b 不支持任何端口级别转换。
- c 不支持 SNAT 匹配目标地址和 DNAT 匹配源地址。指定 SNAT 规则时，使用 SNAT 匹配目标地址作为目标 IP 地址。指定 DNAT 规则时，使用 DNAT 匹配源地址作为源 IP 地址。例如，如果存在 SNAT 规则中提及的目标 IP 地址，则 vRealize Network Insight 会应用 SNAT 规则，而不考虑数据包是否将目标地址作为目标 IP 地址。
- d 在同一逻辑路由器上使用 NAT 服务启用时，NSX-T Edge 防火墙对数据路径有影响。如果流与 NAT 和 Edge 防火墙都匹配，则 NAT 查找结果优先于防火墙。因此防火墙不应用于该流。如果流仅与防火墙规则匹配，则该流接受防火墙查找结果。

VMware SD-WAN 虚拟机-虚拟机路径

在 vRealize Network Insight 中，可以查看 VMware SD-WAN 部署的虚拟机-虚拟机路径。

vRealize Network Insight 支持以下方案：

- IP 到 IP 路径：两个 IP 都必须直接位于 VMware SD-WAN Edge 后面的 VLAN 上。
- IP 到 Internet/IP 到未知 IP：源 IP 必须直接位于 VMware SD-WAN Edge 后面的 VLAN 上。

注 Internet 或未知 IP 是 vRealize Network Insight 中未发现的任何 IP。

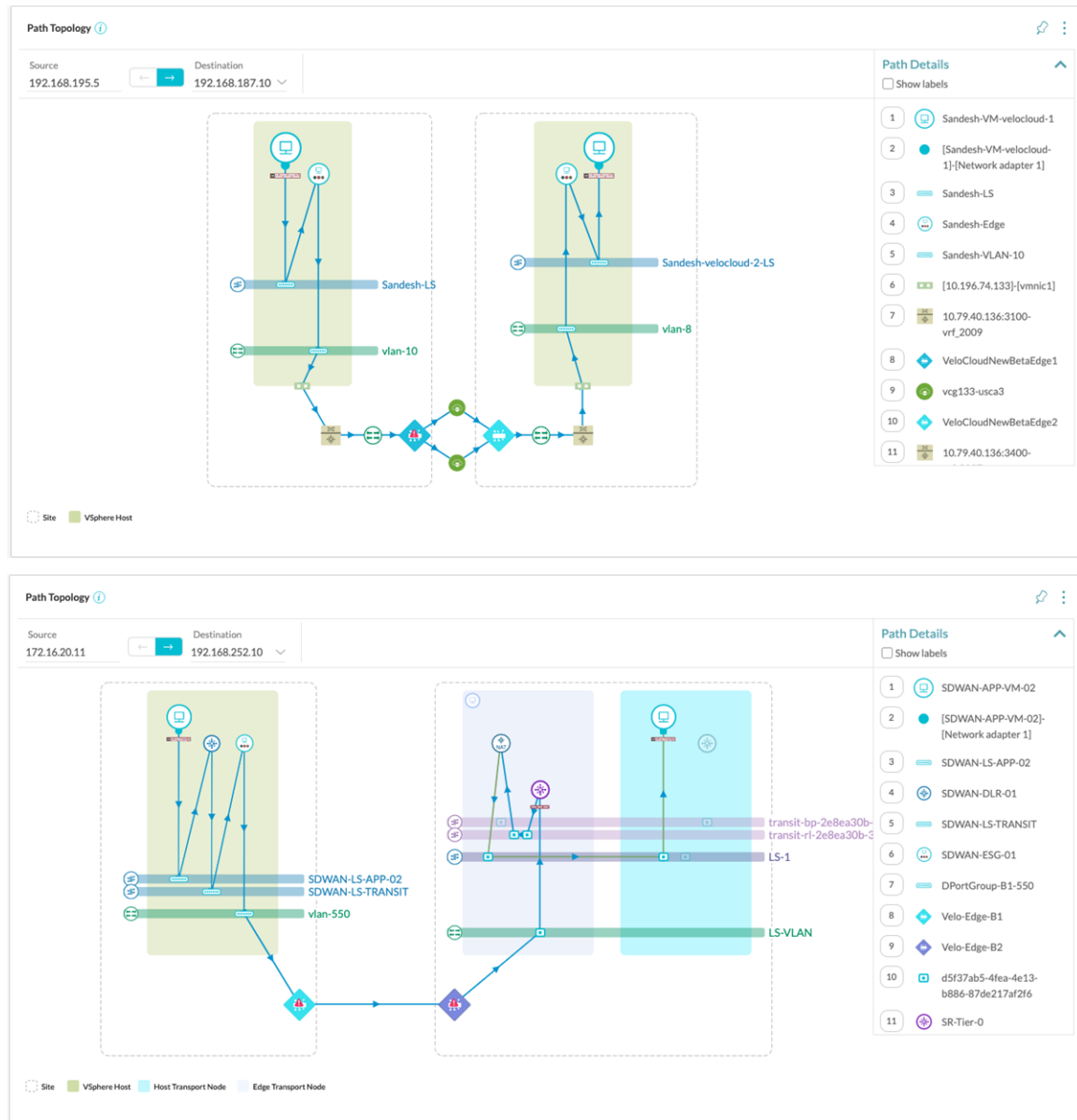
■ 虚拟机到 IP、IP 到虚拟机或虚拟机到虚拟机路径：

- 仅支持 NSX/NSX-T Data Center 中的虚拟机。不支持 VMware Cloud on AWS、Amazon Web Services 和 AZURE 中的虚拟机。
- VMware SD-WAN Edge 必须通过 VLAN 连接到数据中心内的物理/虚拟路由器。

- **注** 如果为源 VMware SD-WAN Edge 和目标 VMware SD-WAN Edge 配置的 VMware SD-WAN 网关不同，则会通过源 VMware SD-WAN Edge 的网关显示路径。

如果 VMware SD-WAN Edge 之间的分支到分支 VPN 通过 VMware SD-WAN 群集，则该群集中的所有成员都将显示在路径中。

以下是几个 VMware SD-WAN 虚拟机-虚拟机路径示例：



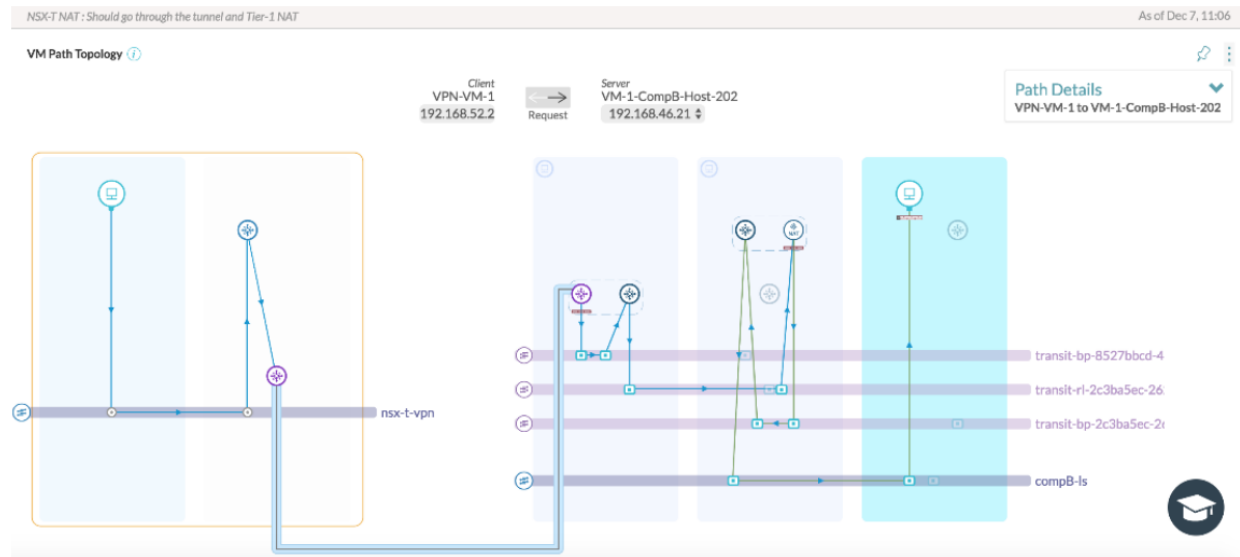
VMware Cloud on AWS: 虚拟机-虚拟机路径

vRealize Network Insight 在 VMware Cloud on AWS 中支持以下混合路径:

- VMware Cloud on AWS 和 VMware Cloud on AWS
- VMware Cloud on AWS 和 NSX-T
- VMware Cloud on AWS 和 NSX-V
- VMware Cloud on AWS 和 AWS
- VMware Cloud on AWS 内

对于 VMware Cloud on AWS 中存在的所有虚拟机，底层信息仅显示到虚拟机所在的分段，因为网络的底层物理元素已由 VMware Cloud on AWS 提取出，并且该级别不存在可见性。

VMware Cloud on AWS 和 NSX-T 虚拟机到虚拟机路径的示例如下所示：



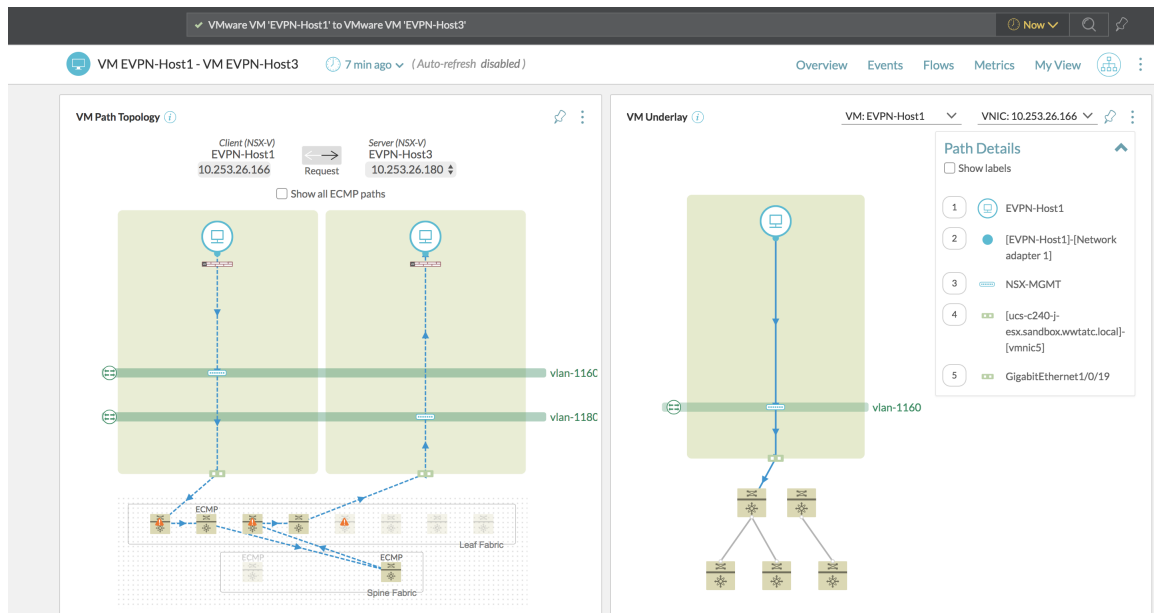
暗蓝色线描绘隧道。

支持 Cisco BGP-EVPN 模式

vRealize Network Insight 仅支持在企业版的 Cisco BGP-EVPN 配置模式下配置的 Cisco 9000 交换机的结构层。vRealize Network Insight 不支持具有 Cisco BGP-EVPN 配置的 Cisco Nexus 9000 以外的交换机型号。

属于结构层的每个 Cisco Nexus 9000 交换机会被单独添加为数据源。要查看结构层中的所有主干交换机或分支交换机，请使用 `switches where role is set` 查询。

Cisco BGP-EVPN 模式的虚拟机-虚拟机路径的示例如下所示：

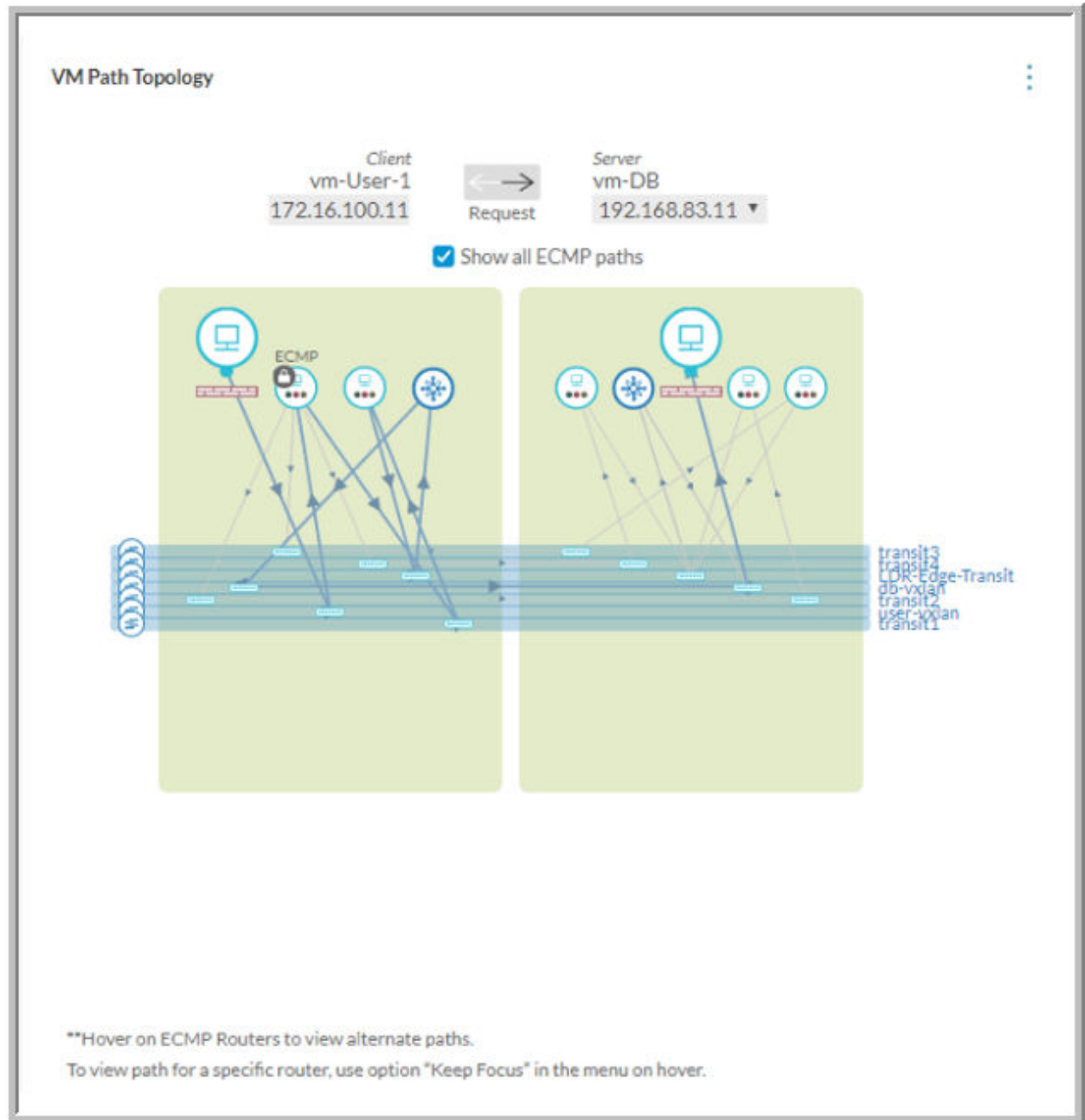


支持等价多路径 (ECMP) 路由

vRealize Network Insight 在虚拟机-虚拟机路径中提供 ECMP 支持。

虚拟机-虚拟机路径显示有关 ECMP 的以下信息：

- 从源到目标的多个 ECMP 路径
- 实现 ECMP 的路由器
- 给定路由器的可能出站路径 (VRF)
- 可能路径的路由



在上图中，可以看到已启用 ECMP 的路由器。如果指向这些路由器，则会显示其他路径。此外，还可以根据需要，通过选择和锁定路由器来创建路径。如果要查看两个虚拟机之间的所有 ECMP 路径，请在拓扑图中选择**显示所有 ECMP 路径**选项。

如果要查看特定路由器的路径，请指向该路由器，然后单击**保持焦点**。将显示特定于该路由器的路径。

对 L2 网桥的支持

L2 或 VLAN 网桥从多个 VLAN 创建单个广播域。在以前的版本中，如果虚拟机-虚拟机路径涉及两个或更多个 VLAN 之间的 L2 网桥，则虚拟机-虚拟机路径不起作用。从此版本起，vRealize Network Insight 支持 L2 桥接。当前，仅 Cisco ASA 路由器支持此功能。

监控 BGP 的各种状态

vRealize Network Insight 支持监控 BGP 的状态。可以查看 NSX edge 或逻辑路由器的 BGP 邻居。

步骤

- 1 在搜索栏中输入 Routers。
- 2 要查看特定 NSX Manager 的结果，请从左侧面板中选择 NSX Manager 以进行筛选。
- 3 展开列表中的特定路由器以查看详细信息。
- 4 可以在 **BGP 邻居**下查看以下信息。

- IP Address
- Remote AS
- Weight
- Keep Alive Time
- Hold Down Time
- Status

注

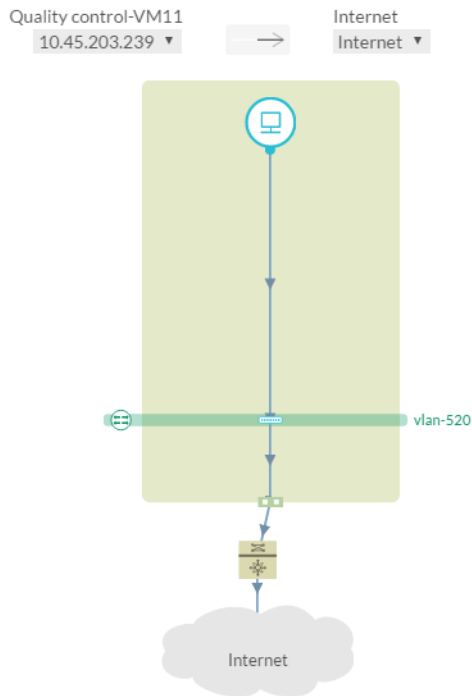
- 如果未提取有关邻居的信息，则 Status 将显示为 Unknown。
- 如果 Status 不是 Established.up，则为该 Edge 引发 One or more BGP neighbours are not in established state 事件。也可以在搜索 problems 时查看此事件。

到 Internet 的路径

对于环境中存在的每个虚拟机，vRealize Network Insight 向您显示如何在**到 Internet 的路径**插针中使用动画路径将虚拟机连接到 Internet。

该路径将填充在虚拟机与 Internet 之间存在的所有组件（虚拟和物理）。它绘制一个动画路径，该路径按顺序连接每个组件。也可以使用可视化上方的箭头反转路径方向。

将鼠标指针指向实体图标可获取其可寻址名称。单击路径上的图标可显示其主要属性的概述。也可以最大化插针以查看路径详细信息。



安全性

跨 vCenter NSX

在跨 vCenter NSX 环境中，可以拥有多个 vCenter Server，每个都必须与其自己的 NSX Manager 进行配对。

一个 NSX Manager 分配了主 NSX Manager 的角色，其他 NSX Manager 分配了辅助 NSX Manager 的角色。主 NSX Manager 用于部署通用控制器群集，该群集为跨 vCenter NSX 环境提供控制层面。辅助 NSX Manager 没有其自己的控制器群集。主 NSX Manager 可以创建通用对象，如通用逻辑交换机。这些对象通过 NSX 通用同步服务与辅助 NSX Manager 同步。可以在辅助 NSX Manager 中查看这些对象，但无法在其中编辑这些对象。必须使用主 NSX Manager 来管理通用对象。主 NSX Manager 可用于配置环境中的任何辅助 NSX Manager。

支持以下通用对象：

- 通用 LDR
- 通用传输区域
- 通用逻辑交换机
- 通用防火墙规则
- 通用安全组

- 通用 IPSet
- 通用服务
- 通用服务组
- 通用分段范围

Palo Alto 网络

vRealize Network Insight 支持 Palo Alto Panorama 防火墙。

注 vRealize Network Insight 不支持将 Palo Alto Panorama 与多个 NSX Manager 集成。

要在 vRealize Network Insight 中添加 Palo Alto Panorama，Palo Alto Networks 用户必须拥有具有 XML API 访问权限的**管理员角色**。执行以下步骤，为 XML API 添加管理员角色。

- 1 选择 **Panorama > 管理员角色**。
- 2 单击**添加**以添加新的管理员角色。
- 3 将打开“管理员角色配置文件”窗口。
- 4 输入角色的名称，然后选择 **Panorama**。
- 5 单击 **Web UI** 选项卡，然后禁用所有条目。
- 6 单击 **XML API** 选项卡，并禁用除**配置**和**操作请求**以外的所有条目。
- 7 单击**确定**关闭窗口。

新的管理员角色将显示在列表中。

- 8 单击**提交**。
- 9 将此角色分配给管理员帐户，或创建新用户并将此角色分配给新用户。

vRealize Network Insight 支持的 Palo Alto 网络功能如下所示：

- **Palo Alto 和 NSX 实体的相互关系：**Palo Alto 网络的地址和地址组的虚拟机成员资格基于 IP 地址到虚拟机的映射进行计算。可以按以下方式查询此成员资格信息：
 - `VM where Address = <>`
 - `Palo Alto address where vm = <>`
 - `VM where Address Group = <>`
 - `Palo Alto address group where vm = <>`

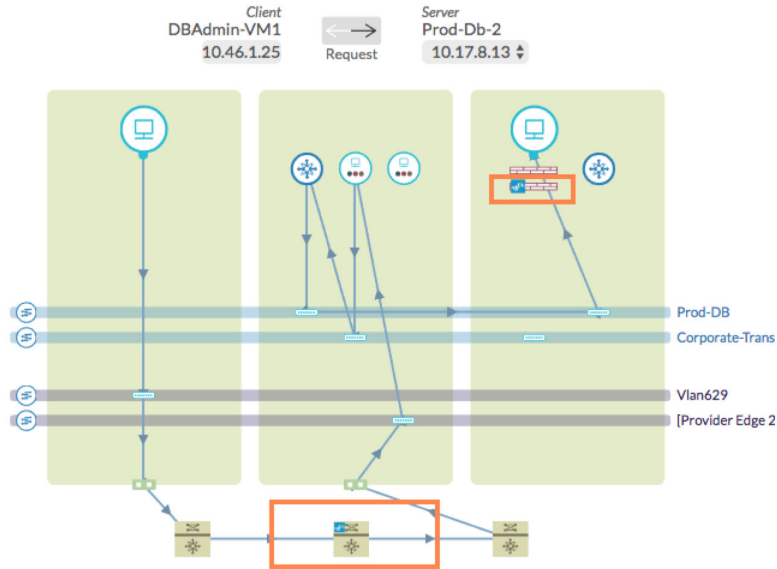
- **查询：**可以对 vRealize Network Insight 支持的所有 Palo Alto 实体执行查询。所有实体都以 Palo Alto 为前缀。一些查询如下所示：

表 12-1.

实体	查询
Palo Alto 地址	Palo Alto address where vm = <> VM where Address = <>
Palo Alto 地址组	Palo Alto address group where Translated VMs = <> VM where address group = <>
Palo Alto 设备	Palo Alto Device where Version = <> Palo Alto Device where connected = true Palo Alto Device where family = 'PA-5060'
Palo Alto 物理设备	Palo Alto Physical Device where model = 'PA-5060'
Palo Alto 虚拟机设备	Palo Alto VM Device where model = 'PA-VM'
Palo Alto 设备组	Palo Alto Device Group where device = <> Palo Alto Device Group where address = <> Palo Alto Device Group where address group = <>
Palo Alto 服务	Palo Alto service where Port = <> Palo Alto service where Protocol = <>
Palo Alto 服务组	Palo Alto service group where Member = <>
Palo Alto 策略	Palo Alto Policy where Source vm = <> and Destination vm = <> Palo Alto Policy where Source IP = <> and Destination IP = <>
Palo Alto 防火墙	Palo Alto firewall where Rule = <>
Palo Alto 区域	Palo Alto Zone where device = <>
Palo Alto 虚拟系统	Palo Alto Virtual System where Device = <> Palo Alto Virtual System where Device Group = <>

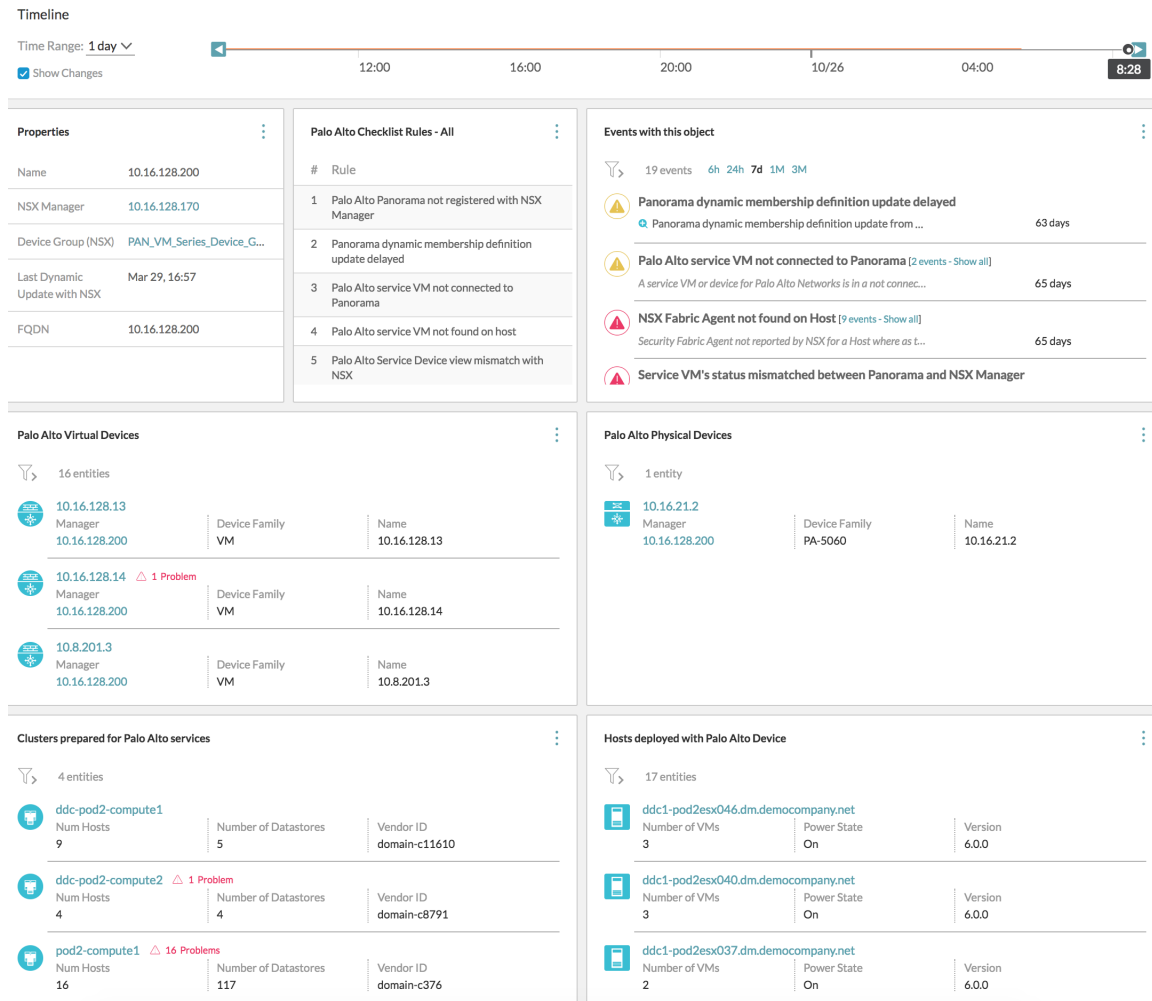
注 除了查询外，还可以使用面来分析搜索结果。

- **虚拟机到虚拟机路径：**作为虚拟机-虚拟机拓扑的一部分，vRealize Network Insight 在主机上显示 Palo Alto 虚拟机系列防火墙。单击防火墙图标时，将显示适用的规则。如果 Palo Alto 网络的防火墙设备（路由设备）也存在于路径中，则也会显示该设备。单击设备图标时，可以看到基本信息，如路由表、接口和包含已应用防火墙规则的表。



- 可以查看与 Palo Alto 网络的以下方案相关的一些系统事件：
 - Palo Alto 设备未连接到 Panorama（管理器）
 - NSX Manager 未在 Panorama 中注册
 - 在 palo alto 设备的 ESX 上未找到 NSX 结构层代理
 - 在 NSX 结构层代理的 Panorama 上未找到 Palo alto 设备
 - 安全组成员资格数据不同步
- 可以使用给定的 NSX Manager 在 Panorama 中创建和注册多个服务定义。如果不同的 ESXi 群集具有需要虚拟机系列防火墙以不同方式处理流量的工作负载，则创建多个服务定义。每个服务定义都具有从中选取策略的关联设备组。在 vRealize Network Insight 中显示虚拟机-虚拟机路径时，应考虑基于虚拟机群集信息的正确策略集。

Palo Alto Manager 仪表板示例

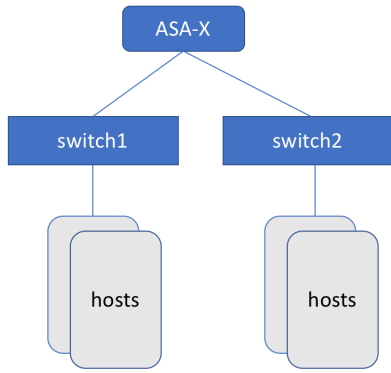


Cisco ASA 防火墙

vRealize Network Insight 支持 Cisco ASA 防火墙。

Cisco ASA 防火墙的功能如下所示：

- vRealize Network Insight 仅支持 Cisco ASA-X 系列。
- vRealize Network Insight 不支持 Firepower 模块。
- 当前，vRealize Network Insight 支持 Cisco ASA 操作系统版本 9.4。
- vRealize Network Insight 不支持 Cisco ASA 的群集部署。
- vRealize Network Insight 不支持 Cisco ASA 的高可用性。
- 如果 Cisco ASA 直接连接到主机，则它不受 vRealize Network Insight 支持。支持类似如下的拓扑：



- 仅支持 Extended 类型的 Cisco ASA 访问规则。不支持其他访问规则类型，如 Standard、WebType、EtherType 等。
- 如果在 Transparent 模式下配置防火墙，则虚拟机到虚拟机路径中的 Cisco ASA 防火墙不会显示适用的访问规则。

示例

可以对 vRealize Network Insight 支持的所有 Cisco ASA 实体执行查询。

表 12-2.

