

# 安装 vRealize Network Insight

VMware vRealize Network Insight 5.2

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](http://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](http://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](http://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](http://www.vmware.com/cn)

版权所有 © 2020 VMware, Inc. 保留所有权利。 版权和商标信息

# 目录

关于《vRealize Network Insight 安装指南》	5
-----------------------------------	---

## 1 安装准备工作 6

系统建议和要求	6
特权	9
系统端口	10
网络通信端口	14
受支持的产品和版本	16

## 2 安装 vRealize Network Insight 19

安装工作流	20
部署 vRealize Network Insight 平台 OVA	21
使用 vSphere Web Client 进行部署	21
使用 vSphere Windows 本机客户端进行部署	23
激活许可证	24
生成共享密钥	24
设置 Network Insight 收集器 (OVA)	25
使用 vSphere Web Client 的部署	25
使用 vSphere Windows 本机客户端进行部署	26
对于 VMware SD-WAN 在 AWS 中设置 Network Insight 收集器 (AMI)	27
在现有设置中部署其他收集器	29

## 3 使用评估许可证访问 vRealize Network Insight 30

添加 vCenter Server	30
分析流量流	31
生成报告	32

## 4 计划纵向扩展部署 33

计划纵向扩展平台群集	33
计划纵向扩展收集器	34
增加设置的块大小	35

## 5 升级 vRealize Network Insight 36

联机升级	37
一键式脱机升级	39
CLI 升级	41

## 6 卸载 vRealize Network Insight 44

在 vCenter 中启用 Netflow 时移除收集器 IP 44

在 NSX 中启用 Netflow 时移除收集器 IP 45

# 关于《vRealize Network Insight 安装指南》

《vRealize Network Insight 安装指南》面向负责安装 vRealize Network Insight 的管理员或专业人员。

## 目标读者

本信息面向负责安装 vRealize Network Insight 的管理员或专业人员。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。

# 安装准备工作

# 1

在安装 vRealize Network Insight 之前，请准备部署环境以满足系统要求。

本章讨论了以下主题：

- 系统建议和要求
- 受支持的产品和版本

## 系统建议和要求

为了获得最佳性能，必须满足最低部署建议。

## 平台部署建议

表 1-1. 平台块大小规格

块大小	所需内核数 - 2.1 GHz CPU	所需内核数 - 2.3 GHz CPU	所需内核数 - 2.6 GHz CPU	RAM	磁盘
中型	10	9	8	32 GB	1 TB
大型	15	14	12	48 GB	1 TB
超大型	20	18	16	64 GB	2 TB

### 注

- 每个节点的预留 CPU 速度和 RAM 必须为以上指定值的 100%。
- 要使设置与所有规格相匹配，可能需要添加资源（RAM、磁盘、CPU）。请参见 <https://kb.vmware.com/s/article/53550> 和增加设置的块大小。

表 1-2. 非群集部署 - 最大容量

块大小	虚拟机数 (以千为单位)	每日流数 (以百万为单位)	总流数 (以百万为单位)	流规划 (以百万为单位)
中型	4K	1M	4M	2M
大型	6K	2M	8M	4M

表 1-3. 非群集部署 - 最大容量（对于 VMware SD-WAN）

块大小	Edge 数 (以千为单位)	每日流数 (以百万为单位)	总流数 (以百万为单位)
中型	2K	1M	4M
大型	2K	2M	8M

**注**

- 虚拟机计数也包括 vCenter 上的模板。
- 总流数是指保留期内系统可以存储的最大流计数。
- 流规划是指系统可以对其执行安全计划的总流数。

表 1-4. 群集部署 - 最大容量

块大小	群集大小	虚拟机数 (以千为单位)	每日流数 (以百万为单位)	总流数 (以百万为单位)	流规划 (以百万为单位)	VMware SD-WAN 的 Edge 数 (以千为单位)
大型	3	10K	2M	8M	4M	4K
超大型	3	18K	6M	24M	4M	6K
超大型	5	30K	10M	40M	4M	10K
超大型	10	100K	15M	55M	4M	10K

**注**

- 虚拟机计数也包括 vCenter 上的模板。
- 群集大小是指群集中的总节点数。
- 总流数是指保留期内系统中的流计数。
- 用于确定总流数的查询为 `count of flows in last 31 days`，假定保留期为 31 天。
- 流规划是指系统可以对其执行安全计划的总流数。

## 收集器部署建议

表 1-5. 收集器块大小规格

块大小	2.1 GHz CPU 所需的内核数	2.3 GHz CPU 所需的内核数	2.6 GHz CPU 所需的内核数	RAM	磁盘
中型	5	5	4	12 GB	200 GB
大型	10	9	8	16 GB	200 GB
超大型	10	9	8	24 GB	200 GB

**注** 每个节点的预留 CPU 速度和 RAM 必须为以上指定值的 100%。

表 1-6. 收集器部署 - 最大容量

收集器大小	虚拟机数 (以千为单位)	每日流数 (以百万为单位)	4 天内的流计数 (以百万为单位)	VMware SD-WAN 的 Edge 数 (以千为单位)
中型	4K	2.5M	3.25M	4K
大型	10K	5M	6.5M	6K
超大型	20K	10M	13M	10K