Cisco ASA 中的实体	关键字	示例查询
安全上下文	ASA 防火墙 ASA 安全上下文	asa firewall where access group = <>
访问规则	ASA 访问规则	asa access rule where source ip = <> asa access rule where destination ip = '192.168.2.2' asa access rule where port = <> asa access rule where interface = <>
访问组	ASA 访问组	asa access group where interface = <>
网络对象/网络对象组	ASA 网络对象 ASA 网络对象组	asa network object where ip address = <> asa network object group where ip address = <>
服务对象/服务对象组	ASA 服务对象 ASA 服务对象组	asa service object where port = <> asa service where protocol = <> asa service object group

Check Point 防火墙

vRealize Network Insight 支持以下 Check Point 管理服务器：

- Check Point 安全管理器 (SmartCenter)
- Check Point 多域管理器 (MDS/Provider-1)

Check Point 管理服务器应接受来自收集器 IP 地址的 API 访问。可以从**管理与设置 > 刀片 > 管理 API > 高级设置**中进行设置。

如果将 Check Point MDS 添加为数据源，则 vRealize Network Insight 将从用户定义的所有域和全局域中提取数据。

vRealize Network Insight 使用 Check Point 公共 Web API 从 Check Point 管理服务器提取数据。如果 VSX 网关连接到管理服务器，则我们使用基于 SSH 的 CLI 命令提取受 VSX 管理的虚拟系统 VS 路由表，以支持在虚拟机-虚拟机路径中显示 VS 网关。

vRealize Network Insight 需要对 Web-API 访问的只读特权，以便提取大多数 Check Point 数据。例外情况很少，如下所示：

- 如果非 VSX 物理网关连接到管理服务器，则用户应具有对 Web API 的读写访问特权。要获取网关路由以将 `run script Web API` 用于虚拟机-虚拟机路径计算，这一点是必需的。
- 如果 VSX 网关连接到管理服务器，则用户应具有使用相同密码的 SSH 访问权限。此外，用户还应具有对 CLI 命令 `vsx_util view_vs_conf` 的访问权限。此命令用于提取虚拟机-虚拟机路径计算的 VSX 网关路由。
- 为了使 MDS 服务器 IP 作为数据源，用户应具有对所有域（包括 MDS 域和全局域）的 Web API 访问权限。需要从所有域中提取规则、策略软件包和其他数据。

注

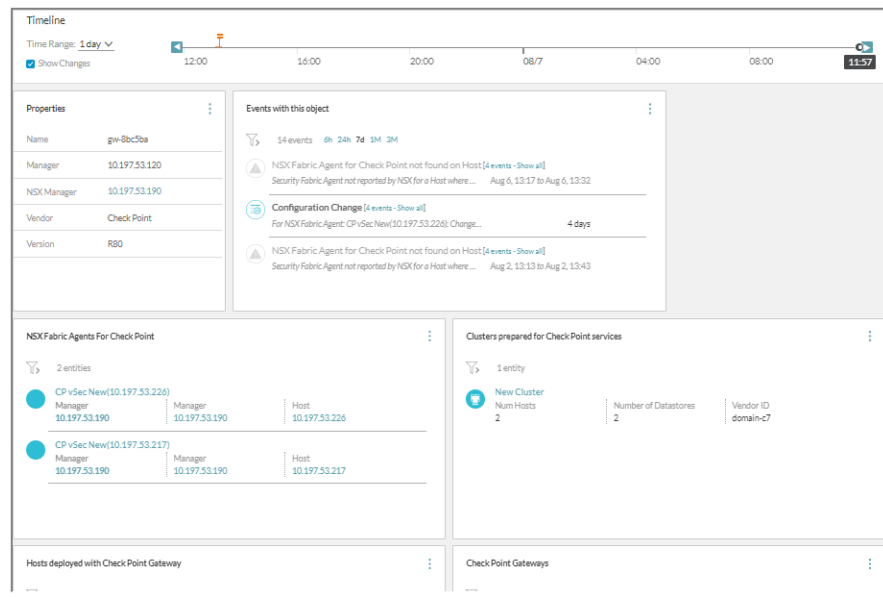
- vRealize Network Insight 支持 Check Point 防火墙版本 R80 和 R80.10。
- 对于虚拟机-虚拟机路径，vRealize Network Insight 不支持包含虚拟交换机和虚拟路由器的 VSX 群集。

可以对 vRealize Network Insight 支持的所有 Check Point 实体执行查询。所有实体都以 Check Point 为前缀。Check Point 的一些查询如下所示：

表 12-3.

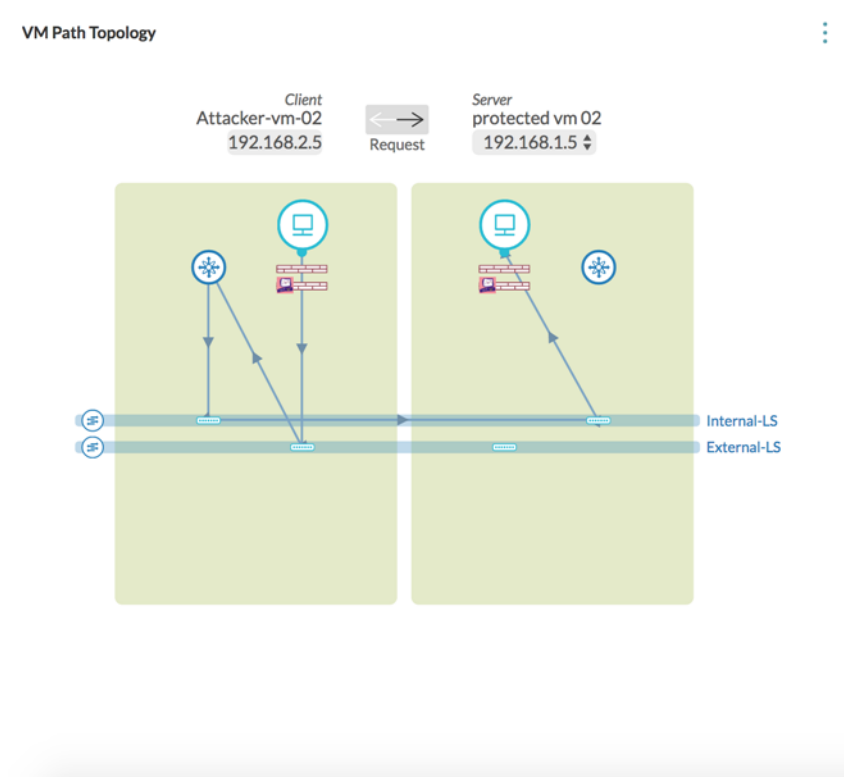
Check Point 中的实体	关键字	查询
IPset	Check Point Address Range Check Point Network	vm where Address Range = <> vm where Address Range = <> Check Point Address Range where Translated VM = <>
分组	Check Point Network Group	Check Point Network Group where Translated VM = <> vm where Network Group = <>
服务/服务组	Check Point Service Check Point Service Group	Check point service where Port = <> Check point service where protocol = <>
访问层	Check Point Access Layer	Check Point Policy where Access Layer = <>
域	Check Point Domain	check point domain where ip address = <> check point policy where domain = <> check point access layer where domain = <>
网关和网关群集	Check Point Gateway Check Point Gateway Cluster	Check Point Gateway Cluster where Policy Package = <>
策略软件包	Check Point Policy package	Check Point Policy where Policy Package = <> Check Point Policy Package where Rule = <>
策略	Check Point Policy	Check point policy where source ip = <> and Destination IP = <> Rule where source ip = <> and Destination IP = <> (will display other rules- nsx, redirect along with check point policies in the system)

Check Point 管理器仪表板的示例如下所示:



在虚拟机-虚拟机拓扑图中，可以查看主机上的 Check Point 服务虚拟机，以表示特定流量上应用的 Check Point 规则。VSX 管理的虚拟系统 (VS) 网关可以在虚拟机-虚拟机路径中视为物理网关。单击网关图标时，将显示适用的 Check Point 策略列表。

注 对于虚拟机-虚拟机路径，vRealize Network Insight 不支持包含虚拟交换机和虚拟路由器的 VSX 群集。



以下是为 Check Point 生成系统事件的一些方案：

- 在 Check Point 网关的 ESX 上未找到 NSX 结构层代理。
- 未找到 Check Point 服务虚拟机。
- Check Point 网关 sic 状态为“未通信”。
- Check Point 实体（如地址范围、网络、策略、组、策略软件包、服务、服务组等）的发现和更新事件功能

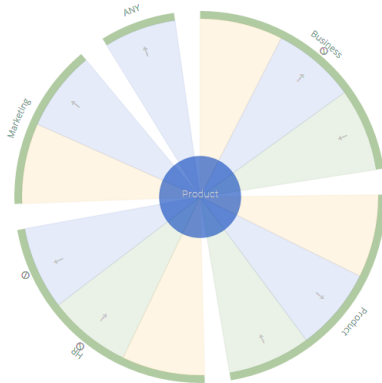
安全组

安全组是通过通用权限集进行管理的组的集合。

安全组拓扑具有以下两个视图：

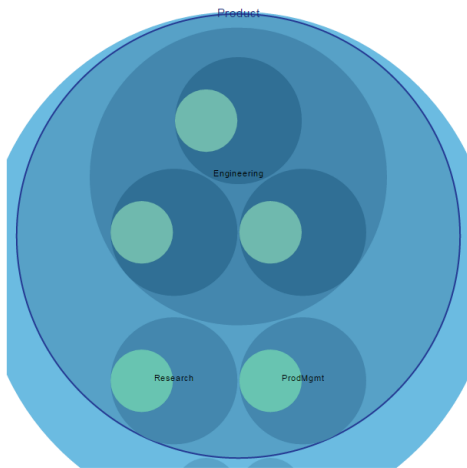
防火墙视图

安全组防火墙拓扑通过展示安全组之间适用的防火墙规则来显示所选安全组与其他安全组之间的关系。



容器视图

安全组容器拓扑显示如何相对于其父安全组或子项（安全组或其他实体）来构造安全组。



基于策略的 VPN

vRealize Network Insight 在 VMware Cloud on AWS、NSX-T 和 NSX-V 中支持基于策略的 VPN。基于策略的 VPN 支持以下方案：

- VMware Cloud on AWS 公用 IP 地址与 NSX-V/NSX-T/AWS 公用 IP 地址之间的 VPN 隧道
- 从 VMware Cloud on AWS 公用 IP 地址和企业防火墙公用 IP 地址到企业防火墙公用 IP 地址与内部 NSX Edge 之间 1:1 NAT 的 VPN 隧道

注 vRealize Network Insight 不支持 VPN 隧道来自结束于企业防火墙的 VMware Cloud on AWS 且未使用内部 NSX Edge 配置 NAT 的方案。

基于策略的 VPN 实体

vRealize Network Insight 为 L3 VPN Session 实体提取数据，该实体是在数据中心内配置的实际 VPN。

以下是基于策略的 VPN 实体的搜索词：

表 12-4.

搜索词	描述
Policy based VPN	VMware Cloud on AWS、NSX-V 和 NSX-T 的所有基于策略的 VPN 会话
VMC Policy based VPN	VMware Cloud on AWS 基于策略的 VPN 会话
NSX-T Policy based VPN	NSX-T 基于策略的 VPN 会话
NSX Policy based VPN	NSX 基于策略的 VPN 会话

NSX 分布式防火墙非活动规则

vRealize Network Insight 支持在某些时间没有流的 NSX 分布式防火墙规则的可见性。这些规则称为非活动规则。此类规则使用内存堆，可能会导致安全问题。为监控这些非活动规则，vRealize Network Insight 在**安全性**仪表板中提供了以下两个小组件：

注 要查看“安全性”仪表板，请在搜索栏中输入**安全性**。

- 未使用的 NSX 防火墙规则：此小组件列出在给定时间未报告任何流的所有 NSX 防火墙规则。也可以使用以下搜索查询检索这些规则：

```
nsx firewall rule where flow is not set
```

注 请确保已为指定的时间启用 NSX 分布式防火墙 IPFIX。

Fortinet 防火墙

在 vRealize Network Insight 中，您可以查看有关 Fortinet 防火墙的见解。

vRealize Network Insight 支持以下 Fortinet 实体 -

- Fortinet Manager
- Fortinet ADOM - Fortinet 管理域详细信息
- Fortinet VDOM - Fortinet 虚拟域详细信息。vRealize Network Insight 仅支持基于流的筛选。不支持透明模式。
- Fortinet 地址 - ADOM 特定地址的列表。vRealize Network Insight 支持 ipmask、iprange 和 NSX 结构层连接器。
- Fortinet 地址组 - ADOM 特定地址组的列表
- Fortinet 动态地址 - ADOM 特定动态地址（VDOM 映射的地址）的列表
- Fortinet 动态地址组 - ADOM 特定动态地址组（VDOM 映射的地址组）的列表
- Fortinet 动态接口 - ADOM 特定动态接口的列表。
- Fortinet 区域 - ADOM 特定区域的列表。
- Fortinet 服务 - 每个 ADOM 的手动和自动生成的服务列表。
- Fortinet 服务组 - 每个 ADOM 的服务组列表。
- Fortinet 策略 - 每个 ADOM 的 Fortinet 策略。目前，我们仅支持 IPv4 策略、Fortinet 全局页眉策略和 Fortinet 全局页脚策略。
- Fortinet 策略软件包 - 策略软件包列表。策略软件包名称还包含软件包名称前面的策略软件包的路径。
- Fortinet 设备 - 与 FortiManager 关联的 Fortinet 设备的列表。
- Fortinet 设备组 - 由用户指定的 Fortinet 设备组的列表。

不支持以下内容：

- NAT 模式下虚拟机到虚拟机路径。
- 透明模式下物理设备的虚拟机到虚拟机路径。
- 高级（非基于 IP）策略属性，如用户、用户组、应用程序和安全配置文件。

在 vRealize Network Insight 中配置流

13

本章讨论了以下主题：

- 启用 IPFIX 配置
- 对物理服务器的流支持
- 查看已阻止的流和受保护的流
- 网络地址转换 (NAT)
- VMware Cloud on AWS 个流
- 创建 VPC 流日志
- 将流记录从 F5 发送到 vRealize Network Insight 收集器

启用 IPFIX 配置

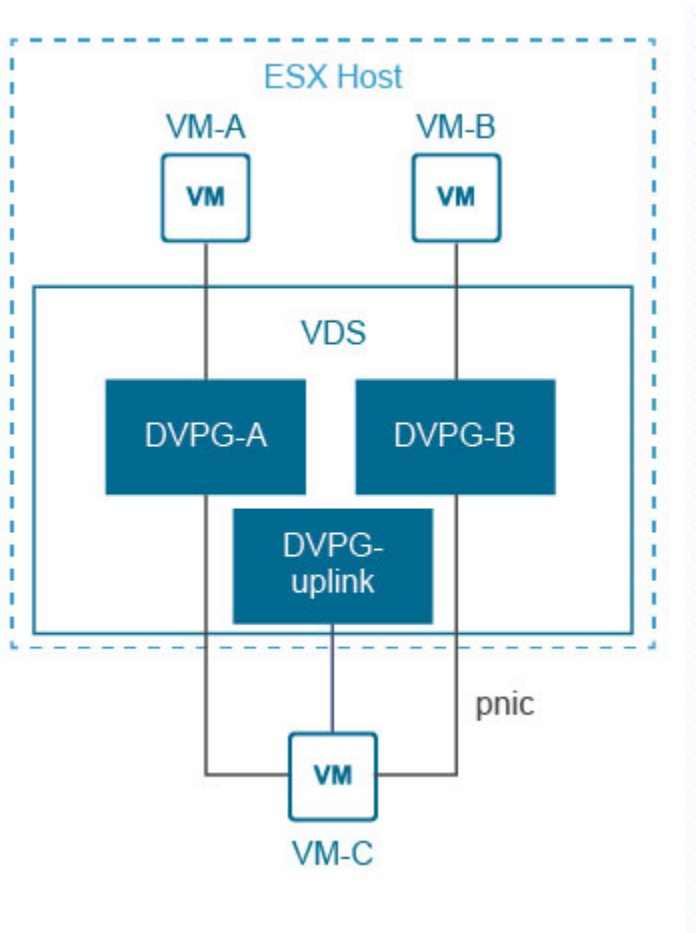
IPFIX 是用于导出流信息的 IETF 协议。

流被定义为在特定时间段内传输且共享相同的 5 元组值（源 IP 地址、源端口、目标 IP 地址、目标端口和协议）的一组数据包。流信息可能包括时间戳、数据包/字节计数、输入/输出接口、TCP 标志、VXLAN ID、封装的流信息等属性。

VDS 和 DVPG 上的 IPFIX 配置

可以将 vSphere 环境中的 VDS 配置为使用 IPFIX 导出流信息。必须在附加到 VDS 的所有端口组上启用流监控。如果数据包到达 VDS 的端口 X 并从端口 Y 退出，则在端口 Y 上启用流监控时会发出对应的流记录。

要分析任何会话的完整信息，需要有关这两个方向的数据包的 IPFIX 数据。请参阅下图，其中 VM-A 连接到 DVPG-A，并与 VM-C 进行通信。此处 DVPG-A 仅提供有关 C→A 数据包的数据，而 DVPG-Uplink 提供有关 A→C 数据包的数据。要获取 A 的完整流量信息，应在 DVPG-A、DVPG-uplink 上启用 IPFIX。



vRealize Network Insight 代理虚拟机具有 IPFIX 流信息的内置收集器/接收方。可以在“vCenter 数据源”设置中按不同的粒度级别启用 IPFIX 信息收集。

在 VDS 和 DVPG 上启用 IPFIX 配置

要在 vCenter 级别上启用 IPFIX 信息，请执行以下操作：

步骤

- 1 添加 vCenter 时，选择**启用 Netflow (IPFIX)**。
- 2 从 vCenter 中可用 VDS 的列表中选择要为其启用 IPFIX 的 VDS。
- 3 对于其中一个主机具有不支持的 ESXi 版本的 VDS，将显示通知图标。如果 vRealize Network Insight 检测到 IPFIX 已为 VDS 配置了除 vRealize Network Insight 代理虚拟机以外的其他某个 IP 地址，则会显示**替代**按钮。单击**替代**以查看该 VDS 下的 DVPG 列表。
- 4 将显示所选 VDS 的可用 DVPG 列表。默认选定所有 DVPG。打开**手动选择**以选择要为其启用 IPFIX 的特定 DVPG。选择所需的 DVPG，然后单击**提交**。

注 带有通知图标的 DVPG 表示它是上行链路 DVPG，且必须选择它。

VMware NSX IPFIX 配置

VMware NSX IPFIX 提供与物理设备所提供类似的网络监控数据，并为管理员提供虚拟网络情况的清晰视图。

VMware NSX 允许网络管理员将网络与物理硬件分离，从而对网络进行虚拟化。利用此功能，可以轻松地将网络扩展和收缩网络，并使网络对遍历它的应用程序变得透明。

通过在虚拟化网络中使用 NSX IPFIX，网络管理员可以查看虚拟覆盖网络。在主机上行链路上启用了使用 Netflow 的 VXLAN IPFIX 报告。它提供了封装数据包的 VTEP 的可见性，以及在 NSX 逻辑交换机 (VXLAN) 上生成主机间流量的虚拟机的详细信息。

分布式防火墙实现流的有状态跟踪。这些跟踪的流经历一组状态更改时，IPFIX 可用于导出有关该流状态的数据。

跟踪的事件包括流创建、流拒绝、流更新和流拆卸。被拒绝的事件导出为 syslog。

启用 VMware NSX-V IPFIX

要在 vRealize Network Insight 中启用 VMware NSX-V IPFIX，请执行以下操作：

前提条件

- 确保您具有安全管理员或企业管理员凭据。
- 建议在必须从其收集 NSX IPFIX 数据的所有 DVS 和 DVPG 上启用 VDS IPFIX。可以从关联 vCenter 的详细信息页面启用 VDS IPFIX。

步骤

- ◆ 添加或编辑 NSX-V Manager 数据源时，选择**启用 IPFIX**。

启用 VMware NSX-T DFW IPFIX

要在 vRealize Network Insight 中启用 VMware NSX-T IPFIX，请执行以下操作：

前提条件

- 确保具有以下特权之一：
 - enterprise_admin
 - network_engineer
 - security_engineer
- 确保分布式 (DFW) 防火墙已启用。
- 确保优先级 0 可用于 Network Insight IPFIX 配置文件。如果存在另一个优先级为 0 的 IPFIX 配置文件，则必须将其更改为某个其他值。

步骤

- ◆ 添加或编辑 NSX-T Manager 数据源时，选择**启用 IPFIX**。

后续步骤

启用 IPFIX 后，vRealize Network Insight 会在 NSX-T 上创建自己的 Network Insight 收集器配置文件和 Network Insight IPFIX 配置文件。确保不修改其中的任何配置文件。

在 NSX-T 上启用 IPFIX 后，如果在 vRealize Network Insight 中未看到流，则可能会发生以下事件：

- 在 NSX-T Manager 中未注册 Network Insight 收集器配置文件。
- 在 NSX-T Manager 中未注册 Network Insight IPFIX 配置文件
- Network Insight IPFIX 配置文件端口号已更改。
- Network Insight 收集器配置文件与 NSX-T Manager 中的 Network Insight IPFIX 配置文件不匹配。

注 要解决上述所有问题，请再次启用 NSX-T IPFIX。

- Network Insight IPFIX 配置文件的优先级在 NSX-T Manager 中不为零。

要解决此问题，请登录到 NSX-T Manager，并将 Network Insight IPFIX 配置文件的优先级设置为零。

- Network Insight 收集器 IP 无法添加到 NSX-T Manager 的现有 Network Insight 收集器配置文件中。

从 NSX-T Manager 中的 Network Insight 收集器配置文件中删除其中一个收集器，然后从数据源页面重新启用 NSX-T IPFIX。

- 分布式防火墙在 NSX-T Manager 中已禁用。

登录到 NSX-T Manager 并启用 DFW 防火墙。

对于 NSX-T 2.4，在 NSX-T 上启用 IPFIX 后，如果在 vRealize Network Insight 中未看到流，则可能会发生以下事件：

- NSX-T Manager 收集器配置文件中缺少 Network Insight IPFIX 收集器配置。
- NSX-T Manager 中缺少 DFW IPFIX 配置文件。

要解决这些问题，请再次启用 DFW IPFIX。

注 NSX-T 中存在的所有逻辑交换机将在 10-15 分钟内附加在 IPFIX 配置文件中。

对物理服务器的流支持

vRealize Network Insight 支持发送版本 v5、v7 和 v9 的 NetFlow 数据的设备。如果提供了 DNS 映射和子网-VLAN 映射信息，则 vRealize Network Insight 可以使用 DNS 域、DNS 主机名、子网和第 2 层网络来扩充 NetFlow 数据。此功能仅适用于企业级许可证用户。

要在 vRealize Network Insight 中配置 NetFlow，请执行以下步骤：

- 1 为 NetFlow 和 sFlow 添加物理流收集器。
- 2 在物理设备中配置 NetFlow 收集器。
- 3 导入 DNS 映射文件。

4 配置子网与 VLAN 之间的映射。

在物理设备中配置 NetFlow 收集器

要将 NetFlow 信息发送到 vRealize Network Insight NetFlow 收集器，请手动配置物理设备。以下是大多数物理设备中的配置步骤：

1 创建流记录。

流记录的必填字段如下所示：

- 将以下字段标记为 Match。
 - `ipv4 protocol`
 - `ipv4 source address`
 - `ipv4 destination address`
 - `transport source-port`
 - `transport destination-port`
 - `interface input`
- 将以下字段标记为 Collect。
 - `direction`
 - `counter bytes`
 - `counter packets`
 - `timestamp sys-uptime first`
 - `timestamp sys-uptime last`
- 将以下字段标记为 Match 或 Collect。否则，跳过它。
 - `transport tcp flags`

2 创建流导出器。

- 提供 vRealize Network Insight NetFlow 代理 IP 和端口 2055。

3 配置流缓存，如下所示：

- 活动超时：30 秒
- 非活动超时：60 秒

4 使用创建的流记录和流导出器创建流监控器。

5 在每个接口上配置监控器。

前提条件

示例

以下几节提供配置物理设备的示例步骤：

- [Cisco 4500](#)
- [Cisco Nexus 1000v](#)
- [Cisco Nexus 9000](#)

注 这些步骤可能因版本和设备而异。

Cisco 4500

1 创建流记录

```
configure terminal

flow record netflow-original

match ipv4 protocol

match ipv4 source address

match ipv4 destination address

match transport source-port

match transport destination-port

match interface input

collect transport tcp flags

collect counter bytes

collect counter packets

collect timestamp sys-uptime first

collect timestamp sys-uptime last

End
```

2 创建流导出器

```
configure terminal

flow exporter e1

destination <PROXY_IP>

transport udp 2055

end
```

3 创建流监控器

```
configure terminal
```

```
flow monitor m1  
  
record netflow-original  
  
exporter e1  
  
end
```

4 配置超时

```
configure terminal  
  
cache timeout inactive 30  
  
cache timeout active 60  
  
end
```

5 在输入模式和输出模式下或者至少在输入模式下为每个接口配置流监控器

```
configure terminal  
  
interface <INTERFACE_NAME>  
  
ip flow monitor m1 unicast input  
  
end
```

Cisco Nexus 1000v

1 配置超时

```
configure terminal  
  
Active timeout 60  
  
Inactive timeout 15  
  
end
```

2 配置导出器

```
configure terminal  
  
flow exporter <EXPORTER_NAME>  
  
destination <PROXY_IP>  
  
transport udp 2055  
  
source <VSM_IP_OR_SUBNET>  
  
end
```

3 要为每个接口配置流监控器，请执行以下操作：

```
configure terminal  
  
flow monitor <MONITOR_NAME>
```

```
record netflow-original
exporter <EXPORTER_NAME>
end
```

- 4 在输入模式和输出模式下或者至少在输入模式下为每个接口配置流监控器

```
configure terminal
port-profile type vethernet <IF_NAME>
ip flow monitor <MONITOR_NAME> input
ip flow monitor <MONITOR_NAME> output
.
.
end
```

Cisco Nexus 9000

以下是 Cisco Nexus 9000 的一些设备命令示例:

- 1 启用 NetFlow 功能

```
configure terminal
feature netflow
end
```

- 2 创建流记录

```
configure terminal
flow record vrni-record
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
collect transport tcp flags
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
```

```
collect timestamp sys-uptime last

End
```

3 创建流导出器

```
configure terminal

flow exporter vrni-exporter

destination <PROXY_IP>

transport udp 2055

version 9

source <INTERFACE_NAME>

end
```

4 为每个接口创建流监控器

```
configure terminal

flow monitor vrni-monitor

record vrni-record

exporter vrni-exporter

end
```

5 配置超时

```
configure terminal

cache timeout inactive 30

cache timeout active 60

end
```

6 在输入模式和输出模式下或者至少在输入模式下为每个接口配置流监控器

```
configure terminal

interface <INTERFACE_NAME>

ip flow monitor vrni-monitor input

end
```

扩充流和 IP 端点

可以通过 UI 导入 DNS 映射和子网-VLAN 映射信息。

基于 DNS 数据的导入和子网-VLAN 映射的规范，使用以下类型的信息扩充流信息。

■ 源 DNS 域

- 源 DNS 主机名
- 目标 DNS 域
- 目标 DNS 主机名
- 源 L2 网络
- 源子网网络
- 目标 L2 网络
- 目标子网网络

基于 DNS 数据的导入和子网-VLAN 映射的规范，使用以下类型的信息扩充 IP 端点信息。

- DNS 域
- DNS 主机名
- FQDN
- L2 网络
- 子网网络

有关通过 DNS 信息扩充流的详细信息，请参阅[导入 DNS 映射文件](#)。

有关通过子网-VLAN 映射扩充流的详细信息，请参阅[配置子网与 VLAN 之间的映射](#)。

注

- 仅为物理 IP 增强 DNS 映射和子网信息。没有子网或 DNS 映射信息与任何虚拟网卡关联。
 - 仅在导入此信息后，才会为已被 vRNI 发现的流扩充信息。
-

搜索物理到物理流

可以基于以下属性搜索物理到物理流：

- 源 DNS 主机
- 目标 DNS 主机
- 源 DNS 域
- 目标 DNS 域
- 源子网网络
- 目标子网网络

可以基于以下属性搜索物理-物理流。使用扩充的 DNS 和子网-VLAN 映射信息进行流搜索查询的几个示例如下所示：

```
bytes,Dns Domain,Dns Host,l2 network of flows where flow type = 'Physical-Physical'
```

```
bytes,Dns Domain,Dns Host,l2 network of flows where flow type = 'Source is VM' and  
flow type = 'Destination is Physical'
```

```
bytes,Dns Domain,Dns Host,l2 network of flows where flow type = 'Source is Internet'  
and flow type = 'Destination is Physical'
```

查看已阻止的流和受保护的流

通过 NSX-IPFIX 集成，可以查看系统中已阻止的流和受保护的流。

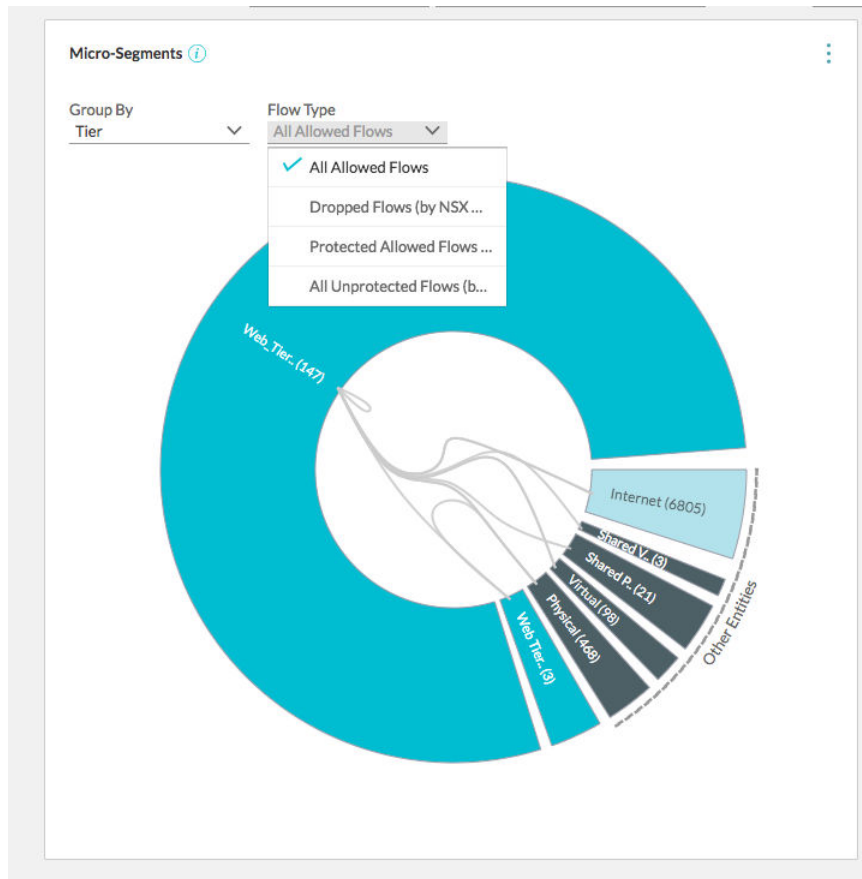
“微分段规划”页面中的基本筛选器如下所示：

- 所有已允许的流：默认选中此选项。要查看防火墙规则中的操作设置为**已允许**的所有流，请选择此选项。
- 已丢弃的流：此选项有助于检测已丢弃的流并以更好的方式来规划安全性。
- 所有受保护的流：此选项有助于检测具有与其关联的类型不为 `any(source)any(dest)any(service)allow` 的规则的所有流。此类流称为受保护的流。
- 所有不受保护的流：此选项有助于检测具有 `any(source)any(dest)any(service)allow` 类型的默认规则的所有流。此类流称为不受保护的流。

防火墙规则仅对已允许的流和不受保护的流可见。

例如，如果处于规划阶段，且要查看系统中已允许的流，请执行以下步骤：

- 1 在“微分段规划”页面中，对于特定的组，从下拉菜单中选择**所有已允许的流**。
- 2 单击拓扑图中已丢弃的流，以查看相应的建议防火墙规则。
- 3 将防火墙规则导出到 **NSX Manager** 以对其加以实施。



网络地址转换 (NAT)

vRealize Network Insight 中的 NAT 流支持如下所示：

- 当前，vRealize Network Insight 仅支持流中的 SNAT、DNAT、反身规则以及 NSX-V 和 NSX-T Edge 的虚拟机到虚拟机路径。

注 不支持 NSX Edge 版本 5.5 或早期版本上的 NAT 规则。

- 要获取 NSX-T 中的所有 NAT 规则，请使用 NSX-T Edge NAT Rule 查询。要获取 NSX-V 和 NSX-T 中的所有 NAT 规则，请使用 NAT Rules 查询。
- 只有在 VMware NSX-T 层路由器的上行链路接口上配置的 NAT 规则才由虚拟机到虚拟机路径处理。如果在任何 NSX-T 层路由器上配置了 NAT，则连接到路由器的所有虚拟机都应该具有 NAT 规则，否则虚拟机到虚拟机路径和到 Internet 的路径不起作用。相反，它显示缺少规则的消息。
- vRealize Network Insight 支持嵌套的 NAT 层次结构。
- vRealize Network Insight 支持具有 NAT 定义的上行链路的 Edge 和层路由器。
- vRealize Network Insight 支持带有范围的 SNAT 规则。但是，DNAT 必须是目标和转换的 IP 地址之间的一对一映射（通过 NSX-V 的奇偶校验）。

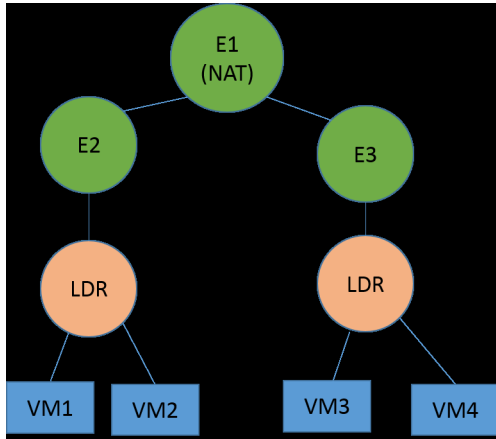
■ vRealize Network Insight 不支持以下用例：

- a 在 NSX-T 中，可以在服务级别上应用 NAT 规则。例如，在 NSX-T 中，L4 端口集是一种服务类型，关联的协议可以是 TCP 或 UDP。因此，在虚拟机-虚拟机路径中，不支持服务级别详细信息。
- b 不支持任何端口级别转换。
- c 不支持 SNAT 匹配目标地址和 DNAT 匹配源地址。指定 SNAT 规则时，使用 SNAT 匹配目标地址作为目标 IP 地址。指定 DNAT 规则时，使用 DNAT 匹配源地址作为源 IP 地址。例如，如果存在 SNAT 规则中提及的目标 IP 地址，则 vRealize Network Insight 会应用 SNAT 规则，而不考虑数据包是否将目标地址作为目标 IP 地址。

NAT 流支持 - 示例

此部分包含 vRealize Network Insight 中支持的 NAT 流的几个示例。

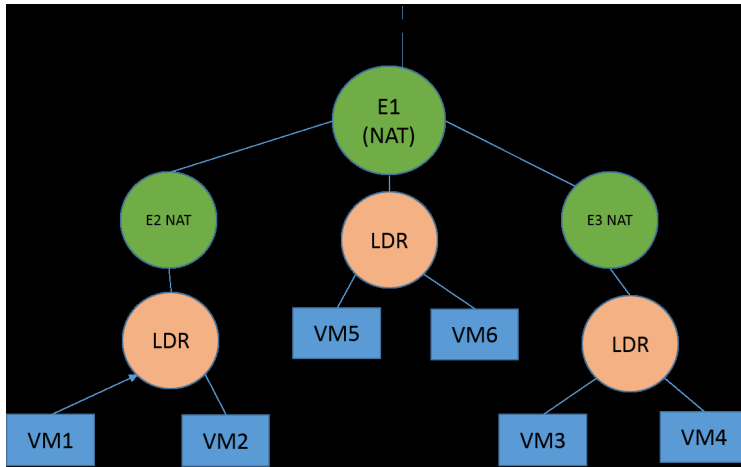
示例 1



在以上拓扑中，E2、E3、LDR、虚拟机（VM1、VM2、VM3、VM4）是 NAT 域 E1 的一部分。E1 之上的任何内容（如 E1 的上行链路）都是默认 NAT 域的一部分。以上拓扑包含以下内容：

在 vRealize Network Insight 中报告了从 VM1 到 VM2 的流以及从 VM2 到 VM1 的流。同样，也会报告从 VM3 到 VM4 的流以及从 VM4 到 VM3 的流。

示例 2



以上拓扑包含以下内容：

- VM1 和 VM2 是 E2 域的一部分。
- VM3 和 VM4 是 E2 域的一部分。
- E2 和 E3 NAT 域是 E1 NAT 域的子域。
- E1 是默认 NAT 域的单个子项。
- VM5 和 VM6 是 E1 NAT 域的一部分。

在以上拓扑中，以下流在 vRealize Network Insight 中报告：

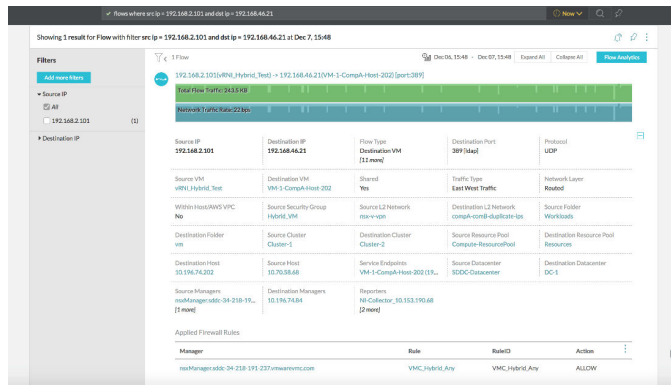
- 从 VM5 到 VM6 的流
- 从 (VM1, VM2) 到 (VM3, VM4) 的流

VMware Cloud on AWS 个流

如果在设置页面中的数据源上已启用 IPFIX，则可以查看流计数和上次收集时间。

可以搜索任何特定流，并获取与实体关联的详细信息。例如，可以分别在 Source L2 Network 和 Source Security Group 中查看策略分段和策略组信息。还可以查看附加到流的策略防火墙规则。

vRealize Network Insight 支持通过 VPN 的混合流。将使用源实体和目标实体扩充流信息。



创建 VPC 流日志

通过 Virtual Private Cloud (VPC) 流日志，您可以捕获有关进出 VPC 中网络接口的 IP 流量的信息。

您可以通过 **AWS 门户** 创建流日志。

步骤

- 1 登录到 **AWS 控制台**。
 - 2 在**查找服务** 文本框中， 输入并选择 **CloudWatch**。
 - 3 转到**日志 > 操作 > 创建日志组**。
- 此时将显示**创建日志组**窗口。
- 4 在**创建组名称**字段中， 输入一个组名称， 然后单击**创建日志组**。
 - 5 在顶部导航窗格中， 单击**服务**， 然后 输入并选择 **VPC**。
 - 6 在 **VPC 仪表板**页面中， 单击**您的 VPC**。
 - 7 选择要修改的 VPC， 然后单击**流日志 > 创建流日志**。
 - 8 在**创建流日志**窗口中， 配置流日志：

选项	操作
筛选器	选择以下选项之一： 接受 、 拒绝 或 全部 。
目标	选择 发送到 CloudWatch 日志 。
目标日志组	选择您创建的日志组。

- 9 单击**设置权限**。

系统将打开 **VPC 流日志请求使用您的帐户中资源的权限** 页面。
- 10 创建 IAM 角色。
 - a 在 **VPC 流日志请求使用您的帐户中资源的权限** 页面的 **IAM 角色** 中，选择**创建新 IAM 角色**。
 - b 在**角色名称**文本框中，输入角色名称。
 - a 单击**允许**。

11 在**创建流日志**页面的 **IAM 角色**下拉列表中，选择您创建的角色。

12 单击**创建**

结果

流日志将开始在选定的日志组中发布。有关 VPC 流日志的详细信息，请参见 AWS 文档 (<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html#create-flow-log>)。

将流记录从 F5 发送到 vRealize Network Insight 收集器

要发送流记录，您必须执行以下操作：

SI 编号	任务	链接
1	创建 IPFIX 收集器池，以便接收来自 BIG-IP 系统的 IPFIX 日志消息。	创建 IPFIX 收集器池
2	创建日志目标以设置 IPFIX 模板中日志的格式。	创建 IPFIX 日志目标
3	创建日志发布者以将日志发送到指定的日志目标。	创建日志发布者
4	创建一个 iRule 以将流信息发送到配置的 vRealize Network Insight 收集器。	创建 iRule
5	将 iRule 添加到虚拟服务器配置，以便 iRule 解析虚拟服务器的所有网络流量。	将 iRule 添加到虚拟服务器
6	如果无法从 F5 中访问收集器虚拟机，则必须创建一个路由条目，收集器才能发送流记录。	创建路由条目

创建 IPFIX 收集器池

创建 IPFIX 收集器池。BIG-IP 系统会将 IPFIX 日志消息发送到此池。

步骤

- 1 登录到 F5 控制台。
- 2 单击**主 > 本地流量 > 池 > 池列表 > 创建**。
此时将打开**新建池**屏幕。
- 3 在**名称**文本框中，输入池的唯一名称。
- 4 在**运行状况监控器**中，选择 **gateway_icmp**，然后将其移动到**活动**框中。

- 5 在**新建成员**部分中，配置收集器 IP 地址，然后单击**添加**。

选项	操作
节点名称	输入收集器 IP 地址。
服务端口	2055

- 6 单击**完成**。

后续步骤

创建 IPFIX 日志目标

创建日志目标以设置 IPFIX 模板中日志的格式。设置格式后，这些日志将发送到 IPFIX 收集器。

步骤

- 1 在 F5 控制台中，单击**主 > 系统 > 日志 > 配置 > 日志目标 > 创建**。

此时将显示**日志目标**屏幕。

- 2 在**名称**文本框中，输入唯一的名称。
- 3 在**类型**列表中，单击 **IPFIX**。
- 4 配置 **IPFIX** 设置。

选项	操作
协议	单击 Netflow V9 。
池名称	单击在上一步中创建的池名称。

- 5 单击**完成**。

创建日志发布者

要将日志发送到指定的日志目标，您需要创建一个日志发布者。

步骤

- 1 在 F5 控制台中，单击**主 > 系统 > 日志 > 配置 > 日志发布者 > 创建**。
- 此时将显示**日志发布者**屏幕。
- 2 在**名称**字段中，输入唯一的名称。
 - 3 在**目标**框中，从**可用**框中选择您之前创建的日志目标，然后将其移动到**选定**框中。
 - 4 单击**完成**。

创建 iRule

要将流信息发送到已配置的 vRealize Network Insight 收集器，必须创建 iRule。您必须创建两个 iRule。一个 iRule 用于 TCP 协议，另一个 iRule 用于 UDP 协议。

步骤

- 1 在 F5 控制台中，单击 **主 > iRule > iRule 列表 > 创建**。

此时将显示 **新建 iRule** 屏幕。

- 2 在 **名称** 文本框中，输入唯一的名称。
- 3 在 **定义** 文本框中，为 TCP 协议输入 TCP 规则，并为 UDP 协议输入 UDP 规则。有关角色的信息，请参见 [TCP 和 UDP 协议的 iRule](#)。

确保 iRule 指向之前创建的发布者。

- 4 单击 **完成**。

TCP 和 UDP 协议的 iRule

使用这些为 TCP 和 UDP 协议创建 iRule

TCP 规则

使用以下规则为 TCP 协议创建 iRule:

注 确保 iRule 指向之前创建的日志发布者。

```
when RULE_INIT {
    set static::http_rule1_dest ""
    set static::http_rule1_tmplt ""
}

# CLIENT_ACCEPTED event to initiate IPFIX destination and template
when CLIENT_ACCEPTED {
    set start [clock clicks -milliseconds]
    if { $static::http_rule1_dest == "" } {
        # open the logging destination if it has not been opened yet
        set static::http_rule1_dest [IPFIX::destination open -publisher /Common/<Log Publisher>]
    }
    if { $static::http_rule1_tmplt == "" } {
        # if the template has not been created yet, create the template
        set static::http_rule1_tmplt [IPFIX::template create "flowStartMilliseconds \
                                                                sourceIPv4Address \
                                                                sourceIPv6Address \
                                                                destinationIPv4Address \
                                                                destinationIPv6Address \
                                                                sourceTransportPort \
                                                                destinationTransportPort \
                                                                protocolIdentifier \
                                                                octetTotalCount \
                                                                packetTotalCount \
                                                                octetDeltaCount \
                                                                "
```

```

        packetDeltaCount \
        postNATSourceIPv4Address \
        postNATSourceIPv6Address \
        postNATDestinationIPv4Address \
        postNATDestinationIPv6Address \
        postNAPTSourceTransportPort \
        postNAPTDestinationTransportPort \
        postOctetTotalCount \
        postPacketTotalCount \
        postOctetDeltaCount \
        postPacketDeltaCount \
        flowEndMilliseconds"]
    }
}

# SERVER_CONNECTED event to initiate flow data to vrni and populate 5 tuples
when SERVER_CONNECTED {
    set rule1_msg1 [IPFIX::msg create $static::http_rule1_tmplt]
    set client_closed_flag 0
    set server_closed_flag 0
    IPFIX::msg set $rule1_msg1 flowStartMilliseconds $start
    IPFIX::msg set $rule1_msg1 protocolIdentifier [IP::protocol]

    # Clientside
    if { [clientside {IP::version}] equals "4" } {
        # Client IPv4 address
        IPFIX::msg set $rule1_msg1 sourceIPv4Address [IP::client_addr]
        # BIG-IP IPv4 VIP address
        IPFIX::msg set $rule1_msg1 destinationIPv4Address [clientside {IP::local_addr}]
    } else {
        # Client IPv6 address
        IPFIX::msg set $rule1_msg1 sourceIPv6Address [IP::client_addr]
        # BIG-IP IPv6 VIP address
        IPFIX::msg set $rule1_msg1 destinationIPv6Address [clientside {IP::local_addr}]
    }
    # Client port
    IPFIX::msg set $rule1_msg1 sourceTransportPort [TCP::client_port]
    # BIG-IP VIP port
    IPFIX::msg set $rule1_msg1 destinationTransportPort [clientside {TCP::local_port}]

    # Serverside
    if { [serverside {IP::version}] equals "4" } {
        # BIG-IP IPv4 self IP address
        IPFIX::msg set $rule1_msg1 postNATSourceIPv4Address [IP::local_addr]
        # Server IPv4 IP address
        IPFIX::msg set $rule1_msg1 postNATDestinationIPv4Address [IP::server_addr]
    } else {
        # BIG-IP IPv6 self IP address
        IPFIX::msg set $rule1_msg1 postNATSourceIPv6Address [IP::local_addr]
        # Server IPv6 IP address
        IPFIX::msg set $rule1_msg1 postNATDestinationIPv6Address [IP::server_addr]
    }
    # BIG-IP self IP port
    IPFIX::msg set $rule1_msg1 postNAPTSourceTransportPort [TCP::local_port]
    # Server port

```

```

    IPFIX::msg set $rule1_msg1 postNAPTDestinationTransportPort [TCP::server_port]
}

# SERVER_CLOSED event to collect IP pkts and bytes count on serverside
when SERVER_CLOSED {
    set server_closed_flag 1
    # when flow is completed, BIG-IP to server REQUEST pkts and bytes count
    IPFIX::msg set $rule1_msg1 octetTotalCount [IP::stats bytes out]
    IPFIX::msg set $rule1_msg1 packetTotalCount [IP::stats pkts out]
    # when flow is completed, server to BIG-IP RESPONSE pkts and bytes count
    IPFIX::msg set $rule1_msg1 octetDeltaCount [IP::stats bytes in]
    IPFIX::msg set $rule1_msg1 packetDeltaCount [IP::stats pkts in]
    if { $client_closed_flag == 1 } {
        # send the IPFIX log
        IPFIX::destination send $static::http_rule1_dest $rule1_msg1
    }
}

# CLIENT_CLOSED event to collect IP pkts and bytes count on clientside
when CLIENT_CLOSED {
    set client_closed_flag 1
    # when flow is completed, client to BIG-IP REQUEST pkts and bytes octetDeltaCount
    IPFIX::msg set $rule1_msg1 postOctetTotalCount [IP::stats bytes in]
    IPFIX::msg set $rule1_msg1 postPacketTotalCount [IP::stats pkts in]
    # when flow is completed, BIG-IP to client RESPONSE pkts and bytes count
    IPFIX::msg set $rule1_msg1 postOctetDeltaCount [IP::stats bytes out]
    IPFIX::msg set $rule1_msg1 postPacketDeltaCount [IP::stats pkts out]
    # record the client closed time in ms
    IPFIX::msg set $rule1_msg1 flowEndMilliseconds [clock click -milliseconds]
    if { $server_closed_flag == 1 } {
        # send the IPFIX log
        IPFIX::destination send $static::http_rule1_dest $rule1_msg1
    }
}

```

UDP 规则

使用以下规则为 UDP 协议创建 iRule:

注 确保 iRule 指向之前创建的日志发布者。

```

when RULE_INIT {
    set static::http_rule1_dest ""
    set static::http_rule1_tmplt ""
}

# CLIENT_ACCEPTED event to initiate IPFIX destination and template
when CLIENT_ACCEPTED {
    set start [clock clicks -milliseconds]
    if { $static::http_rule1_dest == "" } {
        # open the logging destination if it has not been opened yet
        set static::http_rule1_dest [IPFIX::destination open -publisher /Common/<Log Publisher>]
    }
    if { $static::http_rule1_tmplt == "" } {

```

```

# if the template has not been created yet, create the template
set static::http_rule1_tmplt [IPFIX::template create "flowStartMilliseconds \
                                                    sourceIPv4Address \
                                                    sourceIPv6Address \
                                                    destinationIPv4Address \
                                                    destinationIPv6Address \
                                                    sourceTransportPort \
                                                    destinationTransportPort \
                                                    protocolIdentifier \
                                                    octetTotalCount \
                                                    packetTotalCount \
                                                    octetDeltaCount \
                                                    packetDeltaCount \
                                                    postNATSourceIPv4Address \
                                                    postNATSourceIPv6Address \
                                                    postNATDestinationIPv4Address \
                                                    postNATDestinationIPv6Address \
                                                    postNAPTSourceTransportPort \
                                                    postNAPTDestinationTransportPort \
                                                    postOctetTotalCount \
                                                    postPacketTotalCount \
                                                    postOctetDeltaCount \
                                                    postPacketDeltaCount \
                                                    flowEndMilliseconds"]
}
}

# SERVER_CONNECTED event to initiate flow data to vrni and populate 5 tuples
when SERVER_CONNECTED {
  set rule1_msg1 [IPFIX::msg create $static::http_rule1_tmplt]
  set client_closed_flag 0
  set server_closed_flag 0
  IPFIX::msg set $rule1_msg1 flowStartMilliseconds $start
  IPFIX::msg set $rule1_msg1 protocolIdentifier [IP::protocol]

  # Clientside
  if { [clientside {IP::version}] equals "4" } {
    # Client IPv4 address
    IPFIX::msg set $rule1_msg1 sourceIPv4Address [IP::client_addr]
    # BIG-IP IPv4 VIP address
    IPFIX::msg set $rule1_msg1 destinationIPv4Address [clientside {IP::local_addr}]
  } else {
    # Client IPv6 address
    IPFIX::msg set $rule1_msg1 sourceIPv6Address [IP::client_addr]
    # BIG-IP IPv6 VIP address
    IPFIX::msg set $rule1_msg1 destinationIPv6Address [clientside {IP::local_addr}]
  }
  # Client port
  IPFIX::msg set $rule1_msg1 sourceTransportPort [UDP::client_port]
  # BIG-IP VIP port
  IPFIX::msg set $rule1_msg1 destinationTransportPort [clientside {UDP::local_port}]

  # Serverside
  if { [serverside {IP::version}] equals "4" } {
    # BIG-IP IPv4 self IP address

```

```

    IPFIX::msg set $rule1_msg1 postNATSourceIPv4Address [IP::local_addr]
    # Server IPv4 IP address
    IPFIX::msg set $rule1_msg1 postNATDestinationIPv4Address [IP::server_addr]
} else {
    # BIG-IP IPv6 self IP address
    IPFIX::msg set $rule1_msg1 postNATSourceIPv6Address [IP::local_addr]
    # Server IPv6 IP address
    IPFIX::msg set $rule1_msg1 postNATDestinationIPv6Address [IP::server_addr]
}
# BIG-IP self IP port
IPFIX::msg set $rule1_msg1 postNAPTSourceTransportPort [UDP::local_port]
# Server port
IPFIX::msg set $rule1_msg1 postNAPTDestinationTransportPort [UDP::server_port]
}

# SERVER_CLOSED event to collect IP pkts and bytes count on serverside
when SERVER_CLOSED {
    set server_closed_flag 1
    # when flow is completed, BIG-IP to server REQUEST pkts and bytes count
    IPFIX::msg set $rule1_msg1 octetTotalCount [IP::stats bytes out]
    IPFIX::msg set $rule1_msg1 packetTotalCount [IP::stats pkts out]
    # when flow is completed, server to BIG-IP RESPONSE pkts and bytes count
    IPFIX::msg set $rule1_msg1 octetDeltaCount [IP::stats bytes in]
    IPFIX::msg set $rule1_msg1 packetDeltaCount [IP::stats pkts in]
    if { $client_closed_flag == 1 } {
        # send the IPFIX log
        IPFIX::destination send $static::http_rule1_dest $rule1_msg1
    }
}

# CLIENT_CLOSED event to collect IP pkts and bytes count on clientside
when CLIENT_CLOSED {
    set client_closed_flag 1
    # when flow is completed, client to BIG-IP REQUEST pkts and bytes count
    IPFIX::msg set $rule1_msg1 postOctetTotalCount [IP::stats bytes in]
    IPFIX::msg set $rule1_msg1 postPacketTotalCount [IP::stats pkts in]
    # when flow is completed, BIG-IP to client RESPONSE pkts and bytes count
    IPFIX::msg set $rule1_msg1 postOctetDeltaCount [IP::stats bytes out]
    IPFIX::msg set $rule1_msg1 postPacketDeltaCount [IP::stats pkts out]
    # record the client closed time in ms
    IPFIX::msg set $rule1_msg1 flowEndMilliseconds [clock click -milliseconds]
    if { $server_closed_flag == 1 } {
        # send the IPFIX log
        IPFIX::destination send $static::http_rule1_dest $rule1_msg1
    }
}