**注**

- 虚拟机计数也包括 vCenter 上的模板。
- 对于具有多个收集器的单个部署，对各收集器的总流数限制取决于平台的容量。

## 其他要求和注意事项

- 平台节点之间的最大时间偏差必须小于 30 秒。
- NTP 服务的可用性对系统操作至关重要。请确保在 NTP 服务不可用时不重新引导平台节点或收集器节点。
- 当平台上的其他进程完全使用现有计算资源时，vRealize Network Insight 会崩溃且不会自动恢复。如果服务无法恢复，请重新引导平台节点。
- 如果平台节点和升级服务器之间的网络延迟大于 500 毫秒，则 vRealize Network Insight 升级可能会遇到错误。因此，网络延迟必须小于 500 毫秒。
- 为获得最佳性能，建议磁盘延迟最长为 5 毫秒。如果磁盘延迟大于 5 毫秒，则系统性能会下降。
- 磁盘 IOPS 建议为 7500。

## 支持的 Web 浏览器

- Google Chrome: 最新的两个版本。
- Mozilla Firefox: 最新的两个版本。



## 支持高可用性建议

可以自定义 vSphere HA 选项以启用 vSphere High Availability。

- 主机故障 - 重新启动虚拟机
- 主机隔离 - 已禁用
- 客户机没有检测信号 - 已禁用

## 特权

### 数据源所需的特权

- 配置和使用 IPFIX 所需的特权
  - 具有特权的 vCenter Server 凭据：
    - 分布式交换机：修改
    - dvPort 组：修改
  - 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

要了解有关 vCenter 中角色的更多信息，请参见《vSphere 安全性》指南中的“使用角色分配特权”部分。

- NSX Manager 数据提供程序所需的特权
  - NSX Manager 数据提供程序需要企业角色。
  - 如果启用了 Central CLI，则 NSX Manager 数据提供程序需要 `system admin` 凭据。
- 在 Cisco 交换机上收集衡量指标所需的用户特权
  - vRealize Network Insight 能够通过 SNMP 从 Cisco 交换机收集衡量指标数据，以及通过 SSH 收集配置数据。Cisco 交换机 UCS 平台要求同时使用 SSH 和 API 进行收集。

表 1-7.

数据类型	用户特权
配置数据	只读
衡量指标数据	SNMP 只读

表 1-7. (续)

数据类型	用户特权
	SNMPv2 只读 SNMP 社区
	SNMPv3 只读

## 系统端口

以下是 vRealize Network Insight 入站通信所需的端口列表：

### 用于平台集群设置的端口

表 1-8.

源	目标	端口	协议	用途	敏感	SSL	身份验证
SSH 客户端	平台	22	SSH	CLI 或主机访问	否	是	基于用户/密码或基于 SSH 密钥的身份验证
客户端 Web 浏览器和 vRNI 收集器	平台	443	HTTPS	UI/API 访问以及 vRNI 收集器进行通信	是	是	使用基于 2048b RSA 密钥的 SHA2 证书（或用户配置的自定义证书）加密的 SSL 通道。对于通过此通道从收集器传输到平台的消息，还进一步使用 HMAC 进行加密。
平台	平台	2181	HTTP	其他节点上的 zookeeper 服务器之间的通信（如果为集群）。存储元数据信息（znode 数据）	否	否	
平台	平台	2888	HTTP	用于连接到 zookeeper 主节点	否	否	
平台	平台	3000	HTTP	用于发送电子邮件通知	是	否	
平台	平台	3888	HTTP	用于选举 zookeeper 主节点	是	否	

表 1-8. (续)

源	目标	端口	协议	用途	敏感	SSL	身份验证
平台	平台	5432	JDBC	存储虚拟机配置数据和基础架构元数据	是	否	
平台	平台	8020	TCP/RPC	其他名称节点与数据节点之间的通信	是	否	
平台	平台	8025	HTTP	节点管理器使用此端口连接到资源管理器	否	否	
平台	平台	8030	HTTP	由资源管理器用于调度任务	否	否	
平台	平台	8032	HTTP	RM 中应用程序管理器接口的地址	否	否	
平台	平台	8033	HTTP	RM 管理接口的地址	否	否	
平台	平台	8042	HTTP	节点管理器 Web 应用程序地址	否	否	
平台	平台	8080	HTTP	处理 UI 请求	是	否	
平台	平台	8088	HTTP	资源管理器 Web 应用程序的 HTTP 地址	否	否	
平台	平台	8480	TCP/RPC	JournalNode HTTP 服务器	否	否	
平台	平台	8485	TCP/RPC	HDFS 共享编辑数据目录	否	否	
平台	平台	9090	HTTP	处理收集器发出的请求并将命令发送到收集器	是	是（通过 nginx 保护）	
平台	平台	9092	基于 TCP 的二进制	其他代理进行通信所用的端口	是	否	
平台	平台	9200-9300	HTTP	处理搜索请求。ES 使用端口范围侦听，如果 9200 已使用，则使用下一个可用端口。	是	否	

表 1-8. (续)

源	目标	端口	协议	用途	敏感	SSL	身份验证
平台	平台	9300	HTTP	处理搜索请求。ES 使用端口范围侦听，如果 9200 已使用，则使用下一个可用端口。	是	否	
平台	平台	30000:65535	TCP	由各种进程用来与其他进程进行 TCP 连接的临时端口范围	否	否	
平台	平台	60000	IPC	用于其他 hbase 主服务器和区域服务器之间的通信	是	否	
平台	平台	60010	HTTP	用于 hbase Web UI	否	否	
平台	平台	60020	IPC	hbase 主服务器和区域服务器之间的通信	是	否	
平台	平台	4500-4510	TCP	不同平台上运行的 Foundation 数据库服务器之间的通信	是	否	

## 用于单平台设置的端口

表 1-9.

源	目标	端口	协议	用途	敏感	SSL	身份验证
SSH 客户端	平台	22	SSH	CLI 或主机访问	否	是	基于用户/密码或基于 SSH 密钥的身份验证
客户端 Web 浏览器和 vRNI 收集器	平台	443	HTTPS	UI/API 访问以及 vRNI 收集器进行通信	是	是	使用基于 2048b RSA 密钥的 SHA2 证书（或用户配置的自定义证书）加密的 SSL 通道。对于通过此通道从收集器传输到平台的消息，还进一步使用 HMAC 进行加密。

## 用于收集器服务器的端口

表 1-10.

源	目标	端口	协议	用途	敏感	SSL	身份验证
SSH 客户端	收集器	22	SSH	CLI 或主机访问	否	是	基于用户/密码或基于 SSH 密钥的身份验证
vRNI 收集器	平台	443	HTTPS	与平台的主通信通道	是	是	使用基于 2048b RSA 密钥的 SHA2 证书（或用户配置的自定义证书）加密的 SSL 通道。对于通过此通道从收集器传输到平台的消息，还进一步使用 HMAC 进行加密。
流转发器	收集器	UDP 2055	NetFlow/IPFIX	来自目标的流将推送到此端口	是	否	
流转发器	收集器	UDP 6343	sFlow	来自目标的流将推送到此端口	是	否	

表 1-10. (续)

源	目标	端口	协议	用途	敏感	SSL	身份验证
ESXi 主机	收集器	1991	TCP	收集虚拟基础架构的延迟测量，例如： vNIC 到 pNIC、VTEP 到 VTEP、TEP 到 TEP 等的延迟。	否	否	
Dell OS10	收集器	50000	GRPC	从 Dell OS10 设备接收缓冲区统计信息遥测信息	否	否	

## 网络通信端口

下表列出了在 vRealize Network Insight 中用于网络通信的端口和协议。

还可以从 <https://ports.vmware.com/home/vRealize-Network-Insight> 查看端口列表。

表 1-11.

用途	源	目标	端口	协议
vRealize Network Insight 虚拟机之间的通信	收集器	平台 <small>注 必须为所有平台启用该端口。</small>	443	HTTPS
需要访问 Internet 的服务	平台和收集器	svc.ni.vmware.com support2.ni.vmware.com reg.ni.vmware.com	443	HTTPS
已配置的其他服务的通信	平台	LDAP 服务器	389、636	LDAP 和 LDAPS
		SNMP 服务器	可配置	SNMP
	平台和收集器	DNS 服务器	53	UDP
		Syslog 服务器	可配置	
	ESXi 主机	收集器	2055	
与作为数据源的 AWS 的通信	收集器	AWS(*.amazonaws.com)	443	HTTPS
	浏览器	遥测 URL <a href="https://vcsa.vmware.com">https://vcsa.vmware.com</a>	433	HTTPS

表 1-11. (续)

用途	源	目标	端口	协议
与数据中心内其他数据源的通信	收集器	Arista 交换机	161 和 22	SNMP 和 SSH
		Azure	443	HTTPS
		Brocade 交换机	161 和 22	SNMP 和 SSH
		Check Point 防火墙	443	HTTPS
		Cisco Nexus	161 和 22	SNMP 和 SSH
		Cisco UCS (Unified Computing System)	161、22 和 443	SNMP、SSH 和 HTTPS
		Cisco Catalyst 交换机	161 和 22	SNMP 和 SSH
		Cisco ACI 交换机	161	SNMP
		Cisco APIC 控制器	161 和 443	HTTPS 和 SNMP
		Dell 交换机	161 和 22	SNMP 和 SSH
		Dell OS10	50000	TCP
		VeloCloud	443、2055	HTTPS
		HP	22	SSH
		Juniper 交换机	161 和 22	SNMP 和 SSH
		Palo Alto 网络	443	HTTPS
		VMware vSphere	443	HTTPS
		VMware NSX - V (所有组件)	22 和 443	SSH 和 HTTPS
		NSX-T Manager	443	TCP
		VMware PKS API 服务器	8443 和 9021	TCP
		Kubernetes API 服务器	8443	TCP
		vRealize Log Insight	443	HTTPS
		Fortinet FortiManager	443	HTTPS

## 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	请参见用户指南中的“添加数据源”部分。
Arista 交换机	7050TX、7250QX、7050QX-32S、7280SE-72	SSH、SNMP	请参见用户指南中的“添加数据源”部分。
Azure 订阅	不适用	HTTPS	请参见用户指南中的“添加数据源”部分。
Brocade 交换机	VDX 6740、VDX 6940、MLX、MLXe	SSH、SNMP	请参见用户指南中的“添加数据源”部分。
Check Point 防火墙	Check Point R80、R80.10、R80.20、R80.30	HTTPS、SSH	请参见用户指南中的“添加数据源”部分。
Cisco ACI	3.2	HTTPS (到 APIC 控制器) SNMP (到 APIC 控制器和 ACI 交换机)	请参见用户指南中的“添加数据源”部分。
Cisco ASA	运行操作系统 9.4 的 X 系列	SSH、SNMP	请参见用户指南中的“添加数据源”部分。
Cisco Catalyst	3000、3750、4500、6000、6500	SSH、SNMP	请参见用户指南中的“添加数据源”部分。
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"> <li>■ 至少能够访问所有 ADOM 和策略软件包的受限用户角色。</li> <li>■ 已从命令行界面 (CLI) 启用 <b>rpc-permit read</b> 访问权限。</li> </ul>
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