```

将 iRule 添加到虚拟服务器

步骤

- 1 在 F5 控制台中，单击 **主 > 虚拟服务器 > 虚拟服务器列表**。

此时将显示 **虚拟服务器列表** 屏幕。

- 2 选择要添加 iRule 的服务器。
- 3 单击**资源**选项卡，然后在 iRule 部分中单击**管理**。
- 4 选择您之前创建的 TCP iRule 和 UDP iRule，并将这些 iRule 从**可用**框移动到**启用**框。
- 5 单击**完成**。

创建路由条目

收集器虚拟机必须可从 F5 访问。如果从 F5 无法访问收集器虚拟机，则必须为该收集器创建一个路由条目。

要检查是否可从 F5 访问收集器虚拟机，必须从命令行界面 (CLI) 运行以下命令：`ping <collector-ip> -I <virtual interface>`。如果从 F5 无法访问收集器，则必须为该收集器创建一个路由条目。

例如，

```
admin@(localhost) (cfg-sync Standalone) (Active) (/Common) (tmsh)# ping 10.153.191.116 -I VLAN301
PING 10.153.191.116 (10.153.191.116) from 10.115.30.50 VLAN301: 56(84) bytes of data.
From 10.115.30.50 icmp_seq=1 Destination Host Unreachable
From 10.115.30.50 icmp_seq=2 Destination Host Unreachable
```

步骤

- 1 在 F5 控制台中，单击**主 > 网络 > 路由 > 添加**。
此时将显示**新建路由**屏幕。
- 2 在**属性**部分中，配置路由条目以通过虚拟服务器将流记录从 F5 发送到 vRealize Network Insight 收集器。

Kubernetes 和 VMware PKS 范围和流信息

14

您可以设定容器实体的范围并查看 vRealize Network Insight 中的流信息。

VMware PKS 和 Kubernetes 流信息

vRealize Network Insight 支持 Kubernetes 实体的以下流类型。

- 虚拟机到 Kubernetes Pod
- Kubernetes Pod 到 Pod
- 目标为 Kubernetes Pod
- 源为 Kubernetes Pod

您可以使用这些流类型搜索特定的 Kubernetes 实体。

例如，`flows where flow type = x`，其中 *x* 是一种流类型

vRealize Network Insight 可以为所有实体提供流信息，例如衡量指标、时间系列和关系，其中包括容器源和目标详细信息及其实体详细信息。

此外，您可以在“流分析”仪表板上按 Kubernetes 群集、命名空间、服务和节点查看通信最多者。

Kubernetes 实体规划和微分段

您可以通过在“规划安全性”页面中选择 Kubernetes 群集、Kubernetes 服务、Kubernetes 命名空间或 Kubernetes 节点作为范围和微分段来规划特定的 Kubernetes 实体类型。此外，您还可以规划或分析应用程序的数据，并根据 Kubernetes 实体定义分组以查看应用程序流信息。

此外，您还可以从“规划安全性”页面的微分段中以 YAML 格式导出与 Kubernetes 实体相关的建议防火墙规则。

注 如果应用程序范围包含虚拟机或虚拟机成员，则无法以 YAML 格式导出该应用程序范围。如果应用程序仅包含容器实体，则可以导出为 YAML 格式。

vRealize Network Insight 提供了实施微分段安全的规划和建议。它有助于用户快速而自信地管理和扩展 VMware NSX 部署。

本章讨论了以下主题：

- 分析应用程序
- 应用程序发现
- VMware Cloud on AWS：规划和微分段

分析应用程序

微分段规划拓扑通过将流分为多个分段，显示环境中存在的所有流。

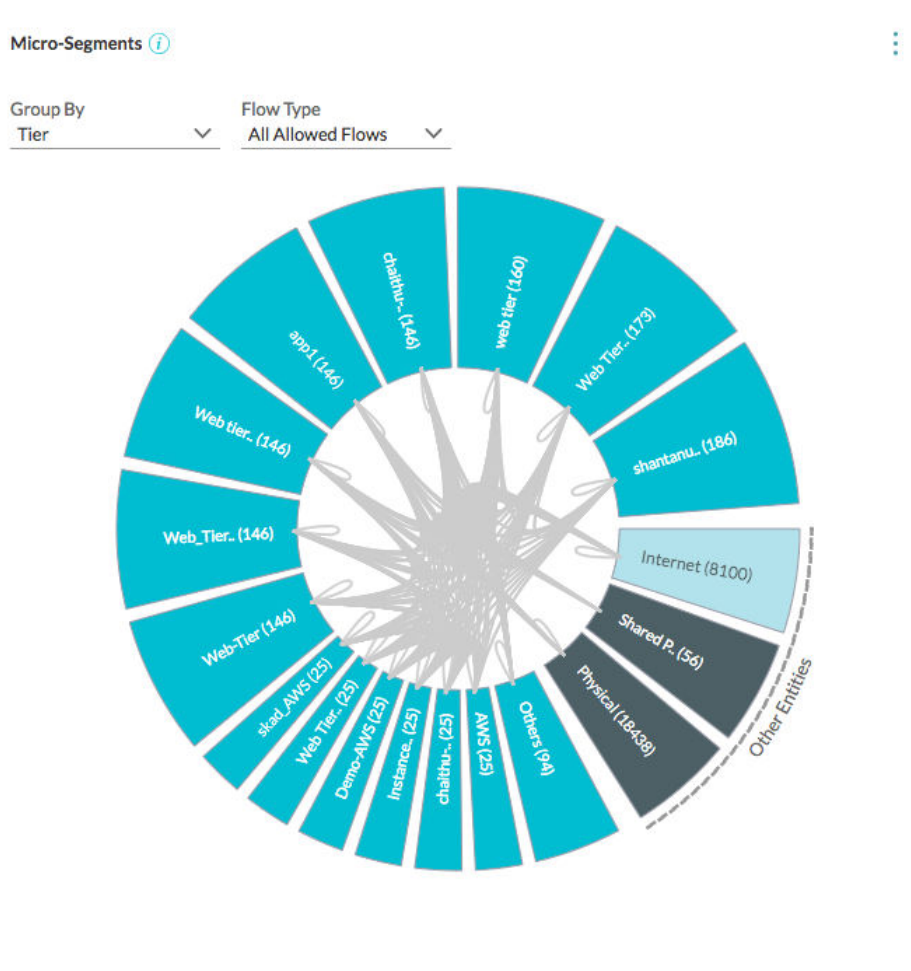
在 vRealize Network Insight 中，流是一个 4 元组。它包括：

- 源 IP
- 目标 IP
- 目标端口
- 协议

您可以采用两种格式查看数据：环形视图和网格视图

在环形视图中查看微分段和流数据

在环形视图中，蓝线表示出站流，绿线表示进站流，黄线表示双向流。可以单击任一分段以查看其详细信息。

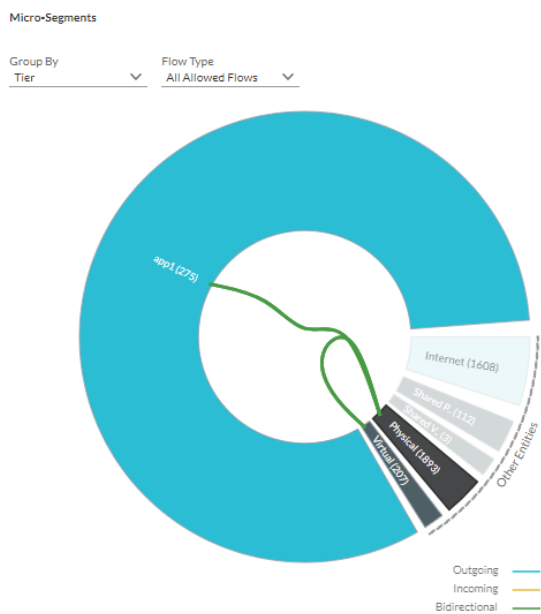


选定范围之外的虚拟机在微分段规划拓扑中分组为**其他实体**。

您也可以通过按物理、其他虚拟和 Internet 类别创建子组来分析流。

Group By	Also show groups for
VLAN/VXLAN	All
Application	Physical
✓ Tier	Virtual
Subnet	Internet
Folder	✓ None
Cluster	
VM	
Port	
Security Tag	
Security Group	
IPSet	
VPC	

每个组都展开成一个楔形。在以下拓扑中，可看到表示**物理组**的楔形。



“流”插针显示不同时间间隔的流（按端口分开）。可以查看所有流，也可以查看两个实体之间的流。可以按“已允许的流”和“已阻止的流”筛选流。可以按“总字节数”或“允许的会话计数”查看流。对于受防火墙保护的流，使用“受防火墙保护”符号表示该端口中的流受防火墙保护。

规划整个数据中心或群集等范围时，会选择具有虚拟机或物理服务器（由物理 IP 标识）作为源或目标的流。

一个拓扑包含两个不同的区域：

- **内部：**此区域包括范围内的虚拟机或 IP 地址。
- **外部：**此区域包括在范围之外但与内部区域中的虚拟机或 IP 地址通信的虚拟机或 IP 地址。外部区域由以下楔形组成：
 - **DC 虚拟：**包括源或目标数据中心内部虚拟机，这些虚拟机与内部区域中的虚拟机或 IP 地址进行通信，但不托管任何熟知的共享服务（如 LDAP、NTP 等）。
 - **共享虚拟：**包括目标数据中心内部虚拟机，这些虚拟机托管熟知的共享服务（如 LDAP、NTP 等）并与内部区域中的虚拟机或 IP 地址进行通信。
 - **DC 物理：**包括源或目标数据中心内部物理 IP 地址，这些地址与内部区域中的虚拟机或 IP 地址进行通信，但不托管任何熟知的共享服务（如 LDAP、NTP 等）。
 - **共享物理：**包括目标数据中心内部物理 IP 地址，这些地址托管熟知的共享服务（如 LDAP、NTP 等）并与内部区域中的虚拟机或 IP 地址进行通信。
 - **Internet：**包括与内部区域中的虚拟机或 IP 地址通信的源或目标数据中心外部虚拟机或物理 IP 地址。

注

- 数据中心内部隐含 RFC 1918 默认指定的 IP + 在 E-W 设置中定义的任何替代项。
- 数据中心外部隐含非 RFC 1918 默认指定的 IP + 在 N-S 设置中定义的任何替代项。

在网格视图中查看微分段和流数据

通过 vRealize Network Insight，您可以在表格或网格视图中查看对象之间的通信。

步骤

- 1 导航到 **安全性 > 规划安全性**，然后单击网格视图  图标。
- 2 针对**分组依据**选项选择一个值（例如**虚拟机**、**应用程序**、**安全组**），以表格格式查看相应的详细信息。

字段名称	描述
源对象	源的名称
目标对象	目标的名称
相关流	源和目标之间的通信或流计数 单击计数值可查看相关的流详细信息。
字节总数	所有流之间的汇总字节数

字段名称	描述
最大流速	所有相关流中观察到的最大流速
会话计数	特定流的活动会话数

注

- 您可以单击每个列标题以按升序或降序对数据进行排序。
- 您可以在表视图中隐藏该字段，单击字段标题旁边的更多图标，然后取消选择字段名称。

3 此外，您可以在网格视图页面上执行多个操作。

- 在屏幕左侧的“筛选器”窗格中，您可以执行以下操作：
 - 选择单个源或目标以筛选与所选源或目标对象相关的流。
 - 选择防火墙操作以查看允许的流或丢弃的流。
 - 选择保护状态以查看流状态。
- 单击**添加更多筛选器**以添加其他筛选器。
- 要以 CSV 格式导出表格数据，请单击表顶部的更多选项，然后选择**导出为 CSV**。

手动创建应用程序

您可以在 vRealize Network Insight 用户界面中手动创建应用程序。

步骤

- 1 在 vRealize Network Insight 主页上，单击**安全性 > 应用程序**。
- 2 在**保存的应用程序**选项卡上，单击**添加应用程序**。
- 3 在**添加应用程序**页面的**应用程序名称**文本框中，输入要创建的应用程序的名称。
- 4 在**层/部署**部分中，输入唯一的名称。

您可以根据要求为虚拟机、物理机或服务创建层/部门。

5 在**成员**字段中，

- a 从下拉菜单中选择一个条件以创建层。

您可以根据虚拟机属性、虚拟机位置（应用程序、群集、文件夹）以及根据 Kubernetes 服务（服务名称、群集 IP 地址、命名空间、群集 IP 或服务标签）定义条件。

要在多个群集中搜索具有相同名称、相同 IP 或相同标记的特定 Kubernetes 服务，请使用自定义搜索。

- b 输入或选择要添加到层的值。

要输入多个值，请在每个值后面使用逗号隔开。

要添加服务作为层的一部分，选择**服务名称**，然后在值中输入名称。

根据定义的条件，您会看到关联的或相关的虚拟机计数或者物理 IP 计数或者服务计数。

6 要添加任何其他条件，单击**添加其他条件**。

7 （可选）要在一个应用程序下创建另一个层，单击**添加层/部署**。

您可以在一个应用程序下创建多个层。

应用程序会创建所有层，并显示与所有条件匹配的虚拟机计数、物理 IP 计数和服务计数。

8 （可选）要创建动态阈值配置，选中**启用阈值分析**复选框。

系统会在**阈值配置**页面中创建阈值配置。vRealize Network Insight 创建了以 sys 前缀开头的阈值配置名称。

注 您无法删除系统生成的阈值配置。当删除应用程序或清除**启用阈值分析**复选框并保存应用程序时，会自动删除系统生成的与该应用程序相关的阈值配置。

注 如果在应用程序中添加成员并选中**启用阈值分析**复选框，可能需要约 20 分钟才能在阈值配置页面中反映该成员。

9 选择“分析流”以在最终添加应用程序之前查看流。您可以相应地查看基于虚拟机或物理地址的层。

10 单击**保存**。

注 如果您的应用程序没有任何 VMware 虚拟机，并且选中**启用阈值分析**复选框，则无法保存该应用程序。您必须添加 VMware 虚拟机或清除**启用阈值分析**复选框，才能保存您的应用程序。

11 （可选）要预览流分析，单击**预览流**。

此时将显示应用程序的微分段视图。

后续步骤

您可以在**保存的应用程序**下查看应用程序详细信息。

为物理 IP 创建层

创建应用程序时，可以从下拉列表中选择**自定义 IP 搜索**，以便基于扩充的字段为物理 IP 创建层。有关扩充的字段的详细信息，请参阅[扩充流和 IP 端点](#)。

在指定层时，可以使用扩充的 DNS、子网、VLAN 信息，如下所示：

■ Web

Query: IP Endpoint where Subnet Network = '172.16.101.0/24'

■ 应用程序

Query: IP Endpoint where Dns Domain = app.example.com

■ 数据库

Query: IP Endpoint where L2 Network = 'vlan-102'

■ 常见服务

Query: IP Endpoint where Dns Domain = svc.example.com

应用程序发现

当您有多个应用程序或在一个应用程序中有多个层时，使用公共 API 或用户界面创建应用程序将成为一个漫长的过程。vRealize Network Insight 会自动发现应用程序，并使您能够自动访问应用程序及其层，从而减少了大量手动工作。

vRealize Network Insight 可以基于以下内容执行应用程序发现：

- 标记（vCenter Server 或 AWS 标记）
- 虚拟机名称
- 添加 [ServiceNow](#)

示例：应用程序发现构造示例

假设：

- 您已将 vCenter Server 添加为数据源
- 您的数据中心有四个虚拟机 - VM1、VM2、VM3 和 VM4。
- 您已定义标记（键-值），用于定义每个虚拟机所属的应用程序名称
- 您已定义标记（键-值），用于定义每个虚拟机所属的层

例如，请参见下表：

虚拟机名称	键-值标记
VM1	<ul style="list-style-type: none"> ■ 应用程序名称: MyApplication1 ■ 应用程序层: App
VM2	<ul style="list-style-type: none"> ■ 应用程序名称: MyApplication1 ■ 应用程序层: Web
VM3	<ul style="list-style-type: none"> ■ 应用程序名称: MyApplication2 ■ 应用程序层: App
VM4	<ul style="list-style-type: none"> ■ 应用程序名称: MyApplication2 ■ 应用程序层: Web

基于标记发现应用程序

在 vRealize Network Insight 中，您可以为这些标记定义应用程序发现的分组条件。

在此示例中，vRealize Network Insight 根据定义的标记和分组条件发现了两个应用程序（MyApplication1 和 MyApplication2），它们具有两层（App 和 Web）及其相关的虚拟机。

应用程序	层及其虚拟机
MyApplication1	<ul style="list-style-type: none"> ■ App 和 VM1 ■ Web 和 VM2
MyApplication2	<ul style="list-style-type: none"> ■ App 和 VM3 ■ Web 和 VM4

基于虚拟机名称创建应用程序和层

假设虚拟机名称采用以下特定格式定义：ApplicationName : Tier : VMName

```
MyApplication1 : App : VM1
MyApplication1 : Web : VM2
MyApplication2 : App : VM3
MyApplication2 : Web : VM4
```

注 无法对随机定义的虚拟机名称进行分组以用于应用程序发现。

使用以下正则表达式时，vRealize Network Insight 发现两个应用程序。

- 应用程序正则表达式： `(.*)_(.*)_.*-.*`
- 层正则表达式： `(.*)_(.*)_(.*)-.*`

应用程序	层及其虚拟机
MyApplication1	<ul style="list-style-type: none"> ■ App 和 MyApplication1: App : VM1 ■ Web 和 MyApplication1: Web : VM2
MyApplication2	<ul style="list-style-type: none"> ■ App 和 MyApplication2: App : VM3 ■ Web 和 MyApplication2: Web : VM4

添加已发现的应用程序

您可以发现现有的应用程序并将其添加到 vRealize Network Insight 中。

步骤

- 1 在搜索框中，使用 **applications** 字符串进行搜索。
- 2 单击**已发现的应用程序**选项卡。

您会看到以下选项卡可添加应用程序，即**标记**、**ServiceNow**、**名称**。

3 选择首选选项卡，然后执行相关步骤。

选项卡	描述
标记	<p>a 定义范围。</p> <ul style="list-style-type: none"> ■ 选择所有虚拟机以查看 vRealize Network Insight 中添加的所有数据源中的所有虚拟机的列表，或者 ■ 选择手动选择，并根据您的要求（例如帐户、数据中心、管理等）筛选虚拟机。 <p>b 定义标记的键和值。</p> <ul style="list-style-type: none"> ■ 输入标记的键。例如 <i>Automation</i>、<i>Category</i>、<i>CreatedBy</i> 和 <i>Owner</i>。 ■ （可选）输入相应键的值。 <p>c 单击未分类的虚拟机以查看未遵循特定名称模式或标记模式的虚拟机的列表。您可以编辑虚拟机以修复名称或标记条件。</p> <p>d 单击保存更改至以创建新模板或更新现有模板。</p> <p>注 如果您是管理员用户，则可以更新所有模板；如果您是成员用户，则只能编辑您创建的模板。</p> <p>e 单击发现。</p>
ServiceNow	您可以查看 ServiceNow 中可用的应用程序。
名称	<p>a 定义范围。</p> <ul style="list-style-type: none"> ■ 选择所有虚拟机以查看 vRealize Network Insight 中添加的所有数据源中的所有虚拟机的列表，或者 ■ 选择手动选择，并根据您的要求（例如帐户、数据中心、管理等）筛选虚拟机。 <p>b 单击模式生成器。</p> <p>根据您定义的范围，vRealize Network Insight 将筛选模式生成器中的虚拟机列表。</p> <ol style="list-style-type: none"> 1 选择默认虚拟机名称，或从列表中选择一个虚拟机，以便基于虚拟机名称生成模式或正则表达式 (regex)。 2 单击某个位置或组以构造模式。 <p>注 选择组后，如果选择字符或位置，则 vRealize Network Insight 会忽略用于生成模式的组选择，反之亦然。</p> <p>根据您的选择，您会看到屏幕上显示的模式。此外，还会看到与相应应用程序中的模式和虚拟机计数匹配的应用程序的列表。</p> <p>3 单击提交。</p> <p>c 单击找到 count 个应用程序链接，以查看应用程序名称列表以及与正则表达式匹配的虚拟机数量</p> <p>d 单击未分类的虚拟机以查看未遵循特定名称模式的虚拟机的列表。</p> <p>e 单击保存更改至以创建新模板或更新现有模板。</p> <p>注 如果您是管理员用户，则可以更新所有模板；如果您是成员用户，则只能编辑您创建的模板。</p> <p>f 单击发现。</p>

您将看到符合条件的所有应用程序的表格视图和六边形映射视图。

在映射视图中，每个六边形表示一个应用程序。您可以将鼠标悬停在六边形上以查看应用程序名称、已发现的虚拟机计数和层计数等信息。应用程序和 **Internet** 之间的直线表示连接。您可以单击这些直线以查看流详细信息，例如源流和目标流的计数，以及不受保护的源流和不受保护的目标流的计数。六边形上的问号表示 vRealize Network Insight 无法找到或提取应用程序的任何流详细信息，这可能是由于应用程序已超出流限制或存在不受保护的流。

在表格视图中，您会看到应用程序详细信息，其中包括应用程序名称、未到达目标并且由于拒绝防火墙操作而被丢弃的流计数，以及层和成员的计数。

映射视图和表格视图是交互式的。在表格视图中单击应用程序时，相应的六边形将在映射视图中处于突出显示或聚焦状态，并显示所有网络连接。

4 （可选）在映射视图中执行以下任一操作：

- 放大和缩小或移动映射以查看应用程序。
- 筛选您可以在拓扑中看到的六边形的数量（例如，前 10 项、前 20 项、前 50 项和前 100 项，以及基于层、名称和成员进行筛选）。
计数越大，六边形的颜色越深。
- 查看所有不受保护的应用程序。
- 查看连接到 **Internet** 的应用程序。
- 查看使用主机共享服务的所有应用程序。
- 查看存在问题的应用程序。

5 （可选）在表格视图中执行以下任一操作：

- 单击列标题以按升序或降序对值进行排序。
- 将鼠标悬停在成员列中的值上，以查看虚拟机、物理 IP 和服务的单独计数。
- 单击应用程序名称以打开应用程序仪表板，并查看该特定应用程序的详细信息。
- 单击表格视图中的 **+** 图标，以展开应用程序详细信息，例如条件以及虚拟机和层计数。

注 该图标仅适用于已发现的应用程序。

6 要保存已发现的应用程序：

- 在映射视图中，将鼠标悬停在六边形上，然后单击**保存应用程序**，或者
- 在表格视图中，单击**保存应用程序**。

注 您可以通过选中表中的多个应用程序复选框并单击**保存应用程序**，来批量保存应用程序。

7 验证“添加应用程序”页面上的详细信息，然后单击提交。

保存后，您会在应用程序六边形悬停列表中看到 `application:Saved`，并会在表格视图中看到应用程序对应的对勾标记。如果应用程序已保存，则可以将鼠标悬停在对勾标记上，然后单击另存为以使用其他名称保存应用程序。

注 如果在 ServiceNow 中修改了应用程序，则不会在 vRealize Network Insight 中进行自动更新。您必须在 vRealize Network Insight 中手动更新应用程序。

表 15-1. 限制

对象	最大限制	建议限制 (基于 5 节点 EXTRA LARGE 平台群集设置)
映射视图中的应用程序列表	3000 个应用程序	不适用
表格视图中的应用程序列表	不适用 (分页)	不适用
保存的应用程序	5K	400
所有应用程序的总层数	20K	3500
每个应用程序的层数	150	20
每层成员数	不适用	不适用
每个应用程序的成员数	5K	1.8K 如果应用程序超出限制，则可能无法在“应用程序拓扑”看板中看到流信息，或者看到一条错误消息。
每个应用程序的流数	500K	300K

如果您的设置超出层数和应用程序数的建议限制，您仍可以继续添加对象，直到达到最大限制，但性能可能会降低。

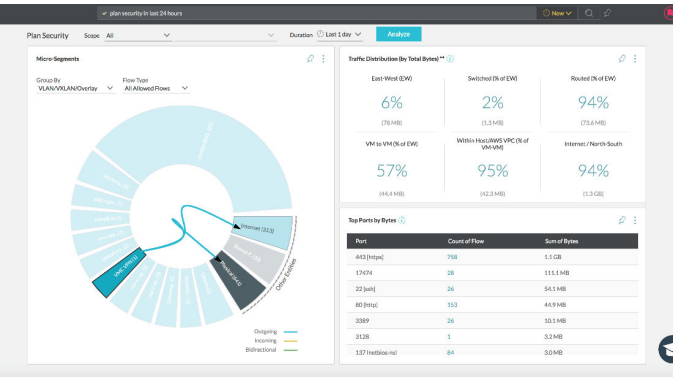
后续步骤

单击**导出为 CSV**以采用 .csv 格式导出应用程序详细信息。您可以定义要导出的应用程序计数和字段。应用程序名称和层名称字段将根据成员计数（每个成员一行）重复。仅填充与应用程序相关的字段，将其余字段留空。

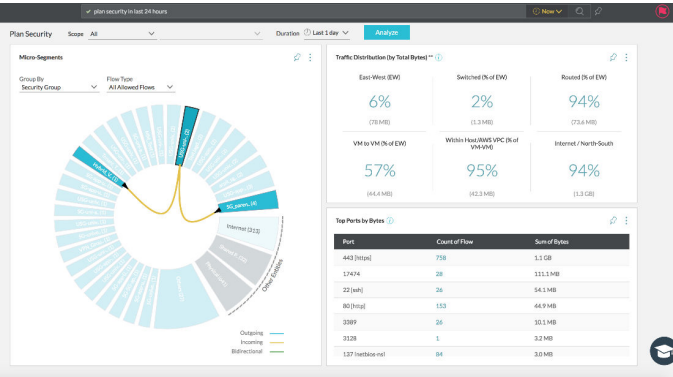
VMware Cloud on AWS：规划和微分段

您可以通过选择 **VMC 分段**作为**规划安全性**页面中的范围来规划特定的 VMware Cloud on AWS 分段。

对于策略分段，请使用组中的 VLAN/VXLAN/Overlay 子句。



对于策略组，请使用组中的 Security Group 子句。

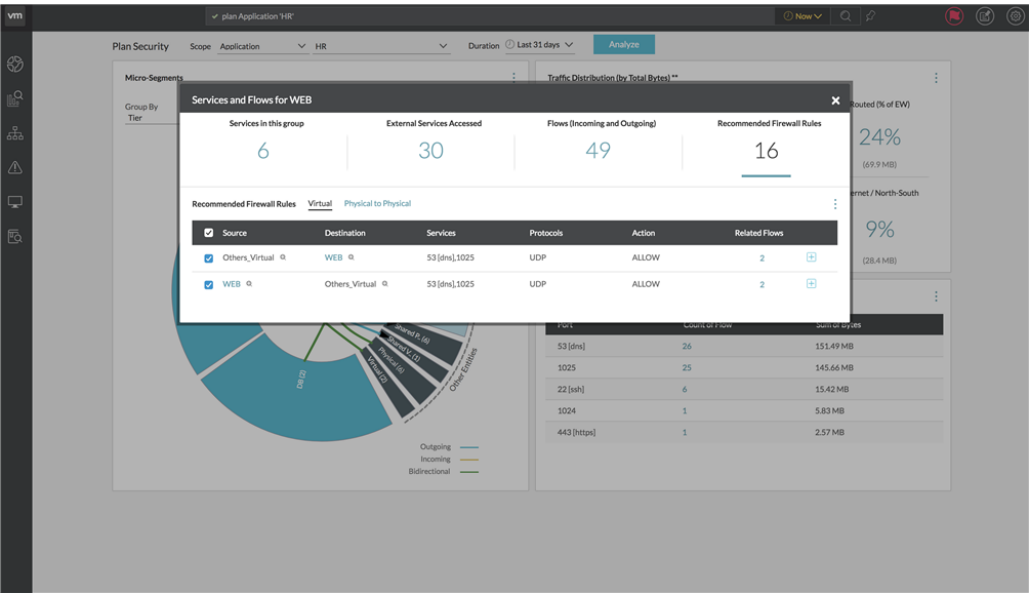


建议的防火墙规则

16

在规划安全性页面上，单击拓扑图中的楔形或 Edge 时，可以查看该特定分段的服务和流列表。单击**建议**的防火墙规则以查看在其上定义的规则。源或目标的成员在以下规则类型下列出：