数据源	版本/型号	连接协议	权限/特权
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"> <li>■ 权限类型 - DNS</li> <li>■ 资源 - A 记录、DNS 区域、DNS 视图</li> </ul>
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
Kubernetes	<ul style="list-style-type: none"> <li>■ NSX-T 2.3.1 上的 1.12</li> <li>■ NSX-T 2.3.2 上的 1.12</li> <li>■ NSX-T 2.3.2 上的 1.13</li> </ul>	HTTPS	用户必须具有群集管理员角色且具有读取权限。
OpenShift	3.1.1	HTTPS	请参见用户指南中的“添加数据源”部分。
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"> <li>■ 超级用户</li> <li>■ 标准管理员</li> <li>■ 客户支持人员</li> </ul>
VMC on AWS - vCenter	M8 及更高版本 <a href="#">注</a> 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"> <li>■ 云管理员：添加数据源并启用 IPFIX。</li> </ul>
VMC on AWS - NSX Manager	M8 及更高版本 <a href="#">注</a> 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"> <li>■ 组织成员.管理员：添加数据源并启用 IPFIX。</li> <li>■ 组织成员.管理员.NSX Cloud 管理员：添加数据源并启用 IPFIX。</li> <li>■ 组织成员.VMware Cloud on AWS（所有角色）：添加数据源并启用 IPFIX。</li> <li>■ 组织成员.NSX Cloud 审核员：添加数据源。</li> </ul>
VMware Identity Manager	3.3 及更高版本	HTTPS	用户必须具有管理员角色。

数据源	版本/型号	连接协议	权限/特权
VMware PKS	<a href="#">支持的版本</a>		用户必须具有群集管理员角色权限 - pks.clusters.admin。
VMware NSX Manager (VMware NSX-V)	<a href="#">支持的版本</a>	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 <a href="#">支持的版本</a>	HTTPS	只读用户
VMware vRealize Log Insight	<a href="#">支持的版本</a>	HTTPS	具有安装、配置和管理内容包权限的 API 用户
VMware vSphere	<a href="#">支持的版本</a> 对于 IPFIX，所需的 VMware ESXi 版本为： <ul style="list-style-type: none"> <li>■ 5.5 Update 2（内部版本 2068190）及更高版本</li> <li>■ 6.0 Update 1b（内部版本 3380124）及更高版本</li> <li>■ VMware VDS 5.5 及更高版本</li> </ul> <p><b>注</b> 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。</p>	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

## 注

- Cisco ASA、ACI、Catalyst 和 Nexus 设备支持的操作系统为 iOS/NX-OS；Cisco UCS 支持的操作系统为 UCSM 版本。
- Arista 支持的操作系统为 Arista EOS。

# 安装 vRealize Network Insight

## 2

可以使用 vSphere Web Client 或 vSphere Window 本机客户端部署 vRealize Network Insight。

**注** 成功部署 vRealize Network Insight 平台 OVA 后，请验证是否在 vCenter Server 上设置了给定的静态 IP。

要在单一窗口内自动执行安装、配置、升级、修补、配置管理、偏差修复和运行状况，可以使用 vRealize Suite Lifecycle Manager。如果您是新用户，请单击此处安装 [vRealize Suite Lifecycle Manager](#)。这样，云管理员资源的 IT 经理能够重点关注关键业务计划，同时缩短了价值实现时间 (TTV) 并且增强了可靠性和一致性。

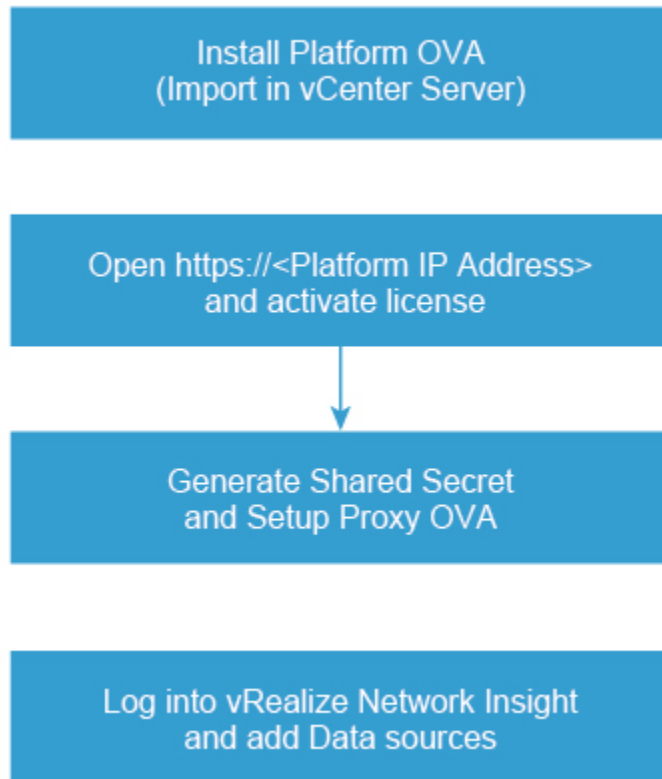
还可以使用 vRealize Suite Lifecycle Manager 安装和升级 vRealize Network Insight。有关详细信息，请参见《[vRealize Suite Lifecycle Manager 安装、升级和管理指南](#)》。

本章讨论了以下主题：

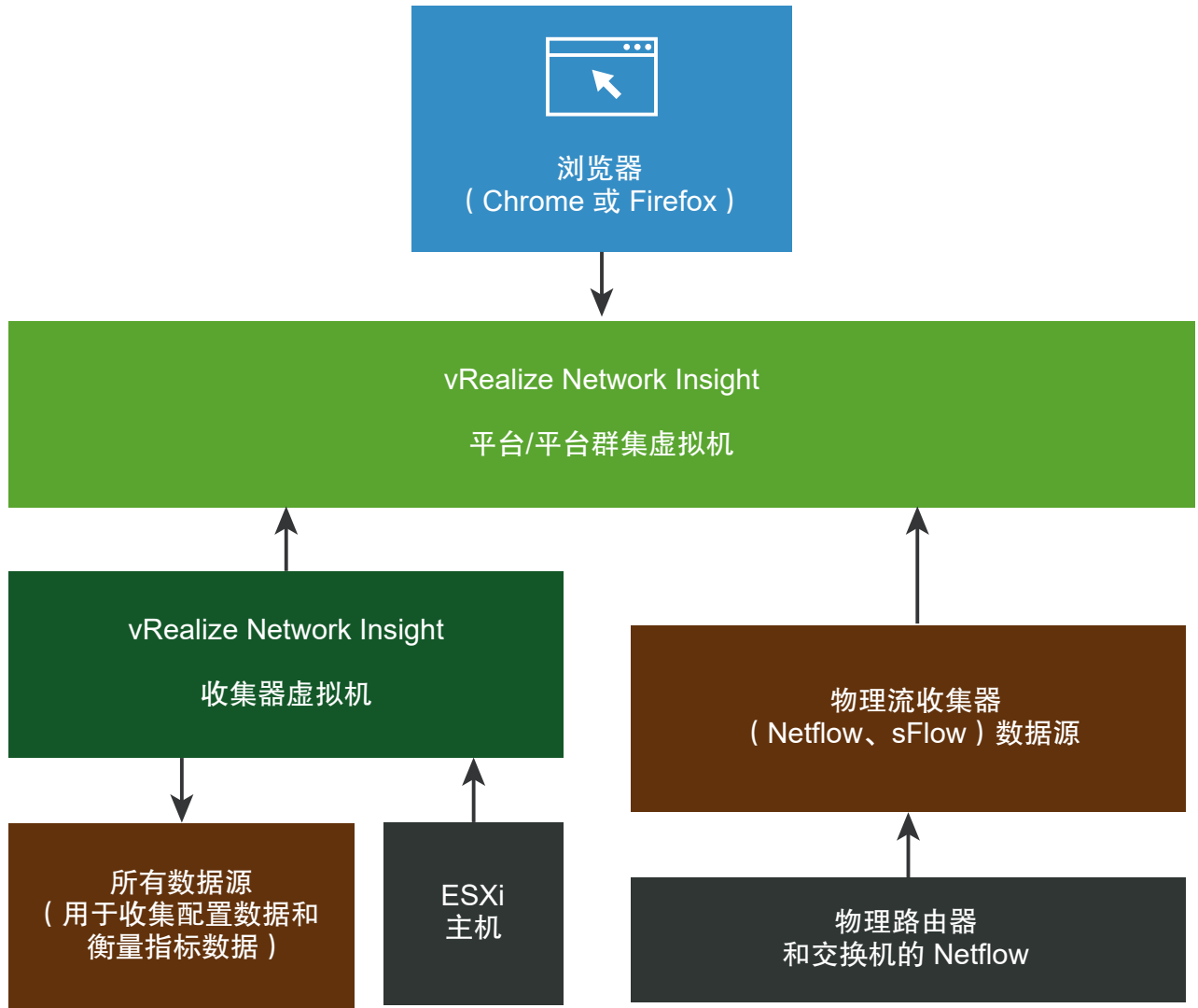
- 安装 workflows
- 部署 vRealize Network Insight 平台 OVA
- 激活许可证
- 生成共享密钥
- 设置 Network Insight 收集器 (OVA)
- 对于 VMware SD-WAN 在 AWS 中设置 Network Insight 收集器 (AMI)
- 在现有设置中部署其他收集器

## 安装 workflow

要安装 vRealize Network Insight，请安装平台 OVA、激活许可证、生成共享密钥并设置收集器 OVA。



经过简化的 vRealize Network Insight 部署图如下所示：



## 部署 vRealize Network Insight 平台 OVA

可以将 vRealize Network Insight 平台 OVA 导入到 vCenter Server 中。

**注** 不支持在 VMC SDDC 上部署 vRealize Network Insight 平台 OVA。

### 使用 vSphere Web Client 进行部署

可以使用 vSphere Web Client 部署 vRealize Network Insight。

#### 步骤

- 1 右键单击要安装设备的**数据中心**，然后选择**部署 OVF 模板**。
- 2 输入 URL 以下载并安装 OVA 软件包，或者通过浏览选择 OVA 软件包的源位置。
- 3 输入 OVA 名称。为部署选择目标文件夹。

- 4 选择要运行已部署模板的主机、群集或资源池。
- 5 验证 OVF 模板详细信息。
- 6 阅读最终用户许可协议，然后单击**接受**。
- 7 选择部署配置。单击**下一步**。
- 8 选择用于存储已部署的模板文件的位置。选择**精简置备**作为虚拟磁盘格式。选择要在其中存储文件的数据存储或数据存储群集。单击**下一步**。
- 9 选择已部署虚拟机将使用的网络。