- 物理到物理：此选项卡列出与物理和 Internet IP 关联的所有规则。这些规则可用于物理-物理、物理-Internet、Internet-物理或 Internet-Internet 实体。
- 虚拟：此选项卡列出至少一个端点为虚拟机的所有规则。



对于每个防火墙规则，以下详细信息可用：

- 显示组的成员：单击实体名称旁边的 + 符号可查看组的成员。

Services and Flows for integration.tier2				External Services Accessed		Flows (Incoming and Outgoing)		Recommended Firewall Rules	
7				22		32		7	
Recommended Firewall Rules									
Virtual Physical to Physical									
Source	Destination	Services	Protocols	Action	Related Flows				
integration.tier2	integration.tier1	53 [dns], 1025	UDP	ALLOW	2				
integration.tier1	integration.tier2	53 [dns], 1025	UDP	ALLOW	2				
integration.tier1	integration.tier2	22 [ssh]	TCP	ALLOW	2				

注

- 不显示属于 Internet 类别的组的成员。
 - 如果安全组同时具有虚拟和物理 IP，则在该特定组的成员列表中不显示物理和 Internet IP。
 - 成员 Kubernetes 服务显示在 **Kubernetes 服务** 选项卡下。
 - 如果虚拟机、物理和 Internet IP 或 Kubernetes 服务的成员计数或条目为零，则该选项卡不可见。
- 源
 - 目标
 - 服务
 - 协议
 - 操作
 - 相关流：单击相关流的编号可查看具有对应流信息的流的列表。
 - 查看应用的防火墙规则：单击相关流旁边的 + 符号可查看与类似流集相对应的已应用防火墙规则。

Services and Flows for integration.tier2						External Services Accessed		Flows (Incoming and Outgoing)		Recommended Firewall Rules	
7						22		32		7	
Recommended Firewall Rules											
Virtual Physical to Physical											
Source	Destination	Services	Protocols	Action	Related Flows						
integration.tier2	integration.tier1	53 [dns], 1025	UDP	ALLOW	2						
integration.tier1	integration.tier2	53 [dns], 1025	UDP	ALLOW	2						
integration.tier1	integration.tier2	22 [ssh]	TCP	ALLOW	2						

可以根据您的要求将建议的规则导出为 XML 或 CSV。

注 您也可以采用 YAML 格式导出与 Kubernetes 对象相关的建议规则。

有关这些项目的详细信息，请参阅[导出规则](#)。

建议的防火墙规则用于保护易受攻击的操作系统

使用以下过程获取建议的防火墙规则以保护易受攻击的操作系统：

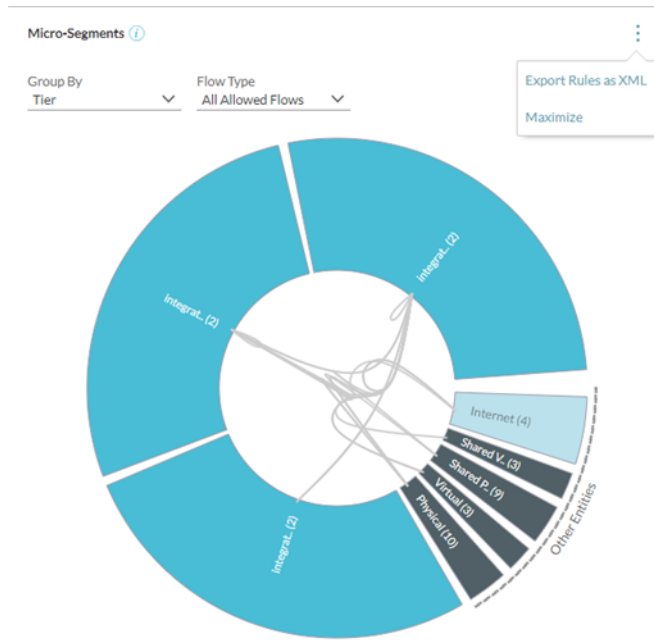
- 1 转到[安全性 > 应用程序 > 创建应用程序](#)。
- 2 输入应用程序和层/部署的名称。
- 3 在[成员](#)下拉框中，选择[自定义虚拟机搜索](#)，在文本框中添加
`in the qualifier put the matching criteria as: Operating System like 'Microsoft Windows Server 2003' or Operating System like 'Microsoft Windows Server 2008' or Operating System like 'Red Hat Enterprise Linux 6' or Operating System like 'Red Hat Enterprise Linux 5' or Operating System like 'SUSE Linux Enterprise 10'` 条件。
- 4 单击[保存](#)。
- 5 转到[安全性 > 规划安全性](#)。
- 6 在[范围](#)下拉列表中，选择[应用程序](#)以及您创建的应用程序的名称。
- 7 在[持续时间](#)下拉列表中，选择[过去 7 天](#)。
- 8 要获取建议的防火墙规则，请单击[分析](#)

本章讨论了以下主题：

- [导出规则](#)
- [导出并应用 Kubernetes 网络策略](#)

导出规则

可以将所有规则导出为整个拓扑的 XML。可以在[微分段规划](#)页面中找到此菜单项，如下所示：



“导出为 XML” 选项仅适用于以下实体：

- 安全组
- 应用程序层

如果规划范围仅涉及单个 NSX Manager，则生成的项目将包含与建议的服务和防火墙规则相对应的 XML 文件。如果规划范围涉及多个 NSX Manager，则生成的项目将包含与建议的服务、IPset、安全组和防火墙规则相对应的 XML 文件。

以下是安全组的占位符项目：

- SG-Others_Internet.xml
- SG-Other.xml

对于拓扑图中描绘的特定楔形或 Edge，可以将所有规则导出为 XML 或 CSV。

注 您也可以采用 YAML 格式导出与 Kubernetes 对象相关的建议规则。

NSX DFW 通用项目

可以很轻松地跨各种 vCenter 和 NSX 部署管理通用安全组中的对象。vRealize Network Insight 仅支持生成和导入应用程序和层组的通用项目。使用通用安全组，在跨 vCenter 场景中轻松部署和管理防火墙规则会变得非常容易。请确保在主 NSX Manager 上导入通用项目。您只能通过主 NSX Manager 管理通用安全组的成员资格。

一个通用安全组可以包含：

- 其他通用组
- 通用 IP 集
- 通用安全标记

将规则导出为 XML 时，除了 NSX Manager 特定文件夹外，还会创建一个通用文件夹，其中包含 NSX DFW 通用项目。导入 NSX DFW 通用项目后，将创建相应的通用安全组、通用 IP 集、通用安全标记和通用 DFW 防火墙规则。

注

- 通用安全标记仅在主动-备用模式下受支持。
- 通用 IP 集在主动-主动模式和主动-备用模式下均受支持。

可以根据要求创建通用 IP 集或通用安全标记。如果创建通用安全标记，则可以将应用程序虚拟机映射到安全标记。否则，使用通用 IP 集。

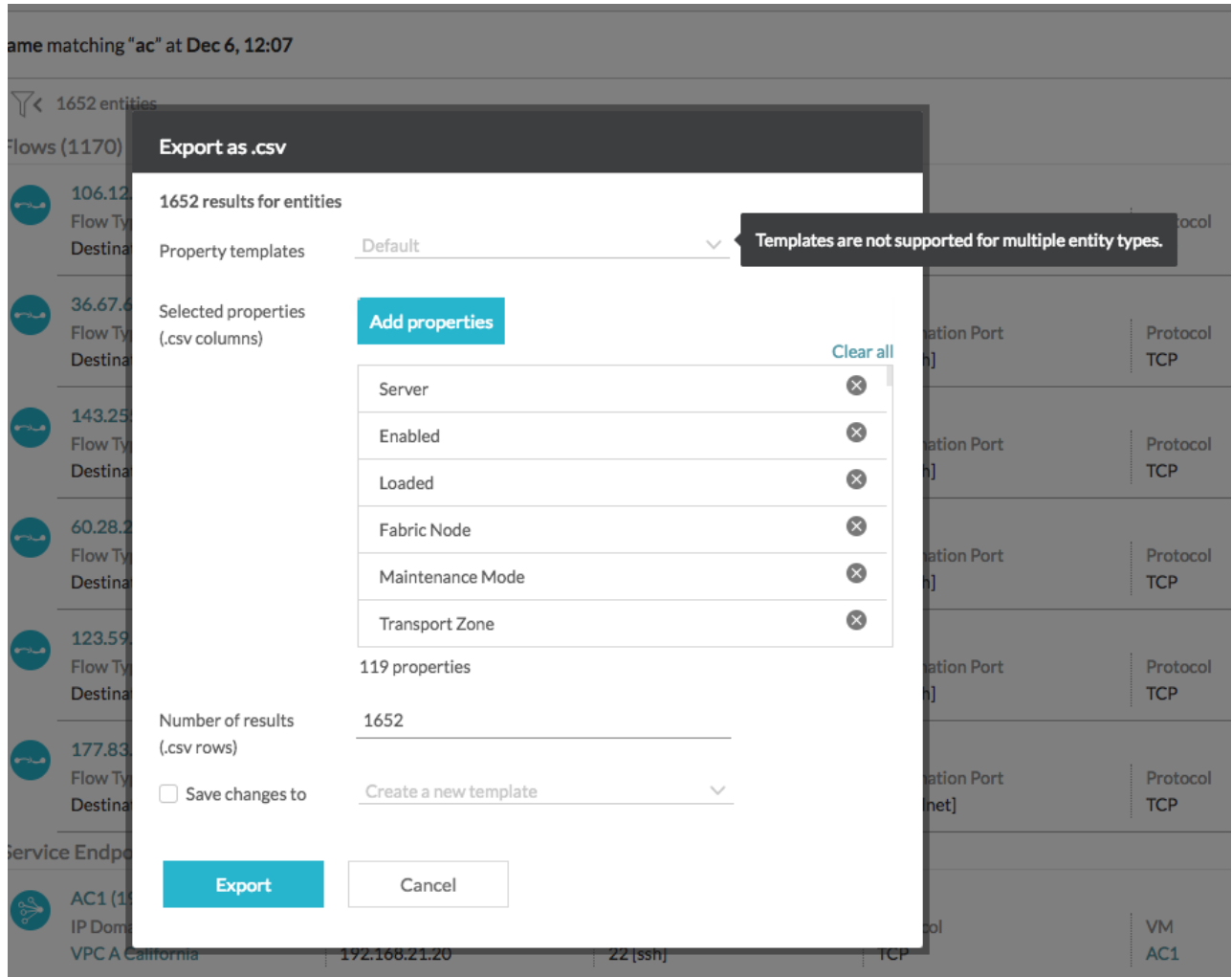
可以在导入工具中使用以下标志：

表 16-1.

标志名称	描述
-uni	从通用文件夹导入项目。
-utag	在通用安全组的成员资格中导入具有通用安全标记的通用项目。
-log	创建在其中启用了日志记录的规则。
	注 此标志不特定于通用选项。

将 CSV 导出的配置保存为属性模板

从 CSV 文件中的小组件导出数据时，可以保存要在属性模板中导出的属性（或列）的组合。当结果属于单个实体类型时，将为 CSV 导出启用这些属性模板。如果您使用列出多个实体类型的关键字进行搜索，则它们无法在属性模板中保存这些属性的组合。



打开 CSV 导出模式时，您将看到搜索结果的默认属性选择（基于实体类型）。您可以更改选定属性的此列表，并保存新配置以供将来参考。或者，也可以从 CSV 导出模式的**模板**部分中加载或打开预先保存的属性模板。更改该值时，您将看到选定属性模板的选定属性。

对要导出的选定属性进行更改后，可以从 CSV 导出模式创建属性模板或编辑现有的属性模板。此模板的实体类型与当前搜索结果的实体类型相同。

通过导航到**设置 > 属性模板**页面，可以查看系统中现有属性模板的列表。**属性模板**页面上的列表显示了包含实体类型、上次更新时间和属性数量等详细信息的现有模板。您可以从**属性模板**页面编辑或删除属性模板。您可以编辑属性模板，但不能更改其名称。

导出并应用 Kubernetes 网络策略

您可以采用 YAML 格式导出与 Kubernetes 对象相关的建议网络策略规则。vRealize Network Insight 支持导出为 YAML 格式（仅适用于分组依据“命名空间”和“服务拓扑”）。

前提条件

- 添加 [Kubernetes](#)
- 添加 [VMware PKS](#)

步骤

- 1 要将建议的规则导出为 YAML 格式，在“规划安全性”模型上选择要为其规划安全性的 Kubernetes 群集，然后执行以下步骤之一。
 - 在微分段小组件中展开更多选项，然后选择**将规则导出为 YAML**，或者
 - 在微分段环形视图中选择一个节点，单击建议的防火墙规则的计数，展开更多选项，然后选择**将规则导出为 YAML**。

vRealize Network Insight 会下载使用 Kubernetes 网络策略命名的 ZIP 文件以及与其关联的时间戳。解压缩该文件时，您会看到以下五个 CSV 文件以及多个文件夹，具体取决于群集的数量。每个文件夹包含群集的多个 YAML 文件。

文件名	描述
network-policy-others-ipaddress.csv	包含服务或命名空间与之通信的物理服务器和虚拟机的 IP 地址。
recommended-namespace-labels-to-add.csv	包含要附加到与命名空间关联的容器的标签。 示例 <ul style="list-style-type: none"> ■ 群集 - pdk8s ■ 命名空间 - sock-shop ■ 标签 - sock-shop-pdk8s
recommended-service-labels-to-add.csv	包含要附加到与服务关联的容器的标签。 示例 <ul style="list-style-type: none"> ■ 群集 - pdk8s ■ 命名空间 - sock-shop ■ 服务 - front-end ■ 标签 - Service:front-sock-shop-pdk8s ■ 群集 - pdk8s ■ 命名空间 - sock-shop ■ 服务 - user ■ 标签 - Service:user-sock-shop
recommended-network-policy.csv	包含 vRealize Network Insight 建议的所有规则。
exported-network-policy-rule-names.csv	列出基于建议的规则导出的所有网络策略。

2 要应用服务标签，请执行以下步骤：**a 运行以下 Kubernetes CLI 命令。**

```
kubectl edit deployment service-name -n namespace-name
```

```
kubectl edit deployment redis-master -n guestbook
```

此时将打开服务的部署文件。

b 在服务标签列表中，将在 CSV 文件中建议的标签附加到服务部署 spec 部分中提到的标签。**3 要应用命名空间标签，请执行以下步骤：****a 运行以下 Kubernetes CLI 命令。**

```
kubectl edit namespace namespace-name
```

```
kubectl edit namespace guestbook
```

此时将打开命名空间的部署文件。

b 在元数据中，将在 CSV 文件中建议的标签附加到命名空间部署的 spec 部分中提到的标签。**4 运行以下命令以验证是否将标签应用于容器。**

```
kubectl get pods -n namespace-name--show-labels
```

```
kubectl get pods guestbook--show-labels
```

在结果视图中查看标签。

注 在命名空间上应用时，标签不会反映在容器上。

5 要创建网络策略，从相应的群集文件夹中复制 YAML 文件，然后运行以下命令：

```
kubectl apply -f *.yaml 或 kubectl apply -f YAML fileyaml
```

结果**示例：****后续步骤**

vRealize Network Insight 可对环境中的所有实体执行强大搜索。

以下是可帮助您使用 vRealize Network Insight 中的搜索功能的一些术语：

- **实体**：数据中心由物理和逻辑构建块（如主机、虚拟机、交换机、路由器、NSX Manager 等）组成。这些块的实例就是实体。
- **属性**：实体由多个属性组成。属性既可以是配置属性，也可以是衡量指标属性。
 - a **配置属性**：实体可以按其配置属性进行描述。配置属性可以是整数或实值，也可以是字符串或布尔值。
 - 虚拟机的名称、CPU 内核数和操作系统
 - 主机的名称和虚拟机数
 - b **衡量指标属性**：衡量实体特定特征的任何属性都是衡量指标属性。衡量指标属性的值按固定时间间隔进行捕获。虚拟机的 CPU 使用情况、内存使用情况和网络使用情况是衡量指标属性的一些示例。
- **聚合函数**：可以在搜索查询中用于计算特定实体类型的实例总数或实体的最大值属性。vRealize Network Insight 支持以下聚合函数。
 - a `sum`
 - b `max`
 - c `min`
 - d `avg`

搜索实体时，软件会在**结果**页面上显示与搜索查询匹配的实体。

对于每个搜索查询，搜索栏会向您建议可用于缩小搜索结果范围的下一个词。例如，输入**虚拟机**一词时，搜索栏会显示可能的词语列表，您可以将其添加到现有词语以缩小搜索结果范围。搜索栏还会验证每个搜索查询。对勾标记表示有效的搜索查询，而叉号标记表示无效的搜索查询。**帮助**页面提供当前受支持查询的示例。

本章讨论了以下主题：

- [搜索查询](#)
- [高级查询](#)

- 时间控制
- 搜索结果
- 筛选器
- vCenter 标记

搜索查询

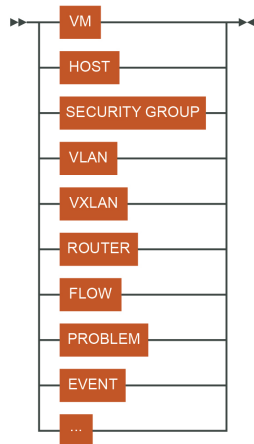
搜索查询可以分为以下类别：

1 结构化查询

结构化查询包含以下组件：



- **实体类型：** 实体类型表示要搜索的对象的类型。可以采用单数形式或复数形式。实体类型在结构化查询中必不可少。



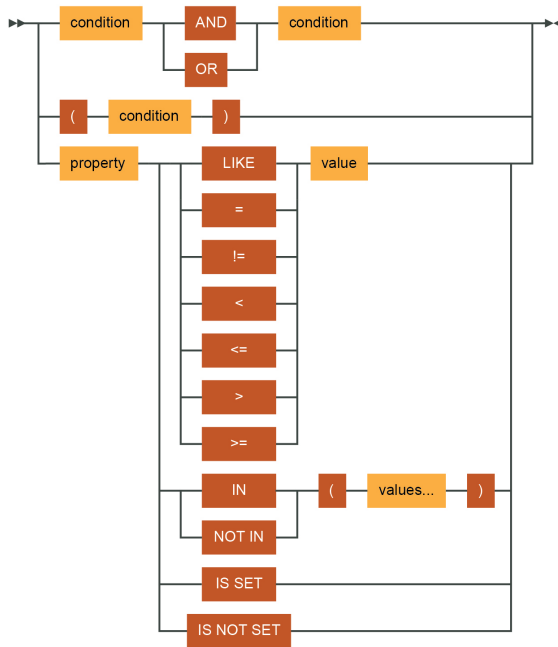
以下是一些示例：

- 1 Virtual machines
- 2 Hosts
- 3 Flows
- 4 MTU Mismatch Events
- 5 Problems

- **筛选器：** 筛选器的语法如下所示：



条件的语法如下所示：



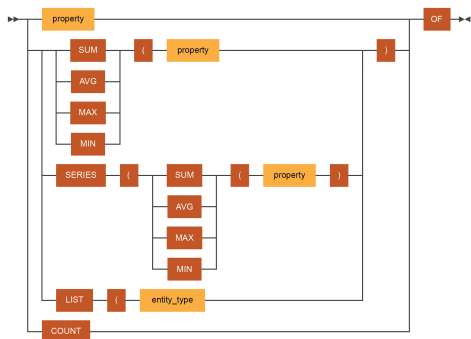
可使用筛选器子句筛选搜索结果。筛选器子句中的条件包含属性、比较运算符和值。可以将条件与逻辑运算符组合以形成复杂条件。以下是可以使用的运算符列表：

运算符	示例
=	flows where source ip address = '10.16.240.0/24' flows where flow type = 'Source is VM'
!=	vms where ip address != '10.17.0.0/16'
>	vms where memory > 4096 mb
<	vms where cpu usage rate < 70%
>=	vms where memory >= 4096 mb
<=	vms where cpu usage rate <= 70%
like	vms where name like 'app'
not like	vms where name not like 'app'
in	flows where port in (22, 23, 80, 443) vm where ip address in (192.168.91.11, 192.168.91.10)
not in	flows where port not in (22, 23, 80, 443) vm where ip address not in (192.168.91.11, 192.168.91.10)
is set	vms where firewall rule is set
is not set	vms where firewall rule is not set

运算符	示例
()	flows where (src tier = 'App' and destination tier = 'DB') OR (destination tier = 'App' and source tier = 'DB')
and	flows where src tier = 'App' and destinationtier = 'DB'
or	flows where flow type = 'Source is VMKNIC' or flow type = 'Destination is VMKNIC'
匹配	vm where name matches '.*' vm where name matches 'a.*' vm where name matches '[a-z]vm-delta[0-9]'
不匹配	vm where name not matches '.*' vm where name not matches 'a.*' vm where name not matches '[a-z]vm-delta[0-9]'
嵌套 “in” 运算符	vm where in (vm where name = 'x') vm where in (vm of host where name = 'x') vm where host in (host of vm where name = 'x') vm where name in (name of vm where name = 'x')

- **投影:** 查询中的投影子句确定了必须显示筛选后实体中的哪些字段。这是可选子句。如果未指定投影子句，则在搜索结果中显示默认字段集。投影子句可以包含以下任何一项：

- 1 属性
- 2 计数
- 3 列表
- 4 聚合
- 5 级数



- 1 **属性:** 按实体类型搜索实体时，搜索结果中将显示默认属性集。使用投影，可以选择应在搜索结果中显示的字段。例如，os of vms 在搜索结果中列出具有 OS property 的所有虚拟机。

下面列出了更多这样的示例：

- cpu cores of vms

- `source ip address of flows`

如果使用衡量指标属性，则会为每个实体显示一个图形，其中衡量指标属性作为 `y-axis`，时间作为 `x-axis`。

2 计数：计数查询可用于计算实体类型的对象数。以下是一些示例：

- `count of vms`
- `count of hosts`
- `count of flows`

3 列表：如果无法在您提取的实体上应用筛选条件，则列表运算符很有用。

例如：

```
List(host) of vms where memory <= 2gb
```

此查询提取主机列表，但是在虚拟机上应用了筛选条件。下面列出了更多这样的示例：

- `List(ip address) of vms where cpu cores = 1`

4 聚合函数：聚合函数允许根据数字 `config` 或 `metric` 属性计算单个值。搜索查询语言支持以下聚合函数：

- `max`
- `sum`
- `min`
- `avg`

以下是一些示例：

- `sum(memory) of hosts`
- `sum(memory), sum(cpu cores) of vms`
- `sum(bytes) of flows`

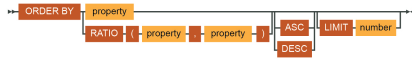
5 级数：级数运算符用于对衡量指标属性执行聚合。例如：

```
series(avg(cpu usage)) of vms where cpu cores = 4
```

此查询显示的图形中包含具有 4 个 `cpu` 内核的所有虚拟机的平均 `cpu` 使用情况。以下是一些示例：

- `series(sum(network usage)) of vms where name like 'app'`
- `series(sum(memory usage)) of vms where name like 'db'`
- `series(avg(cpu usage)), series(avg(memory usage)) of vms`

- **排序：**可以使用 `order by` 子句对搜索结果进行排序。`order by` 子句中仅允许一个字段。默认情况下，结果按降序进行排序。



以下是一些示例：

- 1 vms order by cpu cores
- 2 vms order by cpu cores asc
- 3 flows order by bytes

可以使用 limit 子句限制结果数。此子句前面必须有 order by 子句。例如：

```
vms order by memory limit 5
```

- **分组：**可以按属性对实体进行分组。按属性对实体分组时，默认情况下会显示每个组中的结果数。通过添加投影，可以计算任何属性的总和/最大值/最小值。添加 order by 子句可对结果进行排序。如果查询中存在 order by 或 projection 子句，则必须存在聚合函数。



```
sum(bytes) of flows group by dest vm
```

此查询有效，因为查询在投影子句中具有聚合函数。诸如 bytes of flows group by dest vm 之类的查询无效，因为投影子句中没有聚合函数。

以下是一些示例：

- 1 vms group by host
- 2 sum (bytes) of flows group by dest vm order by sum(bytes)

2 实体查询



- a **按实体类型搜索：**通过搜索实体类型，可以列出该实体类型的所有实体。

示例：vms、hosts、flows、nsx managers

- b **按实体名称搜索**

- **按完整名称搜索：**如果知道实体的完整名称，则可以通过将名称括在单引号中对其进行搜索。

示例：'prod-68-1'、'app1-72-1'

- **按部分名称搜索：**按单个词或多个词搜索将提取与输入词匹配的所有实体。

示例：prod、app1

注 如果输入包含关键字或实体类型，则可能会将其作为搜索查询进行处理。

- **按实体类型和名称搜索：**如果知道实体的名称和类型，则可以通过一起查询实体类型和实体名称来进行搜索。

示例：搜索查询 'vm app1' 会返回包含 app1 的所有虚拟机。

3 规划查询

这些查询可以用于通过分析流来规划数据中心的安全性。

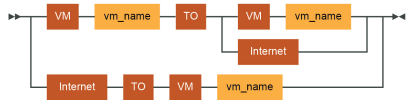


示例:

- a plan securitygroup1
- b plan host1
- c plan security

4 路径查询

这些查询可用于显示两个虚拟机之间的路径或者从虚拟机到 Internet 的路径。



示例:

- a Vm 'vm1' to Vm 'vm2'
- b VM 'vm1' to Internet

注

- 搜索查询不区分大小写。
- 实体类型或配置属性可具有同义词。例如，实体类型 'virtual machine' 具有同义词 'vm'。

Azure 搜索查询

可以在 vRealize Network Insight 中搜索 Azure 实体详细信息。

以下是一些搜索查询示例:

Azure 实体	示例查询
Microsoft Azure	Azure
Azure 应用程序安全组	Azure Application Security Group where Azure Virtual Network = 'Test-vnet2'
Azure 数据源	Azure Data Source
Azure NSG 规则	Azure NSG Rule where Action = 'ALLOW'
Azure 网络接口	Azure Network Interface where Azure Virtual Network = 'Test-vnet2'
Azure 网络安全组	Azure Network Security Group where Subscription = 'vRNI-dev'
Azure 路由	Azure Route where Route Table = 'TestRouteTable'

Azure 实体	示例查询
Azure 路由表	Azure Route Table where Azure Virtual Network = 'aks-vnet-28255566'
Azure 子网	Azure Subnet where Azure Virtual Network = 'vrni-01-vnet'
Azure 订阅	Azure Subscription
Azure 虚拟机	Azure Virtual Machine where Azure Application Security Group = 'TestASG'
Azure 虚拟网络	Azure Virtual Network where Azure Peer Virtual Network = 'vrni-01-vnet'

Cisco ACI 实体

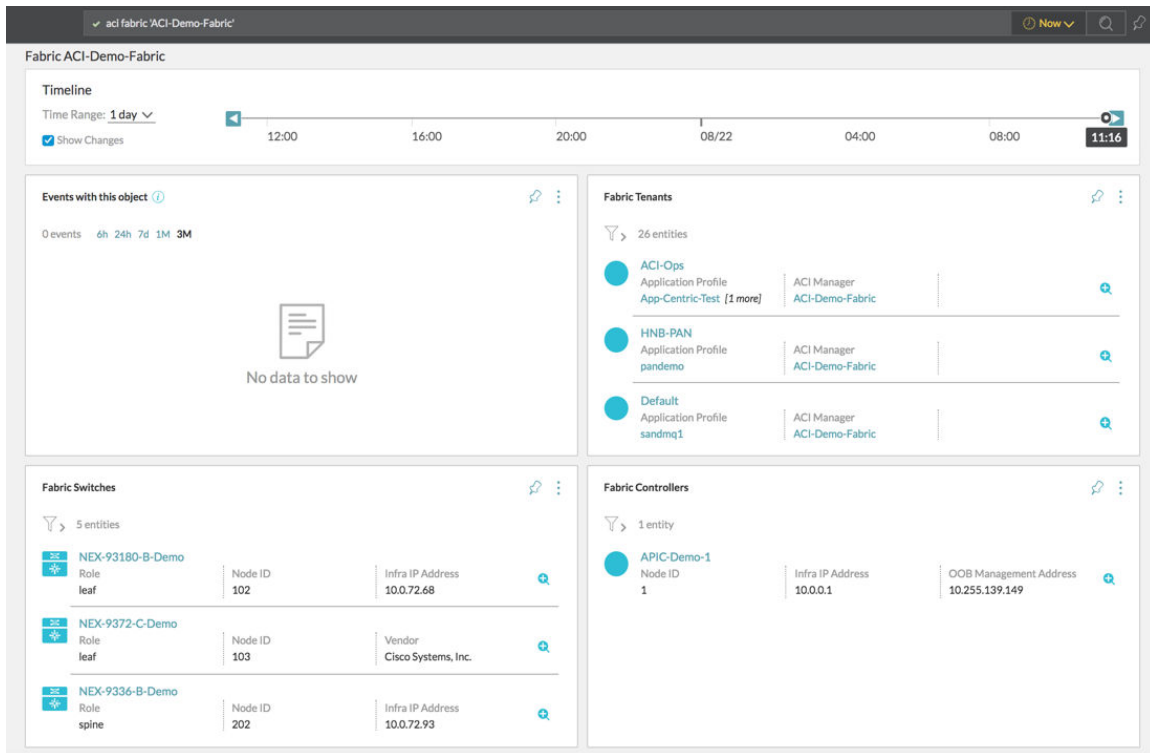
以下是可以对其执行搜索的一些 Cisco ACI 实体的列表：

注 实体以 aci 为前缀。

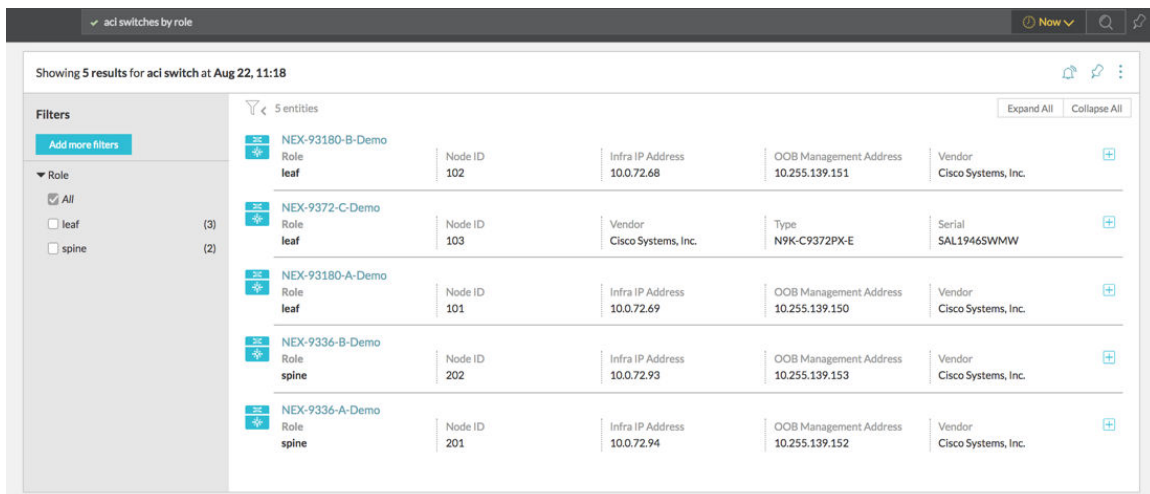
- aci application profile
- aci bridge domain
- aci endpoint group
- aci fabric
- aci switch
- aci tenant

以下是一些搜索查询示例：

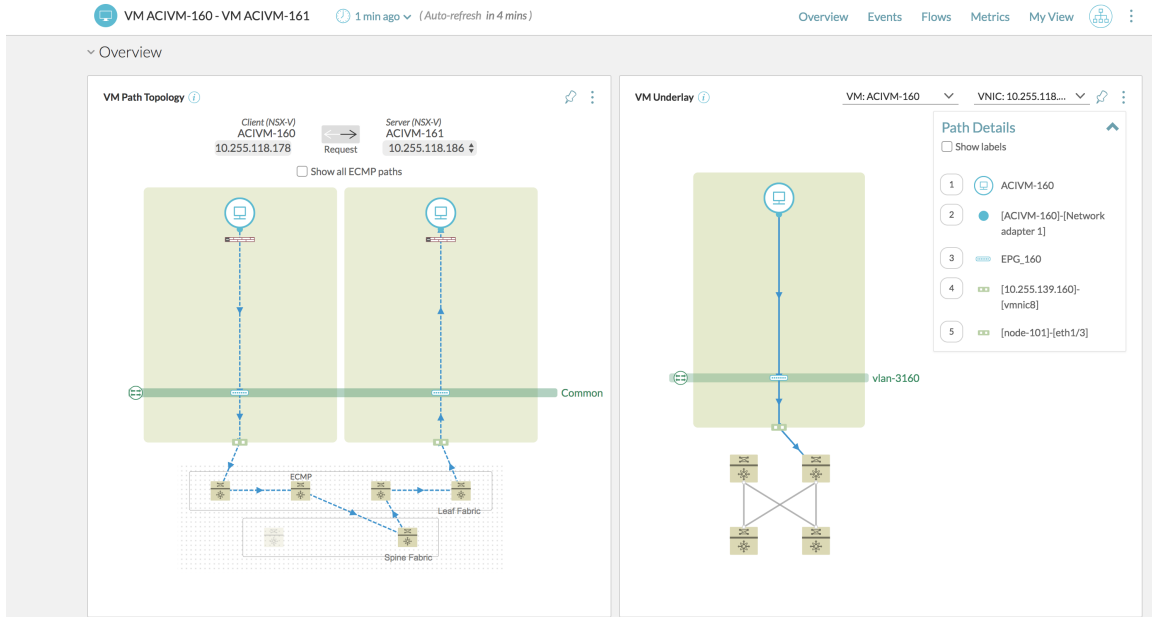
- aci fabric 'ACI-Demo-Fabric': 此查询检索有关 ACI 结构层中租户、交换机和控制器的信息。



- **aci switches by role:** 此查询检索有关 ACI 结构层中各种叶交换机或主干交换机的信息。从交换机列表中，单击交换机名称以获取有关该交换机的更多详细信息。



- **aci endpoint group:** 此查询检索具有关联虚拟机、网桥域和 VRF 的端点组的列表。
- **aci application profile 'Production':** 此查询检索具有包含的端点组和虚拟机的生产应用程序配置文件。
- **VMware VM 'ACIVM-160' to VMware VM 'ACIVM-161':** 此查询显示两个虚拟机之间的虚拟机-虚拟机路径。



- 您可以使用 IP 地址进行搜索，以获取端口、端点组和网桥域详细信息。

10.114.219.158

Showing 2 results for Entities with keywords "10.114.219.158" at Mar 25, 15:10

2 entities

Endpoint Group (1)

Mgmt-1201	Application Profile NSXInfra	Bridge Domain BD-Mgmt	Encap vlan-1201	Number of VMs 0	Endpoints 00:0C:29:44:70:D8 10.114.21... [17 more]
-----------	---------------------------------	--------------------------	--------------------	--------------------	---

Switch Port (1)

[node-104]-[eth1/19]	Operational Status Up	Administrative Status Up	Mac Address 00:D7:8F:85:B9:7B	MTU 9000	Interface speed 10 Gbps
----------------------	--------------------------	-----------------------------	----------------------------------	-------------	----------------------------

- 您可以使用 Mac 地址进行搜索，以获取端口、端点组和网桥域详细信息。

00:0C:29:44:70:D8

Showing 2 results for Entities with keywords "00:0C:29:44:70:D8" at Mar 25, 15:06

2 entities

Endpoint Group (1)

Mgmt-1201	Application Profile NSXInfra	Bridge Domain BD-Mgmt	Encap vlan-1201	Number of VMs 0	Endpoints 00:0C:29:44:70:D8 1... [17 more]
-----------	---------------------------------	--------------------------	--------------------	--------------------	---

Switch Port (1)

[node-104]-[eth1/19]	Operational Status Up	Administrative Status Up	Mac Address 00:D7:8F:85:B9:7B	MTU 9000	Interface speed 10 Gbps
----------------------	--------------------------	-----------------------------	----------------------------------	-------------	----------------------------

Filters

Add more filters

Entity Type

- All
- Switch Port
- Endpoint Group

- 您可以搜索端点组，并获取关联端点的列表。

aci epg where Endpoint is set

Showing 4 results for aci endpoint group with filter Endpoint is set at Mar 25, 15:11

Filters

Add more filters

Endpoints

☒ All

☐ 00:0C:29:44:70:D8 10.114.219.158 (1)

☐ 00:0C:29:4E:6A:B4 10.114.219.146 (1)

☐ 00:0C:29:BE:EF:D5 10.114.219.147 (1)

☐ 00:1B:21:69:83:88 10.114.219.137 (1)

☐ 00:25:90:E1:6C:52 10.114.219.136 (1)

[20 more]

4 entities

Entity	Endpoints	Application Profile	Bridge Domain	Encap	Number of VMs
Mgmt-1201	00:0C:29:44:70:D8... [17 more]	NSXInfra	BD-Mgmt	vlan-1201	0
IPSt...	00:0C:29:44:70:D8 10.114.219.158 00:0C:29:4E:6A:B4 10.114.219.146 00:0C:29:BE:EF:D5 10.114.219.147 00:1B:21:69:83:88 10.114.219.137 00:25:90:E1:6C:52 10.114.219.136 00:25:90:E1:76:9E 10.114.219.135 00:25:90:E1:CC:B8 10.114.219.134 00:25:90:EB:BA:EE 10.114.219.130 00:25:90:EB:BA:F0 10.114.219.131 00:50:56:BE:16:BF 10.114.219.152 00:50:56:BE:7C:FE 10.114.219.133 00:50:56:BE:84:E5 10.114.219.151 00:50:56:BE:0A:C4:41... [1 more]	NSXInfra	BD-IPStorage	vlan-1204	0
Tran...	00:0C:29:44:70:D8 10.114.219.158 00:0C:29:4E:6A:B4 10.114.219.146 00:0C:29:BE:EF:D5 10.114.219.147 00:1B:21:69:83:88 10.114.219.137 00:25:90:E1:6C:52 10.114.219.136 00:25:90:E1:76:9E 10.114.219.135 00:25:90:E1:CC:B8 10.114.219.134 00:25:90:EB:BA:EE 10.114.219.130 00:25:90:EB:BA:F0 10.114.219.131 00:50:56:BE:16:BF 10.114.219.152 00:50:56:BE:7C:FE 10.114.219.133 00:50:56:BE:84:E5 10.114.219.151 00:50:56:BE:0A:C4:41... [1 more]	NSXInfra	BD-Transport	NSX-VRF	0
Vmo...	00:0C:29:44:70:D8 10.114.219.158 00:0C:29:4E:6A:B4 10.114.219.146 00:0C:29:BE:EF:D5 10.114.219.147 00:1B:21:69:83:88 10.114.219.137 00:25:90:E1:6C:52 10.114.219.136 00:25:90:E1:76:9E 10.114.219.135 00:25:90:E1:CC:B8 10.114.219.134 00:25:90:EB:BA:EE 10.114.219.130 00:25:90:EB:BA:F0 10.114.219.131 00:50:56:BE:16:BF 10.114.219.152 00:50:56:BE:7C:FE 10.114.219.133 00:50:56:BE:84:E5 10.114.219.151 00:50:56:BE:0A:C4:41... [1 more]	NSXInfra	BD-Vmotion	vlan-1203	0

- 您可以搜索端点。

aci epg where Endpoint like 10.114.219.158

Showing 1 result for aci endpoint group with filter Endpoint like 10.114.219.158 at Mar 25, 15:19

Filters

Add more filters

Endpoints

☒ All

☐ 00:0C:29:44:70:D8 10.114.219.158 (1)

☐ 00:0C:29:4E:6A:B4 10.114.219.146 (1)

☐ 00:0C:29:BE:EF:D5 10.114.219.147 (1)

☐ 00:1B:21:69:83:88 10.114.219.137 (1)

☐ 00:25:90:E1:6C:52 10.114.219.136 (1)

[13 more]

1 entity

Entity	Endpoints	Application Profile	Bridge Domain	Encap	Number of VMs
Mgmt-1201	00:0C:29:44:70:D8... [17 more]	NSXInfra	BD-Mgmt	vlan-1201	0

Fortinet 搜索查询

您可以在 vRealize Network Insight 中搜索 Fortinet 实体详细信息。

以下是一些搜索查询示例：

Fortinet 实体	示例查询
Fortinet 策略包	Fortinet Policy Package where Domain Manager = 'ADOM_NAME'
Fortinet 策略	Fortinet Policy where Source IP = '10.0.0.15'
Fortinet 地址	Fortinet Address where Address Type = 'ipmask'
Fortinet 动态地址	Fortinet Dynamic Address where Domain Manager = 'ADOM_NAME'
Fortinet 动态地址组	Fortinet Dynamic Address Group where Domain Manager = 'ADOM_NAME'
Fortinet 服务	Fortinet Service where port = 5900
Fortinet 服务组	Fortinet Service Group where Manger = '10.0.15.101'

Fortinet 实体	示例查询
Fortinet ADOM	Fortinet ADOM where Manager ID = '10.0.15.101'
Fortinet VDOM	Fortinet VDOM where Domain Manager = 'ADOM_NAME'
Fortinet 动态接口	Fortinet Dynamic Interface where Domain Manager = 'ADOM_NAME'

使用 Infoblox DNS 数据扩充流

vRealize Network Insight 支持以下两个 DNS 信息源：

- 导入的 CSV 文件
- Infoblox DNS

注 如果 Infoblox DNS 与 CSV 文件之间存在冲突，则来自 Infoblox DNS 的信息优先。

可以使用各种搜索查询来找出有关流中 DNS 条目源的更多信息。

表 17-1.

关键字	搜索查询示例	描述
DNS 提供程序	Flows where DNS Provider='Infoblox'	提供从 Infoblox 获取 DNS 数据的流列表。
DNS 提供程序	Flows where DNS Provider='CSV'	提供从 CSV 获取 DNS 数据的流列表。
源 DNS 提供程序	Flows where Source DNS Provider='Infoblox'	提供源 IP 地址的 DNS 提供程序为 Infoblox 的流列表。
目标 DNS 提供程序	Flows where Destination DNS provider='Infoblox'	提供目标 IP 地址的 DNS 提供程序为 Infoblox 的流列表。

Kubernetes 实体的常见搜索查询

您可以在 vRealize Network Insight 中搜索 Kubernetes 实体详细信息。

常见查询

- 搜索流： `flows where Kubernetes Object = Object name`
示例： `flows where Kubernetes Cluster = 'Production'`
- 查看服务规模： `kubernetes pods group by Kubernetes Services`
- 查看节点加载： `kubernetes Pods group by Kubernetes Node`
- 查看节点运行状况： `MemoryPressure and PIDPressure and DiskPressure and Ready of Kubernetes Node`

- 查看流合规性: flows from Kubernetes Object *name of the object* to Kubernetes Object *name of the object*

示例: flows from Kubernetes Namespace '**PCI**' to Kubernetes Namespace '**Non-PCI**'

- 查看路径拓扑:
 - Kubernetes 服务 *service name* 到 Kubernetes 服务 *service name*
 - Kubernetes 服务 *service name* 到 Kubernetes pod *pod name*
 - Kubernetes pod *pod name* 到 Kubernetes pod *pod name*

表 17-2. 查询 Kubernetes 对象

Kubernetes 对象	查询	描述
命名空间	<ul style="list-style-type: none"> ■ kubernetes namespace where L2 Networks = '<i>a</i>' ■ list(Kubernetes Node) of Kubernetes Pod where Kubernetes Namespace = '<i>a</i>' 	<ul style="list-style-type: none"> ■ 返回连接到 L2 网络 “a” 的 Kubernetes 命名空间 ■ 返回 Kubernetes 命名空间为 “a” 的 Kubernetes 节点列表
Pod	<ul style="list-style-type: none"> ■ NSX-T Logical port where connectedto.modelKey in (modelKey of kubernetes nodes) order by Tx Packets desc ■ NSX-T Logical port where connectedto.modelKey in (modelKey of kubernetes pods) and Rx Packet Drops > 0 ■ new kubernetes pod in last 1 hour 	<ul style="list-style-type: none"> ■ 返回基于传输的数据包按降序连接到节点的逻辑端口的列表 ■ 返回连接到 Kubernetes 容器且丢弃的 Rx 数据包大于 0 的逻辑端口的列表 ■ 最近一小时发现的新 Kubernetes Pod
服务	<ul style="list-style-type: none"> ■ kubernetes pods where kubernetes services is not set ■ kubernetes pods group by Kubernetes Services, Kubernetes Cluster 	<ul style="list-style-type: none"> ■ 没有服务的 Kubernetes Pod 列表 ■ 每个服务上运行的 Pod 数
节点数	<ul style="list-style-type: none"> ■ kubernetes nodes where Ready != 'True' ■ kubernetes node where Virtual Machine = 'vm-a' 	<ul style="list-style-type: none"> ■ 不正常的 Kubernetes 节点的列表 ■ 属于 “vm-a” 虚拟机的 Kubernetes 节点
流	<ul style="list-style-type: none"> ■ flows where kubernetes service is set ■ flows where source kubernetes node = '<i>a</i>' 	<ul style="list-style-type: none"> ■ 源或目标 Kubernetes 服务存在的流列表 ■ 源 Kubernetes 节点为 “a” 或目标 Kubernetes 节点为 “a” 的流列表

负载均衡器相关的示例搜索查询

您可以使用以下示例查询来筛选或搜索与负载均衡器相关的数据。

- `vm where lbServiceNodes is set` - 列出托管分发负载的应用程序的所有虚拟机。
- `vm where lbServiceNodes is set and PowerState != 'POWEREDON'` - 列出托管负载均衡应用程序但当前未正常运行的所有虚拟机。
- `pool member where state = 'DISABLED'` - 列出已禁用的所有池成员。
- `Count of Pool Memembers where Service Port = '80'` - 提供在端口 80 上运行的特定服务类型的所有池成员的计数。
- `service node where virtual machine is not set` - 列出使用物理服务器作为应用程序服务器的所有服务节点，或者托管未添加到 vRealize Network Insight 中的虚拟机的 vCenter Server

NSX 防火墙规则的搜索查询

您可以在 vRealize Network Insight 中搜索 NSX 防火墙规则。

表 17-3. 防火墙规则查询

搜索查询	描述
<code>VM where incoming rules.Source Any</code>	查看具有任何源的规则（可以与特定端口组合）。
<code>Firewall rule where action = allow and service any = true</code>	查看允许任何端口的防火墙规则。
<code>Firewall Rule Masked Event</code>	查看未使用的防火墙规则的列表。
<code>New firewall rules in last 24 hours</code>	查看过去 24 小时内创建的防火墙规则。
<code>New firewall rules in last 7 days</code>	查看过去 7 天内创建的防火墙规则。
<code>New firewall rules in last 30 days</code>	查看过去 30 天内创建的防火墙规则。
<code>Firewall rule where flow is not set</code>	查看非活动防火墙规则的列表。
<code>Flow group by firewall rule</code>	查看命中每个防火墙规则的流计数。
<code>Security group where Indirect Incoming Rules is not set and Indirect Outgoing Rules is not set and Direct Incoming Rules is not set and Direct Outgoing Rules is not set</code>	查看未使用的安全组。
<code>Ipset where Indirect Incoming Rules is not set and Indirect Outgoing Rules is not set and Direct Incoming Rules is not set and Direct Outgoing Rules is not set</code>	查看未使用的 IPSet。
<code>Flow where rule id in (1011, 1012, 1013)</code>	命中特定规则 ID 的流。
<code>Flow where application = appl</code>	命中应用程序的流。

- 未使用的防火墙规则

- 防火墙规则屏蔽规则事件

VMware SD-WAN 搜索查询

可以在 vRealize Network Insight 中搜索 VMware SD-WAN 实体详细信息。

以下是几个搜索查询示例：

VMware SD-WAN 实体	示例查询
VeloCloud 集群	<code>VeloCloud Cluster where Description = 'cluster one'</code>
VeloCloud 数据源	<code>VeloCloud Data Source where Enabled = true</code>
VeloCloud Edge	<code>VeloCloud Edge where Activation State = 'Activated'</code>
VeloCloud 企业	<code>VeloCloud Enterprise where Name = 'VMWare - vRNI'</code>
VeloCloud 网关	<code>VeloCloud Gateway where City = 'Ashburn'</code>
VeloCloud 第 2 层网络	<code>VeloCloud Layer2 Network where Network = '172.16.40.2/24'</code>
VeloCloud 链路	<code>VeloCloud Link where Link Uptime = 100%</code>
VeloCloud 配置文件	<code>VeloCloud Profile where Name = 'APProfile'</code>
VeloCloud 分段	<code>VeloCloud Segment where Vendor ID = '1'</code>

VMware Cloud on AWS for AWS 实体

以下是与 VMware Cloud on AWS NSX Policy Manager 相关的实体：

- NSX Policy Manager Data Source
- NSX Policy Manager
- NSX Policy Firewall
- NSX Policy Firewall Rule
- NSX Policy Segment
- NSX Policy Based VPN
- NSX Policy Group

注 如果将 NSX-T 2.4 和 VMware Cloud on AWS 添加为 vRealize Network Insight 中的数据源，那么要获取 VMware Cloud on AWS 实体，您必须在查询中添加 **SDDC type = VMC** 筛选器。例如，要列出适用于 VMware Cloud on AWS 的基于策略的 VPN，请输入

NSX Policy Based VPN where Tier0 = ‘’ and SDDC Type = ‘VMC’。

与 VMware Cloud on AWS 实体相关的一些搜索查询示例如下：

- `VMs where L2 Network = '' (L2 Network -> NSX Policy Segment)`

- NSX Policy Based VPN where Tier0 = ''
- NSX Policy Based VPN where Local Network = '' (Local Network of Policy Based VPN Rule)
- NSX Policy Based VPN where Remote Network = '' (Remote Network of Policy Based VPN Rule)
- NSX Policy Group where Translated VM = ''
- VM where NSX Policy Group = ''

注

- NSX Policy Manager 不支持子组或 IPSET。因此，将禁用类似 NSX Policy firewall rule where Indirect _____ = '' 或 NSX Policy group where Indirect _____ = '' 的所有搜索。

高级查询

以下是高级查询的一些示例：

通信模式的流查询

- 跨数据中心或站点的总流量（DCI 链接使用）


```
sum(bytes) of flows where ( Dst Manager = 'abc' AND src manager = 'cba') OR ( Dst Manager = 'cba' AND src manager = 'abc')
```
- VTEP 流量总计
 - ```
sum(bytes) of flows where Flow Type = 'Src is VTEP' or flow type = 'Dst is VTEP' VTEP traffic grouped by VMKNIC
```
  - ```
sum(bytes) of flows where Flow Type = 'Src is VTEP' or Flow Type = 'Dst is VTEP' group by ip
```
- 其他管理流量


```
flows where Flow Type = 'Source is VMKNIC' or Flow Type = 'Destination is VMKNIC'
```

用于聚合和分组的流查询

- Internet 流量总计（按源虚拟机）


```
sum(bytes) of flows where Flow Type = 'Internet' group by src vm
```
- 排名靠前的端口（按总字节数）


```
sum(bytes) of flow group by port order by sum(bytes)
```
- 排名靠前的子网对（按路由的流量）


```
sum(bytes) of flow where Flow Type = 'Routed' group by Source Subnet Network, destination subnet network order by sum(bytes)
```

- 虚拟机总计（按成对总字节数）

```
sum(bytes) of flows group by src vm , dest vm order by sum(bytes)
```

- 排名靠前的服务器虚拟机/端口（按总字节数）

```
sum(bytes) of flows group by dest vm , port order by sum(bytes)
```

用于容量估算和大小调整的流查询

- 由 ESX 分组的所有 vm-internet/internet-vm 流量的总字节数（Palo Alto 服务虚拟机大小调整）

```
sum(bytes) of flows where flow type = 'internet' and (flow type = ' src is vm ' OR  
flow type = 'destination is vm ') group by host order by sum(bytes)
```

- 用于匹配流的聚合流量系列（Palo Alto 服务虚拟机大小调整）

```
series( sum(byte rate)) of flows where host = 'ddc1-pod2esx012.dm.democompany.net'  
and (Flow Type = 'Source is VM' OR flow type = 'Destination is VM')
```

应用程序的有用查询

- 给定应用程序中的虚拟机

```
VM where application = 'CRM'
```

- 从给定应用程序路由的流

```
Flows where source application = CRM and Flow Type = 'Routed'
```

- 两层之间的流（单向）

```
Flows where src tier = 'App' and Destination Tier = 'DB'
```

- 两层之间的流（双向）

```
Flows where ( src tier = 'App' and destination Tier = 'DB') OR (destination tier =  
'App' and source tier = 'DB')
```

虚拟机和 ESX 的有用查询

- Prod-Midtier-1 虚拟机的属性（MAC、IP、主机等）

```
CPU Usage Rate, Network Rate, Memory Usage Rate, mac address, ip , vxlan , host of  
vm 'Quality control-VM26'
```

- 具有最高虚拟机计数的网络分段

```
vm group by l2 network
```

- 数据存储具有最高虚拟机计数

```
vm group by datastore
```

- 主机（按 vSphere 版本）

```
host group by version
```

- 主机（按 vSphere 内部版本）

```
host group by OS
```

- 插入特定 UCS 机箱的所有主机/刀片上的所有虚拟机（嵌套查询）

```
vm where host in (host where Blade like 'sys/chassis-1')
```

有用的查询：一般容量

- 数据中心数：

```
count of datacenter
```

- 群集数

```
count of cluster
```

- 主机数

```
count of host
```

- 虚拟机数

```
count of vm
```

- 网络数

```
count of vlan
```

有用的查询：路由

- VNI（按主控制器）

```
vxlan group by Primary Controller
```

- 提供程序 Edge 3 的路由

```
routes where vrf = 'Provider Edge 3'
```

- DMZ DLR 的路由

```
NextHop Router of routes where VRF = 'LDR-DMZ'
```

- 将给定路由器作为下一跃点的路由

```
routes where NextHop Router = 'California-Edge'
```

有用的查询：防火墙规则

- 两个虚拟机之间的防火墙规则

```
firewall rules from 'Prod-Midtier-1' to 'Prod-Db-1'
```

- 具有 ANY 源的规则

```
firewall rules where Service Any = true
```

- 给定规则的虚拟机

```
vm where Firewall Rule = 'Prod MidTier to Prod DB - DBService '
```

- 允许任何端口的防火墙规则

```
firewall rule where action = allow and service any = true
```

- 命中特定防火墙规则的流

```
flows where firewall rule = 'Admin to Prod and Lab - SSH'
```

- 系统中已拒绝的流

```
flows where firewall action = deny
```

有用的查询：一般流量模式

- 东西向和南北向流量计数、交换流量计数、路由流量计数以及虚拟机到虚拟机流量计数

```
plan security in last 7 days
```

有用的查询：来自安全镜头的流量

- 通信最多者虚拟机详细信息

```
top 7 vm group by name, Vlan order by sum(Total Network Traffic) in last 7 days
```

- 承载最多流量的网络

```
top 7 vlan group by Vlan id, vm count order by sum(Total Network Traffic) in last 7 days
```

- 大多数通信位于 VLAN 内的网络（不跨越物理防火墙或 L3 边界）

```
top 7 flow where Flow Type = 'Switched' group by Subnet Network order by sum(Bytes) in last 7 days
```

- 大多数通信都通过 VLAN 的网络（可能会导致物理防火墙出现瓶颈问题）

```
top 7 flow where Flow Type = 'Routed' group by Source Subnet Network, Destination Subnet Network order by sum(Bytes) in last 7 days
```

- 在国家/地区外通信的虚拟机

```
top 7 flow where Destination Country != 'United States' group by Source VM, Destination Country order by sum(Bytes) in last 7 days
```

- 经历最多存储延迟的数据存储

```
avg(Read Latency), avg(Write Latency) of top 7 vm group by Datastore, vlan order by avg(Write Latency) in last 7 days
```