所选网络应允许设备访问 Internet 以获取支持和执行升级。

- 10 要为部署自定义模板，必须使用虚拟机控制台手动配置设备。单击**下一步**。
- 11 验证配置详细信息，然后单击**完成**。
- 12 **增加设置的块大小** 以满足系统建议和要求。
- 13 安装平台后，启动虚拟机并启动控制台。
- 14 使用您在屏幕上看到的控制台凭据登录，然后运行 `setup` 命令。
- 15 为 `support` 登录创建密码并更改 `consoleuser` 的密码。

---

#### 注

- 密码必须至少包含 6 个字符。不允许使用单引号 (')。
  - 必须定期更改 `support` 和 `consoleuser` 密码，以符合您的组织策略。
- 

- 16 输入以下详细信息以配置网络：
  - a **IPv4 地址**：第二个保留的静态 IP 地址
  - b **网络掩码**：上述静态 IP 的子网掩码
  - c **默认网关**：网络的默认网关
  - d **DNS**：环境的 DNS 服务器

---

**注** 对于多个 DNS 服务器，请确保用空格将其分隔。

---

- e **域搜索列表**：需要为 DNS 查找附加的域
  - f 输入 `y` 以保存配置。
- 17 输入 NTP 服务器，并确保可以从虚拟机进行访问。如果 NTP 时间不同步，则服务将无法启动。

---

**注** 对于多个 NTP 服务器，请确保用逗号将其分隔。

---

- 18 （可选）要配置 Web 代理，请输入 `y`。
- 19 验证所有服务。
- 20 根据您的设置要求增加磁盘空间。请参见 <https://kb.vmware.com/s/article/53550>。

## 使用 vSphere Windows 本机客户端进行部署

可以使用 vSphere Windows 本机客户端部署 vRealize Network Insight。

**注** vRealize Network Insight 5.2 是支持使用 vSphere Windows 本机客户端部署 OVA 的最后一个版本。从 5.3 版本开始，您可以继续使用 vSphere Web Client 部署 vRealize Network Insight OVA。

### 步骤

- 1 单击**文件 > 部署 OVF 模板**。
- 2 输入 URL 以从 Internet 下载并安装 OVA 软件包，或者浏览以选择计算机上 OVA 软件包的源位置。
- 3 单击**下一步**，然后验证 OVF 模板详细信息。
- 4 阅读最终用户许可协议，然后单击**接受**。
- 5 为已部署模板提供名称并指定位置。单击**下一步**。
- 6 选择**部署配置**。
- 7 选择要运行已部署模板的**主机/集群**。
- 8 选择要在其中部署此模板的**资源池**。
- 9 为虚拟机文件选择一个目标存储。单击**下一步**。
- 10 指定存储虚拟磁盘要采用的格式。选择**精简置备**作为虚拟磁盘格式。单击**下一步**。
- 11 指定已部署模板应使用的网络。将网络从 OVA 映射到清单。
- 12 为部署自定义模板。提供在载入页面上生成的共享密钥。必须使用虚拟机控制台手动配置设备。单击**下一步**。
- 13 验证所有配置数据。选中**部署后打开电源**。单击**完成**。
- 14 增加设置的块大小，以符合系统建议和要求。
- 15 安装收集器 OVA 后，启动虚拟机并启动控制台。
- 16 使用您在屏幕上看到的控制台凭据登录，然后运行 `setup` 命令。
- 17 为 `support` 登录创建密码并更改 `consoleuser` 的密码。

### 注

- 密码必须至少包含 6 个字符。不允许使用单引号 (')。
- 必须定期更改 `support` 和 `consoleuser` 密码，以符合您的组织策略。

- 18 输入以下详细信息以配置网络：
  - a **IPv4 地址**：第二个保留的静态 IP 地址
  - b **网络掩码**：上述静态 IP 的子网掩码
  - c **默认网关**：网络的默认网关

- d **DNS:** 环境的 DNS 服务器

---

**注** 对于多个 DNS 服务器，请确保用空格将其分隔。

---

- e **域搜索列表:** 需要为 dns lookup 附加的域。

- f 输入 y 以保存配置。

- 19 输入 NTP 服务器，并确保可以从虚拟机进行访问。如果 NTP 时间不同步，则服务将无法启动。

---

**注** 对于多个 NTP 服务器，请确保用逗号将其分隔。

---

- 20 (可选) 要配置 Web 代理，请输入 y。

- 21 验证所有服务。

- 22 根据您的设置要求增加磁盘空间。请参见 <https://kb.vmware.com/s/article/53550>。

## 激活许可证

安装 vRealize Network Insight 平台 OVA 后，请在 Chrome Web 浏览器中打开 <https://<vRealize Network Insight 平台 IP 地址>>。

### 步骤

- 1 输入在欢迎电子邮件中收到的许可证密钥。
- 2 对于 UI 管理员 (admin@local) 的用户名，设置密码。

---

**注** 密码必须为字母数字，且至少为 8 个字符，最多为 100 个字符。字符之间不允许使用空格。

---

- 3 单击**激活**。
- 4 激活许可证后，添加 vRealize Network Insight 收集器。

## 生成共享密钥

可以生成并导入 vRealize Network Insight 收集器虚拟设备。

生成共享密钥并导入 vRealize Network Insight 收集器虚拟设备：

### 步骤

- 1 登录到 vRealize Network Insight UI。
- 2 展开**基础架构和支持**，然后单击**概览和更新**。
- 3 向下滚动，然后单击**添加代理虚拟机**。