有用的查询：合规性/漏洞

- 易受攻击的操作系统详细信息

```
vm where Operating System like 'Microsoft Windows Server 2003' or Operating System
like 'Microsoft Windows Server 2008' or Operating System like 'Red Hat Enterprise
Linux 6' or Operating System like 'Red Hat Enterprise Linux 5' or Operating System
like 'SUSE Linux Enterprise 10' group by vlan, Operating System
```

■ 易受攻击的操作系统计数

```
count of vm where Operating System like 'Microsoft Windows Server 2003' or
Operating System like 'Microsoft Windows Server 2008' or Operating System like 'Red
Hat Enterprise Linux 6' or Operating System like 'Red Hat Enterprise Linux 5' or
Operating System like 'SUSE Linux Enterprise 10'
```

■ 由于旧操作系统造成的总攻击面

```
vm where vlan in (vlan of vm where os in ('Microsoft Windows Server 2003',
'Microsoft Windows Server 2008', 'Red Hat Enterprise Linux 6', 'Red Hat Enterprise
Linux 5', 'SUSE Linux Enterprise 10')) group by Vlan

count of vm where vlan in (vlan of vm where os in ('Microsoft Windows Server 2003',
'Microsoft Windows Server 2008', 'Red Hat Enterprise Linux 6', 'Red Hat Enterprise
Linux 5', 'SUSE Linux Enterprise 10'))
```

注 要获取针对易受攻击的操作系统的建议防火墙规则，请参见[建议的防火墙规则用于保护易受攻击的操作系统](#)。

时间控制

通过时间控制，可以在所选时间或时间范围的上下文中运行搜索查询。可以从预设（如过去 24 小时、过去 3 天等）列表中进行选择。也可以使用[处于](#)选项指定特定的日期和时间，甚至可以使用[介于](#)选项指定范围。

搜索结果

搜索结果页面提供与特定搜索匹配的相关实体的详细列表。页面本身提供了大量信息，这些信息包括实体列表、其对应属性以及筛选搜索结果以优化搜索的层面。

也可以展开或折叠搜索结果中的每个条目，以查看有关特定条目的详细信息。也可以为每个搜索创建通知。

注 可以指向搜索结果以及实体页面中的特定属性，以查看包含有关该属性的详细信息的工具提示。

下图显示了 VXLAN 的搜索结果，其中 num vms > 0 搜索查询过去的时间。

vxlan where Num VMs > 0

Showing 12 results for Vxlan with filter Num VMs > 0 at

Filters

Add more filters

▼ VM Count

☒ All

☐ 1 (5)

☐ 2 (5)

☐ 3 (2)

► NSX Manager

► Scope

12 entities

Expand All Collapse All

Siteb-Aundh-LS	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
3	10.197.17.114	Global	5006	192.168.23.0/24		
Siteb_P-seattle-vxlan	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
3	10.197.17.229	Global	5000	172.17.1.0/24		
Siteb_P-redmond-vxlan	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
2	10.197.17.229	Global	5001	172.17.2.0/24		
Siteb-Wagholi-LS	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
2	10.197.17.114	Global	5005	192.168.26.0/24		
Siteb-pashan-ls-1	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
2	10.197.17.114	Global	5002	192.168.24.0/24		
Siteb_P-transit-vxlan-2	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
2	10.197.17.229	Global	5005	172.17.6.0/24		
Siteb_P-transit-vxlan-1	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
2	10.197.17.229	Global	5004	172.17.5.0/24		
Siteb-Transit-LS-1	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
1	10.197.17.114	Global	5003	192.168.21.0/24		

筛选器

Filters

Add more filters

▼ Default Gateway

☒ All

☐ 192.168.23.10 (1)

► NSX Manager

► Scope

► VM Count

获得搜索结果后，根据您的要求，单击左侧窗格上的“添加更多筛选器”。可以查看一系列筛选器类别，可以使用这些类别缩小搜索结果的范围。每个类别旁边的小框中显示该类别的可用筛选器数。查看该类别的可用筛选器（以及每个筛选器的简短说明），然后单击以应用该筛选器。也可以使用筛选器搜索框来搜索特定的筛选器，vRealize Network Insight 将自动显示与搜索查询匹配的筛选器，您可以单击该筛选器加以应用。每个筛选器都具有多个用于优化搜索结果的属性。从其中一个筛选器中选择筛选器属性时，选定属性将在搜索结果中突出显示。

vCenter 标记

vRealize Network Insight 提供用于搜索和规划的 vCenter 标记。

可以基于 vCenter 标记和自定义属性执行虚拟机的搜索。例如，可以通过使用标记来使用以下查询进行搜索：

```
vm where tag = '{keyname}:{value}'
```

每个标记都属于一个类别。在以上示例中，keyname 是标记所属的类别，value 是标记的名称。

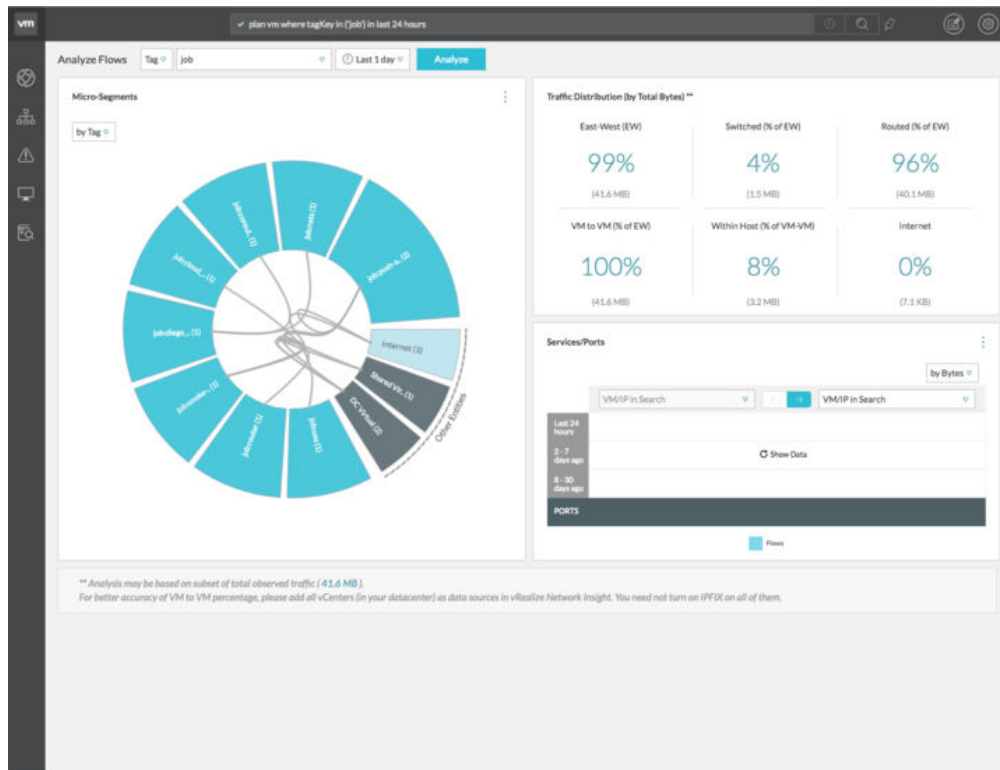
也可以通过 name 键使用 vCenter 标记或自定义属性为虚拟机提供备用名称。此备用名称显示为 other names 属性。也可以使用备用名称搜索并进行路径查询。

例如，支持以下查询：

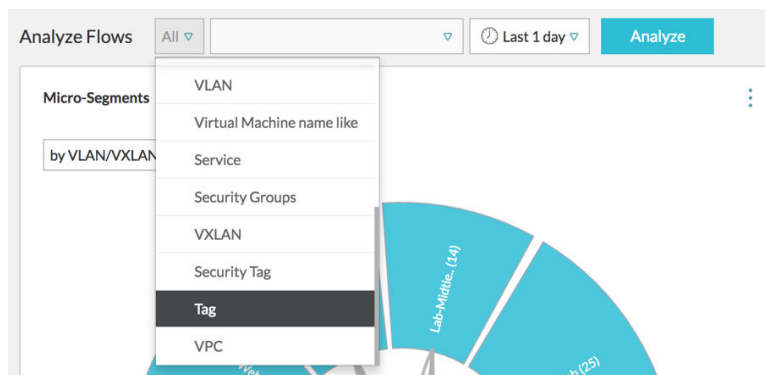
```
vm "other-name-1"
    vm "other-name-1" to vm "other-name-2"
```

在此示例中，other-name-1 和 other-name-2 是自定义属性，name 键或标记属于 name 类别。

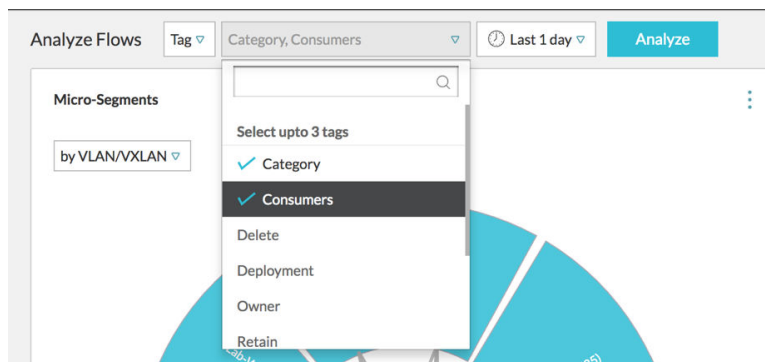
也可以通过使用 vCenter 标记来分析网络中的流，如图所示。



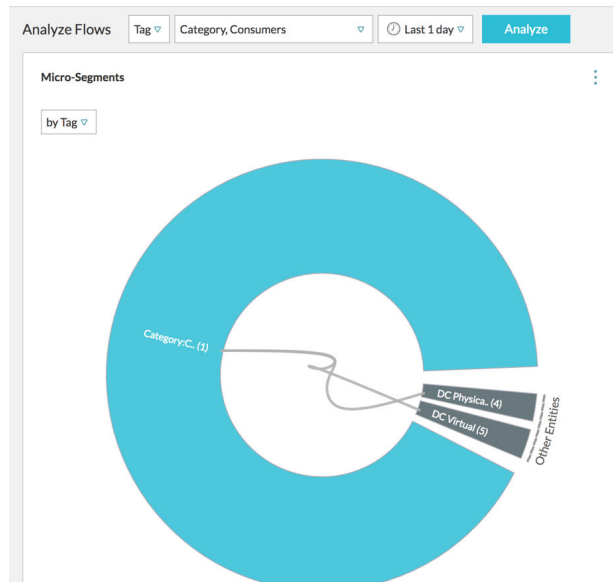
要使用 vCenter 标记，请从分析流下拉列表中选择标记选项。



此外，在此级别上最多可以选择三个标记。选择标记后，单击分析。



在按条件分组中，已选择标记。



规划 vRealize Network Insight 的灾难恢复

18

VMware Site Recovery Manager (SRM) 是一种灾难恢复自动化软件，可提供基于策略的管理、无中断测试和自动编排。vRealize Network Insight 支持 SRM 8.1 及更高版本。为了保护您的 vRealize Network Insight，SRM 会自动执行灾难恢复计划的各个方面以加快恢复速度，并消除使用手动过程时存在的风险。

有关安装、升级和配置 SRM 的信息，请参见 [VMware Site Recovery Manager 文档](#)。

vRealize Network Insight 灾难恢复操作的必备条件如下所示：

- 确保已安装并配置 vSphere Replication。
- 应在受保护站点和恢复站点上部署和配置 SRM。
- 继续创建恢复计划和其他组件之前，请确保已通过 SRM UI 正确配置站点配对。
- 应为环境中 vRNI 安装的每个受保护节点启用 VMware vSphere Replication。启用 VMware vSphere Replication 时，请考虑 vRealize Network Insight 节点大小和使用情况并提供足够的 RPO，以便在灾难期间尽可能减少预期的数据丢失。有关复制的详细信息，请参见 [VMware vSphere Replication 文档](#)。
- 确保为 vRealize Network Insight 创建单独的保护组。对于小型和非分布式部署，请确保所有虚拟机都位于同一个保护组中。对于分布式部署，建议将所有平台置于一个保护组中以便于恢复。您可以将收集器置于不同的保护组中。
- 创建恢复计划，并将包含 vRealize Network Insight 虚拟机的保护组添加到此计划。确保包含平台节点的保护组具有更高优先级。在恢复计划中，确保主平台节点所在保护组比其他平台节点具有更高的优先级。
- 目前，不支持使用 SRM 进行任何类型的 IPv4 自定义

建议将 vRealize Network Insight 虚拟机迁移或恢复到相同的网络配置。此外，根据 SRM 建议，您可以定期执行测试运行，以确保现有计划可与底层基础架构和配置的 RPO 限制结合使用。

- 将 vRealize Network Insight 虚拟机迁移或恢复到相同的网络配置。

如果恢复站点配置为与受保护站点具有相同的网络配置，并且在相同的网络之间创建了映射，请将所有复制的 vRealize Network Insight 虚拟机配置为使用相同的 IP 启动，因为这些虚拟机是受保护节点。成功完成计划的迁移或灾难恢复后，已恢复的系统将正常运行。

- 如果恢复站点与受保护站点具有不同的网络，请勿为恢复计划指定任何 IP 自定义。在这种情况下，SRM 用于恢复设备虚拟机。要配置恢复后的网络，请按以下方式手动分配网络设置：

- 1 在所有平台节点上同时运行 `change-network-settings` 命令。

- 2 在平台 1、平台 2 和平台 3 的节点上相继运行 `update-IP-change` 命令。
- 3 在收集器节点上运行 `vrni-proxy set-platform --ip-or-fqdn <with-updated-ip-of-Platform1>`。
- 4 检查服务状态。如果平台节点上的某些服务未运行，请按照建议的顺序重新引导节点。

注 有关上述命令的详细信息，请参见《vRealize Network Insight 命令行参考指南》。

本章讨论了以下主题：

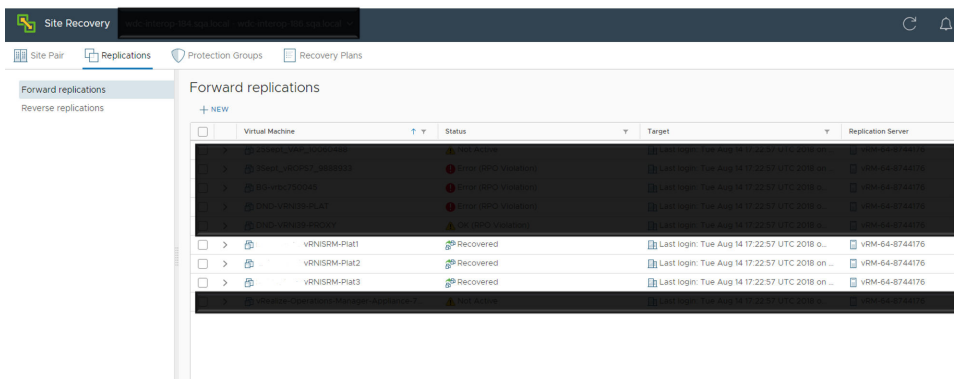
■ 灾难恢复场景示例

灾难恢复场景示例

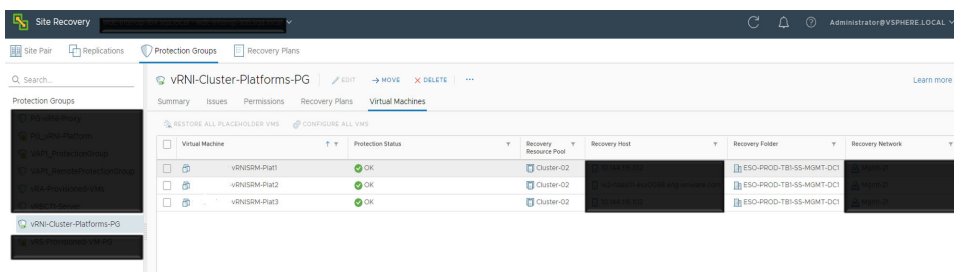
以下是 vRealize Network Insight 灾难恢复 (DR) 示例场景的步骤：

步骤

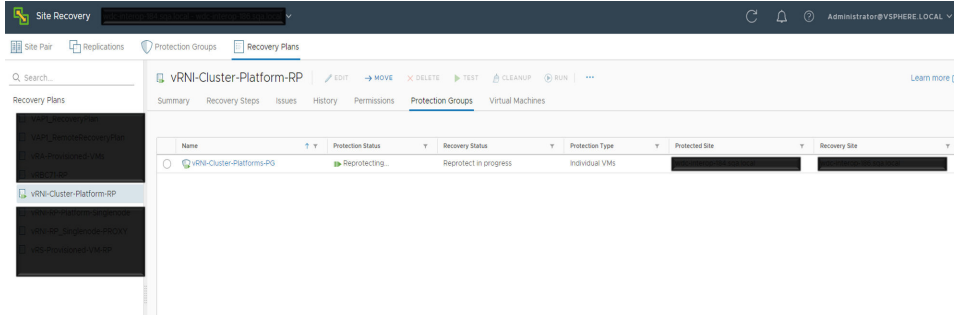
- 1 确保已在受保护站点和恢复站点中配置并启动 SRM。
- 2 为要保护的每个 vRealize Network Insight 节点配置复制。配置复制时，请为 vRealize Network Insight 实例提供足够的恢复点目标 (RPO) 时间。例如，如果是具有单个平台和收集器节点（中等大小）的 vRealize Network Insight 部署，则需要 45 分钟的 RPO。但如果是节点具有较大块大小的群集，则应提供足够的 RPO。快照时间间隔配置特定于用户环境和要求。



- 3 创建保护组。包括要在特定保护组下保护的虚拟机。



4 创建包含相应保护组的恢复计划。



5 执行测试恢复。这可以确保恢复计划按预期工作。

6 SRM 建议用户定期执行计划的迁移，以验证现有 DR 计划的完整性。

7 假设恢复站点的网络配置可强制 vRealize Network Insight 虚拟机提供新的 IP。使用不会对已恢复虚拟机进行网络更改的恢复计划恢复 vRealize Network Insight 虚拟机。在 vRealize Network Insight 中报告成功恢复虚拟机后，将新的 IP 地址手动分配给 vRealize Network Insight 节点，应用新证书，然后重新初始化群集。

8 由于目前不支持使用 SRM 进行 IPv4 自定义，因此，作为解决办法，您可以在执行 vRealize Network Insight DR 时假设不存在网络更改。

要手动分配网络设置，请执行以下操作：

- a 在所有平台节点上同时运行 `change-network-settings` 命令。
- b 在平台 1、平台 2 和平台 3 的节点上相继运行 `update-IP-change` 命令。
- c 在收集器节点上运行 `vrni-proxy set-platform --ip-or-fqdn <with-updated-ip-of-Platform1>`。
- d 检查服务状态。如果平台节点上的某些服务未运行，请按照建议的顺序重新引导节点。

本章讨论了以下主题：

- 常见的数据源错误
- 无法启用 DFW IPFIX

常见的数据源错误

添加数据源时，可能会遇到多个错误。下表列出了常见错误及其原因和解决方案。

表 19-1.

错误文本	原因	解决方案
来自数据源的响应无效 (Invalid Response from Data Source)	vRealize Network Insight 代理无法处理从数据源收到的信息，因为该信息未采用预期格式。	在一些数据提供程序中，此问题间歇性出现，在下一个轮询周期中可能会消失。如果持续出现，请联系支持部门。
无法从代理虚拟机访问数据源 (Data Source is not reachable from Proxy VM)	SSH/REST（端口 22 或 443）上的数据源 IP 地址无法从 vRealize Network Insight 代理虚拟机进行访问，或者数据源未响应。添加数据源时出现此错误。	验证从端口 22 或 443 上的 vRealize Network Insight 代理虚拟机到数据源的连接。确保数据源已启动且正在运行，并且防火墙未阻止从 vRealize Network Insight 代理虚拟机到数据源的连接。
未找到 NSX Controller (No NSX Controller found)	在“NSX Manager 数据源”页面中已选择 NSX Controller，但未安装 NSX Controller。	在 NSX Manager 上安装 NSX Controller，然后在“NSX Manager 数据源”页面上选中“NSX Controller”复选框。
数据源类型或版本不匹配 (Data source type or version mismatch)	提供的数据源 IP 地址/FQDN 不是选定的数据源类型。	验证提供的数据源 IP 地址/FQDN 是否为选定的数据源类型，以及版本是否受 vRealize Network Insight 支持
连接到数据源时出错 (Error connecting to data source)	vRealize Network Insight 代理虚拟机无法连接到数据源。添加数据源后出现此错误。	验证从端口 22 或 443 上的 vRealize Network Insight 代理虚拟机到数据源的连接。确保数据源已启动且正在运行，并且防火墙未阻止从 vRealize Network Insight 代理虚拟机到数据源的连接。
未找到 (Not found)	未找到 vRealize Network Insight 代理虚拟机。	检查是否已在 vRealize Network Insight 代理虚拟机和 vRealize Network Insight 平台虚拟机之间进行配对。

表 19-1. (续)

错误文本	原因	解决方案
特权不足, 无法启用 IPFIX (Insufficient privileges to enable IPFIX)	尝试在 vCenter 中启用 IPFIX 的用户没有以下特权: DVSwitch.Modify; DVPortgroup.Modify	为用户提供足够的特权。
IP/FQDN 无效 (IP/FQDN is invalid)	在数据源页面上提供的 IP/FQDN 无效或不存在。	提供有效的 IP/FQDN 地址。
未收到数据 (No data being received)	vRealize Network Insight 平台虚拟机未收到来自该数据源的 vRealize Network Insight 代理虚拟机的数据。	联系支持部门。
凭据无效 (Invalid credentials)	提供的凭据无效。	提供正确的凭据。
连接字符串无效 (Connection string is invalid)	在数据源页面上提供的 IP/FQDN 未采用正确格式	提供有效的 IP/FQDN 地址。
由于处理滞后, 最新数据可能不可用 (Recent data may not be available, due to processing lag)	vRealize Network Insight 平台虚拟机过载, 在处理数据时滞后。	联系支持部门。
请求已超时, 请重试 (Request timed out, please try again)	无法在指定的时间内完成请求。	重试。如果问题未修复, 请联系支持部门。
由于未知原因而失败, 请重试或联系支持部门 (Failed for unknown reason, please retry or contact support)	由于某个未知原因, 请求失败。	重试。如果问题未修复, 请联系支持部门。
需要在设备上对 SSH 启用密码身份验证 (Password authentication for SSH needs to be enabled on device)	在添加的设备上, 禁用使用密码进行 SSH 登录	在添加以便监控的设备上对 SSH 启用密码身份验证。
SNMP 连接错误 (SNMP connection error)	连接到 SNMP 端口时出错	验证是否已在目标设备上正确配置 SNMP。

无法启用 DFW IPFIX

vRealize Network Insight 不允许启用 DFW IPFIX。

问题

添加策略管理器或 VMware Cloud on AWS 源时, 如果尝试启用 DFW IPFIX 时, 您可能会看到以下错误消息:

- 无法添加新收集器 (No New collectors can be added)。
- 提供的用户没有所需的角色。只有具有云管理员角色的用户才能启用 IPFIX (Provided user does not have the required role. Only users with the following role can enable IPFIX: Cloud Administrator)。

原因

- VMware Cloud on AWS 仅支持其 DFW IPFIX 收集器配置文件的四个收集器。因此，现有配置文件已具有四个收集器时，您会看到：

无法添加新收集器 (No New collectors can be added)

消息。

Settings

Install and Support

Accounts and Data Sources

Data Management

IP Properties and Subnets >

Events >

User Management

Logs >

LDAP

Mail Server

SNMP Service

Property Templates

My Preferences

System Configuration

About

Add a New Policy Manager Account or Source of VMware Cloud on AWS

VCenter * ⓘ vcenter:sddc-35-162-64-191.vmwarevmc.com (VC VMC P... ▼)

Collector (Proxy) VM * Ni-Collector_10.153.189.42(Available Capacity: 951 VMs)
Tip: Want to increase capacity of your collector? [Click here](#)

IP Address/FQDN * nsxManager.sddc-35-162-64-191.vmwarevmc.com

CSP Refresh Token * ⓘ 6f60efe1-6d45-448f-b3d5-76e7e15c92bb

Validate Validation Successful

☐ **Enable DFW IPFIX**
Selecting this option will enable distributed firewall to send IPFIX flow record to the collector

No new collectors can be added.

Nickname *

Notes Optional

Submit Cancel

- 用户没有写入权限。只有具有云管理员角色的用户才能在 VMware Cloud on AWS 策略管理器上执行写入操作。

Settings

Install and Support

Accounts and Data Sources

Data Management

IP Properties and Subnets >

Events >

User Management

Logs >

LDAP

Mail Server

SNMP Service

Property Templates

My Preferences

System Configuration

About

Edit Account or Source

VCenter * ⓘ vcenter:sddc-34-218-191-237.vmwarevmc.com (VC VMC ... ▼)

Collector (Proxy) VM * Ni-Collector_10.153.189.42(Available Capacity: 951 VMs)
Tip: Want to increase capacity of your collector? [Click here](#)

IP Address/FQDN * nsxManager.sddc-34-218-191-237.vmwarevmc.com

CSP Refresh Token * ⓘ 232add00-f35e-4d7d-af61-d6c06aa1d9c2

Validate Validation Successful

☐ **Enable DFW IPFIX**
Selecting this option will enable distributed firewall to send IPFIX flow record to the collector

Provided user does not have the required role. Only users with the following role can enable IPFIX: Enterprise Administrator, Cloud Administrator.