此时将显示**添加新的 Network Insight 数据收集器虚拟设备**对话框。

- 4 单击**复制**以从对话框中复制共享密钥，然后单击**完成**。

将在部署 vRealize Network Insight 收集器 OVA 时需要此密钥。



## 设置 Network Insight 收集器 (OVA)

可以通过将 OVA 导入到 vCenter Server 来设置 vRealize Network Insight 收集器。

请按照以下步骤将 vRealize Network Insight 收集器 OVA 导入到 vCenter Server。

### 使用 vSphere Web Client 的部署

可以使用 vSphere Web Client 导入 vRealize Network Insight 收集器 OVA。

#### 步骤

- 1 右键单击要安装设备的**数据中心**，然后选择**部署 OVF 模板**。
- 2 输入 URL 以便从 Internet 下载并安装 OVA 软件包，或者通过浏览从计算机中选择 OVA 的源位置。
- 3 为已部署模板提供名称并指定位置。单击**下一步**。
- 4 选择要运行已部署模板的资源（主机或群集）。单击**下一步**。
- 5 验证模板的所有详细信息。单击**下一步**。
- 6 阅读最终用户许可协议，然后单击**接受**。单击**下一步**。
- 7 选择部署配置。单击**下一步**。
- 8 选择要存储已部署模板的文件的位置。指定存储虚拟磁盘要采用的格式。选择**精简置备**作为虚拟磁盘格式。选择要在其中安装文件的数据存储。单击**下一步**。
- 9 为源网络指定目标网络。单击**下一步**。
- 10 为部署自定义模板。提供从 UI 生成的共享密钥。必须使用虚拟机控制台手动配置设备。单击**下一步**。
- 11 验证所有配置数据。单击**完成**。
- 12 安装收集器 OVA 后，启动虚拟机并启动控制台。
- 13 使用您在屏幕上看到的控制台凭据登录，然后运行 `setup` 命令。
- 14 为 *support* 登录创建密码并更改 *consoleuser* 的密码。

---

#### 注

- 密码必须至少包含 6 个字符。不允许使用单引号 (')。
  - 必须定期更改 *support* 和 *consoleuser* 密码，以符合您的组织策略。
- 

- 15 输入以下详细信息以配置网络：
  - a **IPv4 地址**：第二个保留的静态 IP 地址
  - b **网络掩码**：上述静态 IP 的子网掩码
  - c **默认网关**：网络的默认网关
  - d **DNS**：环境的 DNS 服务器

---

**注** 对于多个 DNS 服务器，请确保用空格将其分隔。

---

- e **域搜索列表**：需要为 DNS 查找附加的域
- f 输入 `y` 以保存配置。

16 输入 NTP 服务器，并确保可以从虚拟机进行访问。如果 NTP 时间不同步，则服务将无法启动。

---

**注** 对于多个 NTP 服务器，请确保用逗号将其分隔。

---

17 （可选）要配置 Web 代理，请执行以下操作：

- a 输入 `y`。
- b 提供 Web 代理详细信息。

18 进行检查以查看是否已配置共享密钥。收集器将与相应的平台进行配对。这可能需要几分钟的时间。

19 验证所有服务。

20 载入页面上显示**检测到代理!**消息后，单击**完成**。将重定向到登录页面。

## 使用 vSphere Windows 本机客户端进行部署

可以使用 vSphere Windows 本机客户端导入 vRealize Network Insight 收集器 OVA。

---

**注** vRealize Network Insight 5.2 是支持使用 vSphere Windows 本机客户端部署 OVA 的最后一个版本。从 5.3 版本开始，您可以继续使用 vSphere Web Client 部署 vRealize Network Insight OVA。

---

### 步骤

- 1 单击**文件 > 部署 OVF 模板**。
- 2 输入 URL 以从 Internet 下载并安装 OVA 软件包，或者浏览以选择计算机上 OVA 软件包的源位置。
- 3 验证 OVF 模板详细信息。单击**下一步**。
- 4 阅读最终用户许可协议，然后单击**接受**。单击**下一步**。
- 5 为已部署模板提供名称并指定位置。单击**下一步**。
- 6 选择**部署配置**。单击**下一步**。
- 7 选择要运行已部署模板的**主机/集群**。单击**下一步**。
- 8 选择要在其中部署此模板的**资源池**。单击**下一步**。
- 9 为虚拟机文件选择一个目标存储。单击**下一步**。
- 10 指定存储虚拟磁盘要采用的格式。选择**精简置备**作为虚拟磁盘格式。单击**下一步**。
- 11 指定已部署模板应使用的网络。将网络从 OVA 映射到清单。
- 12 为部署自定义模板。提供在载入页面上生成的共享密钥。必须使用虚拟机控制台手动配置设备。单击**下一步**。
- 13 验证所有配置数据。选中**部署后打开电源**。单击**完成**。
- 14 安装收集器 OVA 后，启动虚拟机并启动控制台。

- 15 使用给定的控制台凭据进行登录。运行 `setup` 命令。
- 16 为 `support` 登录创建密码。更改 `consoleuser` 的密码。
- 17 输入以下详细信息以配置网络：
  - a **IPv4 地址**: 第二个保留的静态 IP 地址
  - b **网络掩码**: 上述静态 IP 的子网掩码
  - c **默认网关**: 网络的默认网关
  - d **DNS**: 环境的 DNS 服务器

---

**注** 对于多个 DNS 服务器，请确保用空格将其分隔。

---

- e **域搜索列表**: 需要为 `dns lookup` 附加的域。
  - f 输入 `y` 以保存配置。
- 18 输入 NTP 服务器，并确保可以从虚拟机进行访问。如果 NTP 时间不同步，则服务将无法启动。