Nickname * POLICY VMC M5P2

Notes Optional

Submit Cancel

解决方案

- ◆ 要添加新收集器，您必须：
 - 删除现有收集器，或者
 - 创建新的配置文件，或者
- ◆ 要避免或修复用户角色问题，请执行以下步骤之一：
 - 将**云管理员**角色分配给用户，或者
 - 以具有**云管理员**角色的用户身份登录。

使用 vRealize Network Insight 计划 将应用程序迁移到 VMware Cloud on AWS

20

使用 vRealize Network Insight，您可以评估内部部署环境，以便将应用程序迁移到 VMware Cloud on AWS 或 AWS。

步骤	过程	参考
步骤 1	设置环境	<ul style="list-style-type: none">■ 接受最终用户许可协议 (EULA)。<ul style="list-style-type: none">a 创建 VMware 用户帐户或登录到 VMware 帐户。b 更新注册表。 新用户会收到一封电子邮件以激活其帐户。c 接受 VMware 条款和 EULA。■ 下载 OVA 文件<ul style="list-style-type: none">a 登录到 VMware 产品下载页面，网址为 https://my.vmware.com/group/vmware/homeb 搜索 vRealize Network Insight。c 下载最新的 vRealize Network Insight 平台和代理 OVA 文件。■ 准备安装。<ul style="list-style-type: none">a 验证系统建议和要求。b 验证受支持的产品和版本。
步骤 2	部署	<ol style="list-style-type: none">1 部署 vRealize Network Insight 平台 OVA 文件。2 激活许可证。3 生成共享密钥4 部署 vRealize Network Insight 代理 OVA 文件。5 VMware Cloud on AWS 部署模型。
步骤 3	数据源添加	<ol style="list-style-type: none">1 登录到 vRealize Network Insight。2 添加 VMware Cloud on AWS - vCenter。3 添加 VMware Cloud on AWS - NSX Policy Manager。
步骤 4	模型应用程序	<ul style="list-style-type: none">■ 分析应用程序依赖关系<ul style="list-style-type: none">a 手动创建应用程序b 为物理 IP 创建层c 分析应用程序d VMware Cloud on AWS: 规划和微分段■ 第 16 章 建议的防火墙规则■ 第 17 章 使用搜索查询■ 看板

本章讨论了以下主题：

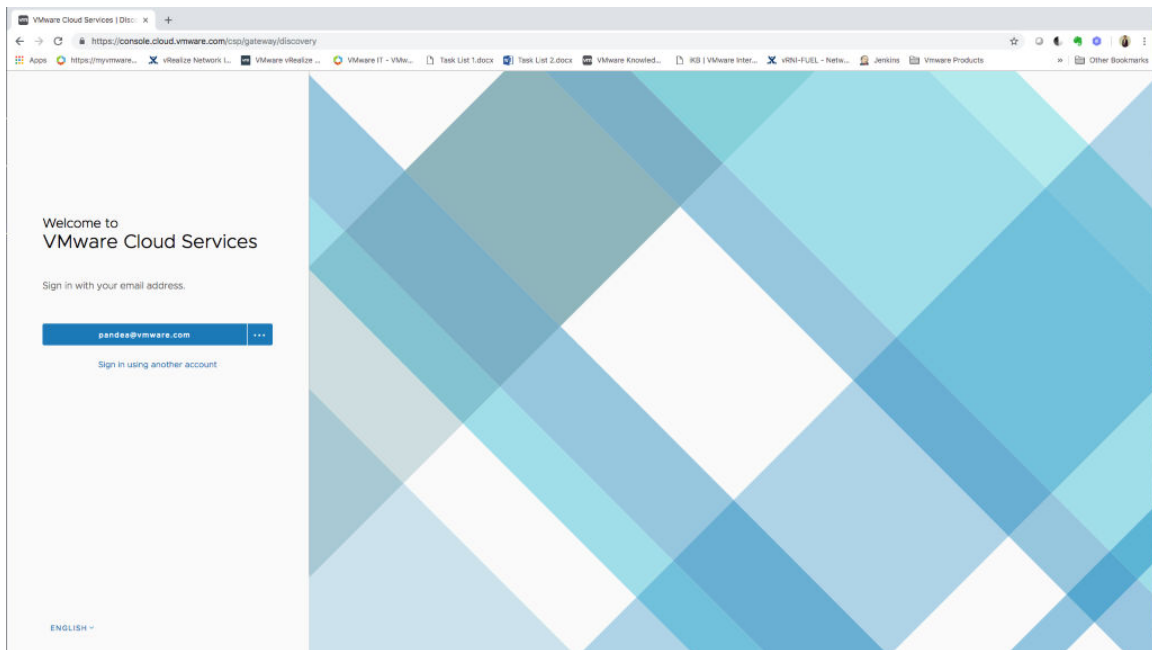
- 如何获取 NSX Manager 的 CSP 刷新令牌
- 如何获取 vCenter 凭据
- 计算网关防火墙规则

如何获取 NSX Manager 的 CSP 刷新令牌

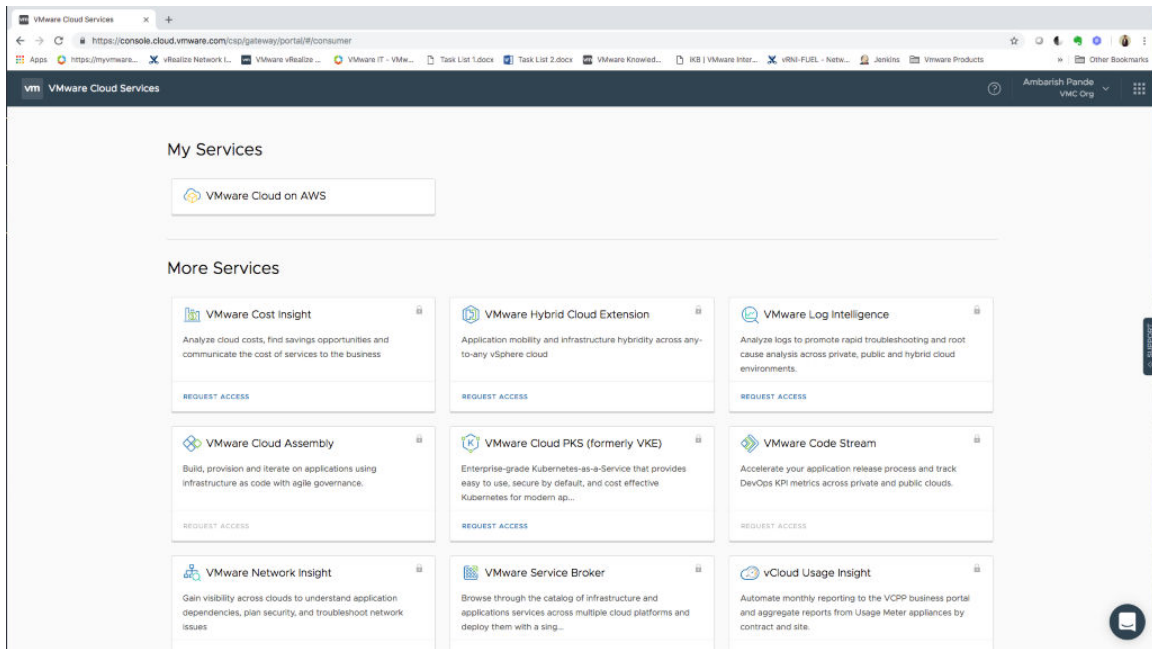
要将 VMware Cloud on AWS NSX Manager 作为数据源添加到 vRealize Network Insight 中，您需要刷新令牌。

步骤

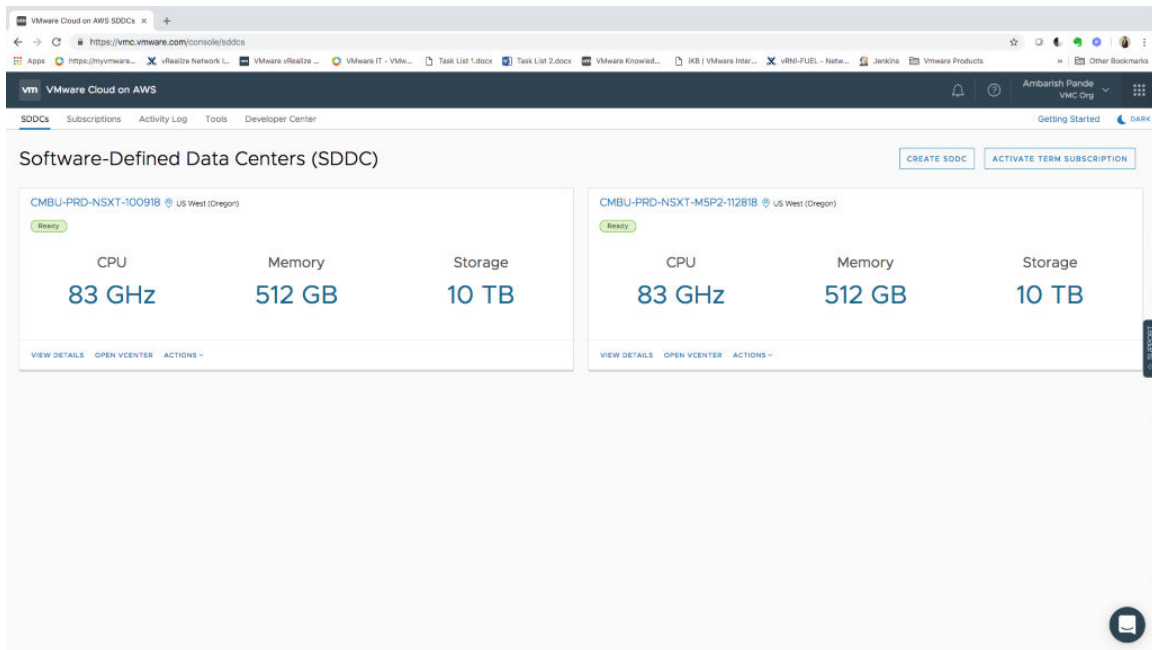
- 1 登录到 VMware Cloud Services 控制台。



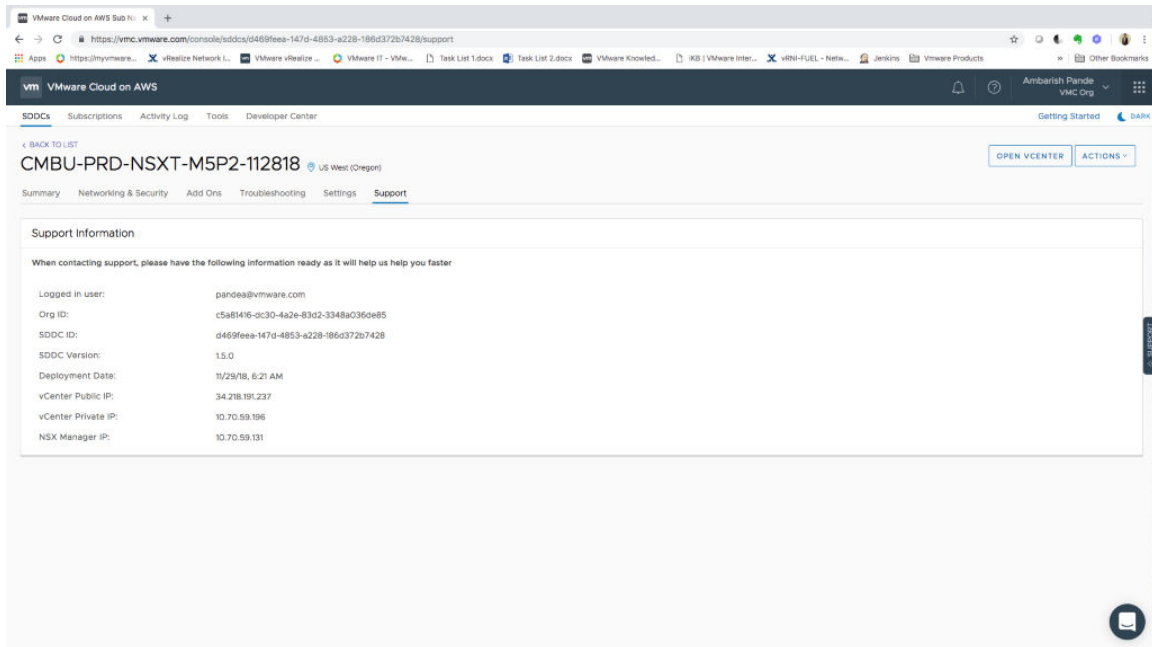
2 在“我的服务”下，单击 VMware Cloud on AWS。



3 选择所需的软件定义的数据中心 (SDDC)。



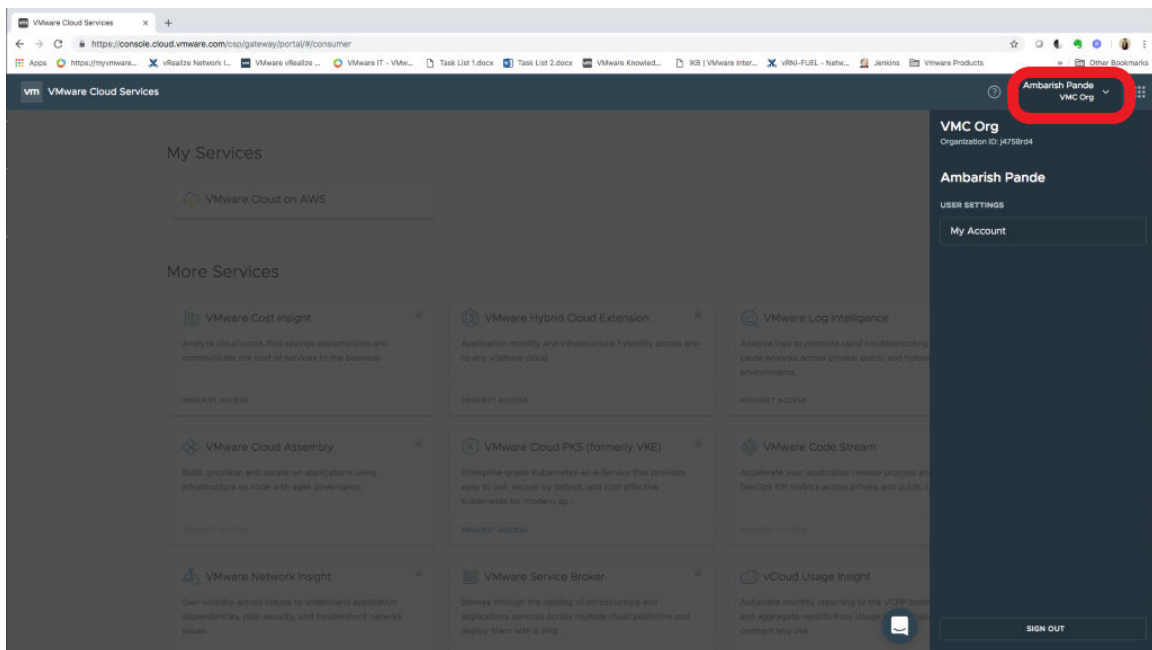
4 单击支持选项卡。



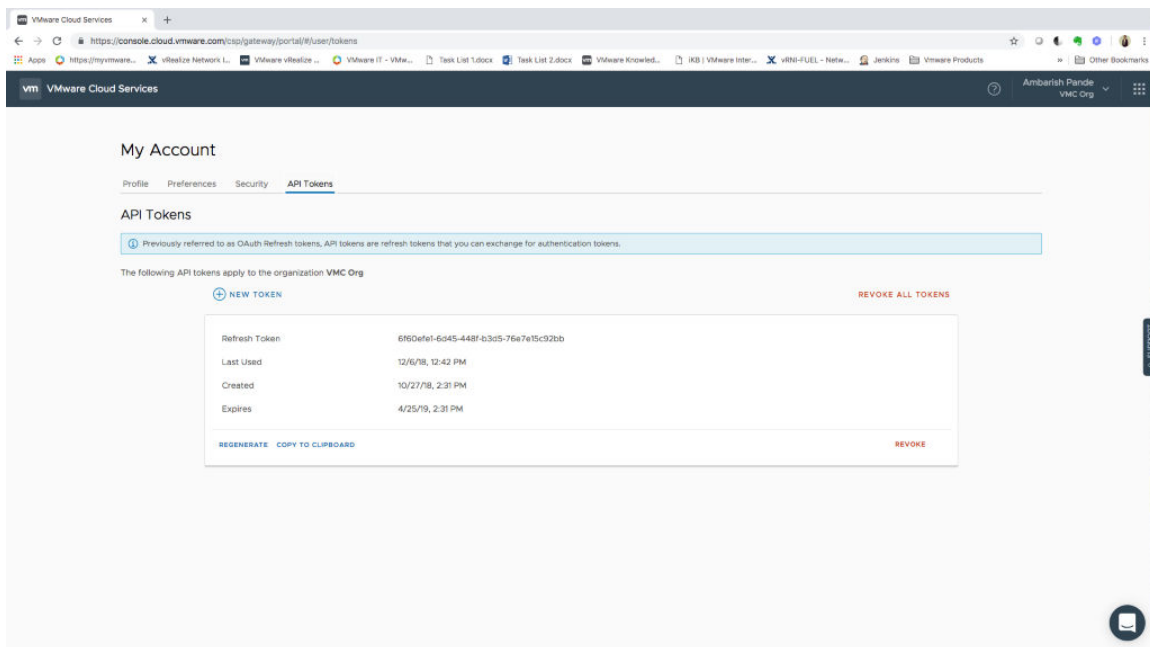
5 记下 NSX Manager IP 地址。

6 单击顶部横幅上的组织名称。

注 确保组织位于选定的 SDDC 中。



7 在 API 令牌选项卡上，复制刷新令牌。



刷新令牌的有效期为六个月。vRealize Network Insight 不跟踪令牌的生命周期。

结果

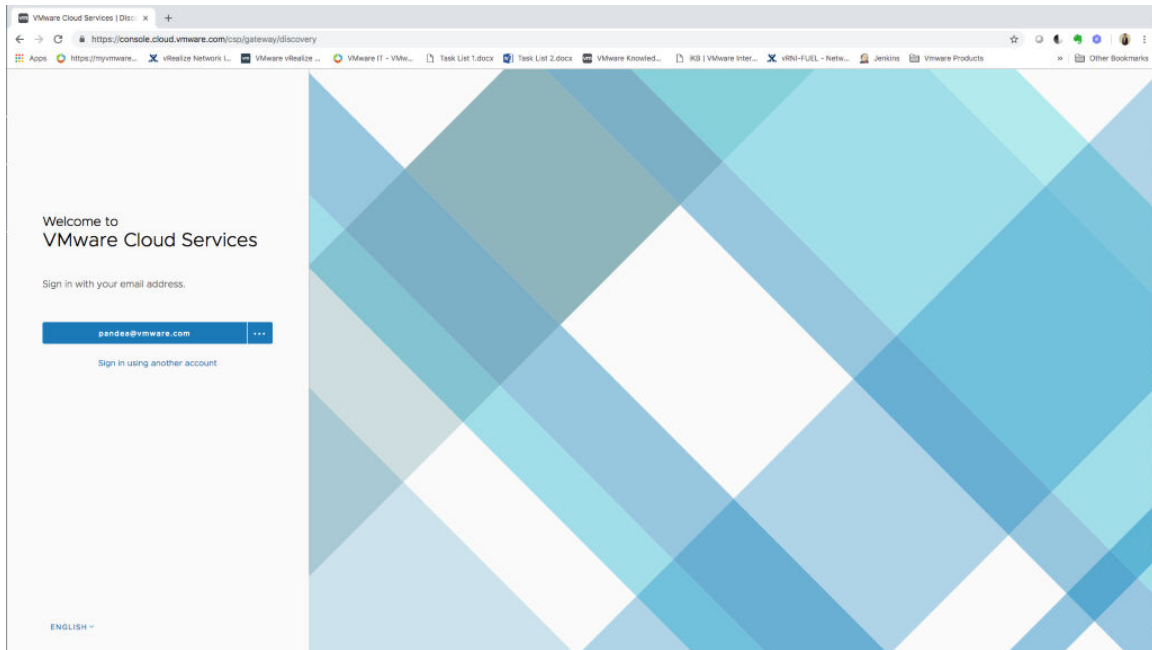
您可以使用此令牌对组织中的所有 VMware Cloud on AWS SDDC 进行身份验证。

如何获取 vCenter 凭据

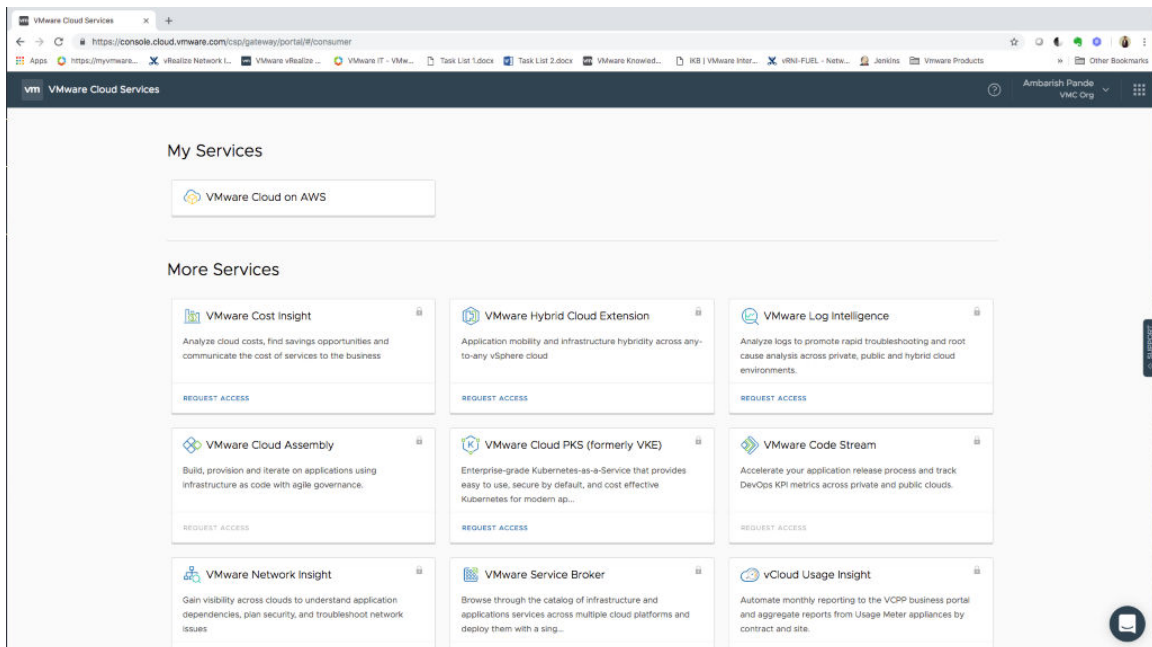
要将 vCenter 数据源添加到 vRealize Network Insight，您需要 vCenter 凭据。

步骤

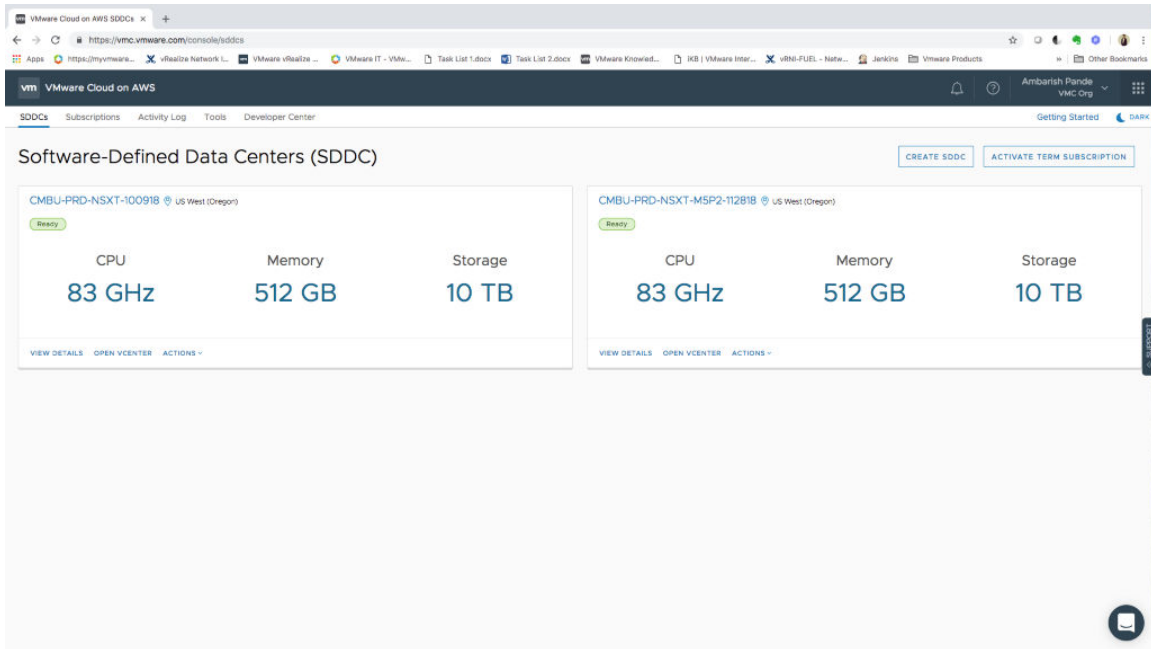
- 1 登录到 VMware Cloud Services 控制台。



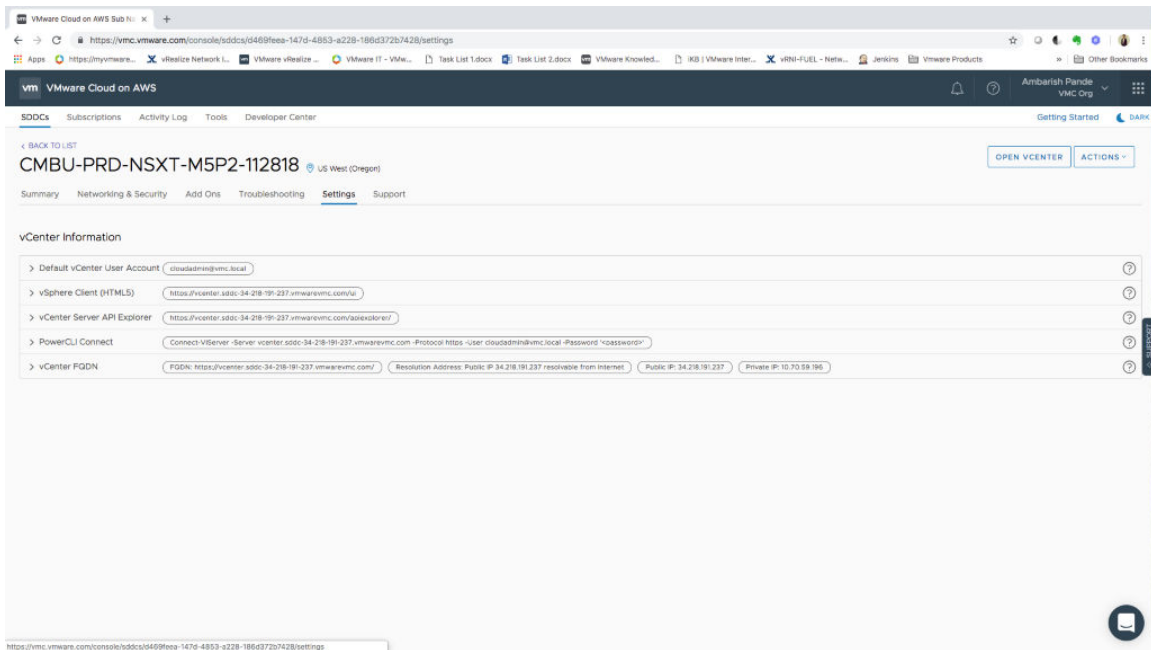
- 2 在“我的服务”下，单击 VMware Cloud on AWS。



3 选择所需的软件定义的数据中心 (SDDC)。



4 单击设置选项卡。

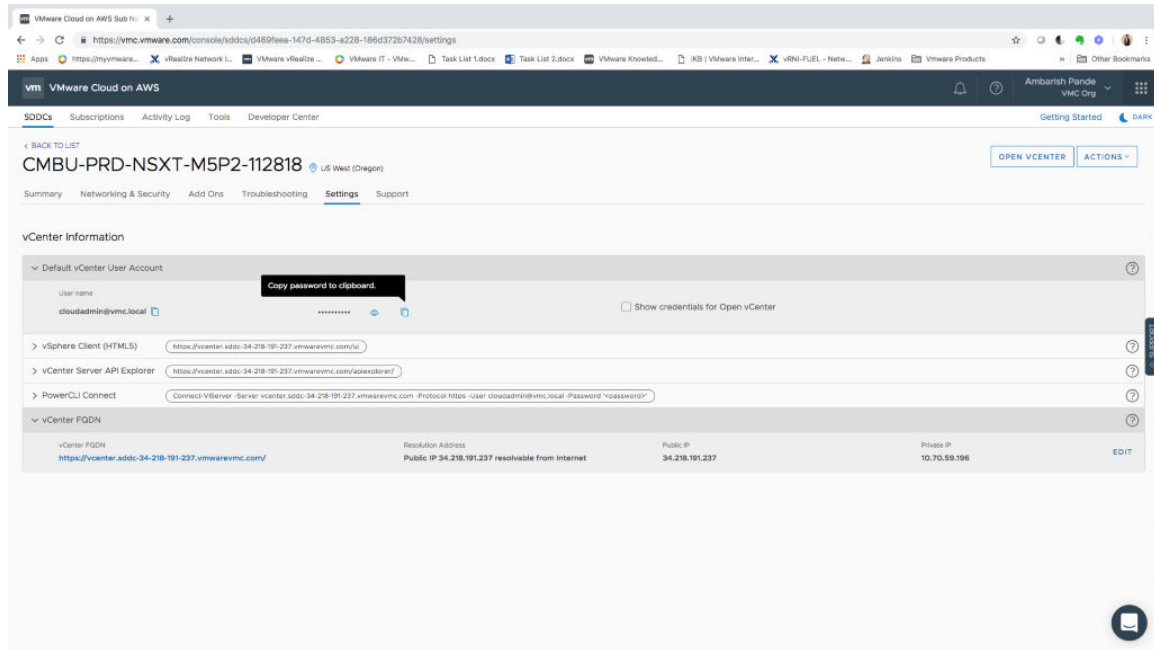


5 展开 vCenter FQDN。

记下 vCenter FQDN 详细信息。

6 展开默认 vCenter 用户帐户以获取用户名和密码。

复制密码并记下用户名。



计算网关防火墙规则

与 vRealize Network Insight 平台通信时，收集器要求 HTTPS 端口 443 对出站流量打开。

收集器通过防火墙访问以下 VMware 托管的 URL：

- *.vmwareidentity.com
- gaz.csp-vidm-prod.com
- *.vmware.com
- *.ni-onsaas.com

此外，应允许 NTP 和 DNS 流量，以便 vRealize Network Insight 或 vRealize Network Insight 收集器正常运行。

使用以下详细信息创建防火墙规则：

- 名称：一个适当的描述性名称
- 源：包含收集器 IP 地址的 VMware Cloud on AWS 组的名称。
- 目标：选择任意
- 服务 - 选择 HTTPS、DNS、DNS-UDP、NTP、ICMP
- 操作 - 允许
- 应用对象 - Internet 接口
- 日志记录 - 根据需要启用日志记录。