---

**注** 对于多个 NTP 服务器，请确保用逗号将其分隔。

---

- 19 (可选) 要配置 Web 代理，请执行以下操作：
  - a 输入 `y`。
  - b 提供 Web 代理详细信息。
- 20 进行检查以查看是否已配置共享密钥。收集器将与相应的平台进行配对。这可能需要几分钟的时间。
- 21 验证所有服务。
- 22 载入页面上显示**检测到代理!**消息后，单击**完成**。将重定向到登录页面。

## 对于 VMware SD-WAN 在 AWS 中设置 Network Insight 收集器 (AMI)

可以通过将 Amazon 计算机映像 (AMI) 导入到 AWS 环境，为 AWS 设置 vRealize Network Insight 收集器。

如果您的环境没有 vCenter Server，并且您希望在云环境中部署收集器，则可以在 AWS 中部署收集器。

---

**注** 目前，vRealize Network Insight 对于 VMware SD-WAN 仅支持在 AWS 中使用 AMI 部署收集器。

---

与 EC2 实例相关的过程和任务记录在 <https://docs.aws.amazon.com/efs/index.html> 中。

## 步骤

- 1 在 Amazon EC2 控制台中使用 VMware 提供的 AMI 启动 EC2 实例。有关过程详细信息，请参见 Amazon Elastic File System 文档中的“创建 EC2 资源和启动 EC2 实例”主题。

**注** 在 AWS 中启动 EC2 实例时，必须选择以下内容：

选项	操作
实例类型	m4.xlarge（中型块）
网络	选择适当的网络和子网。
存储	默认存储。
标记	根据客户策略。
安全组	采用端口 443，允许 0.0.0.0/0 的出站流量（或者，对于受限规则，采用端口 443，允许 NI SaaS Prod FQDN 的出站流量）。
密钥	选择适当的密钥（已为 AMI 启用 SSH 登录）。

- 2 EC2 实例处于正在运行状态时，登录到 EC2 实例。
- 3 使用给定的控制台凭据进行登录。运行 `setup` 命令。
- 4 为 support 登录创建密码。更改 consoleuser 的密码。

**注** 更改密码后，将在设置 CLI 期间跳过网络选项。

代理 AMI 不支持以下内容：

- IP 更改
- IPv6
- Web 代理配置。

- 5 输入 NTP 服务器，并确保可以从虚拟机进行访问。如果 NTP 时间不同步，则服务将无法启动。

**注** 对于多个 NTP 服务器，请确保用逗号将其分隔。

- 6 进行检查以查看是否已配置共享密钥。收集器将与相应的平台进行配对。该过程可能需要几分钟。
- 7 验证所有服务。

## 后续步骤

启用从 Edge 到在 AWS 中部署的收集器的流收集。要启用流收集，请执行以下操作：

- 将在 AWS 中部署的收集器设置为非 VeloCloud 站点。有关详细信息，请联系 VMware 技术支持。

## 在现有设置中部署其他收集器

可以将其他 vRealize Network Insight 收集器添加到现有设置中。

### 步骤

- 1 登录到 vRealize Network Insight UI。
- 2 展开**基础架构和支持**，然后单击**概览和更新**。
- 3 向下滚动，然后单击**添加代理虚拟机**。  
此时将显示**添加新的 Network Insight 数据收集器虚拟设备**对话框。
- 4 单击**复制**以从对话框中复制共享密钥，然后单击**完成**。
- 5 按照设置 **Network Insight 收集器 (OVA)**部分步骤 3 中的步骤执行操作。

# 使用评估许可证访问 vRealize Network Insight

# 3

使用评估许可证时，vRealize Network Insight 将在 NSX 评估模式下启动。

可以将数据源添加到 vRealize Network Insight，分析流量流并生成报告。

---

**注** 要切换到完整产品模式，请单击位于右下角的切换到完整产品评估。

---

本章讨论了以下主题：

- 添加 vCenter Server
- 分析流量流
- 生成报告

## 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。

### 前提条件

- 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**
- 配置和使用 IPFIX 需要以下 vCenter Server 特权：
  - **分布式交换机：修改和端口配置操作**
  - **dvPort 组：修改和策略操作**

要了解有关 vCenter 中角色的更多信息，请参见《vSphere 安全性》指南中的“使用角色分配特权”部分。

### 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
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 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"> <li>■ <b>分布式交换机</b>：修改</li> <li>■ <b>dvPort 组</b>：修改</li> </ul>
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，请参见用户指南中的“在 VDS 和 DVPG 上启用 IPFIX 配置”部分。

**注** 如果在 vCenter 和 VMware NSX Manager 中启用 IPFIX，vRealize Network Insight 会通过禁用关联 vCenter 的一些 DVPG 上的 IPFIX 来自动检测和移除流冗余。

## 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。

# 分析流量流

可以使用 vRealize Network Insight 分析数据中心的流。

### 前提条件

开始流分析之前，必须至少收集两个小时的数据。

### 步骤

- 1 指定分析范围。例如，如果希望分析**群集**中所有虚拟机的流，请从下拉菜单中选择“群集”。您也可以选择连接到 VLAN 或 VXLAN 的所有虚拟机。

- 2 选择要分析其流的实体名称。
- 3 选择持续时间，然后单击**分析**。

## 生成报告

可以生成流评估报告。

### 前提条件

分析数据中心中的流量流。对于综合报告，请在分析之前收集 24 小时的数据。

### 步骤

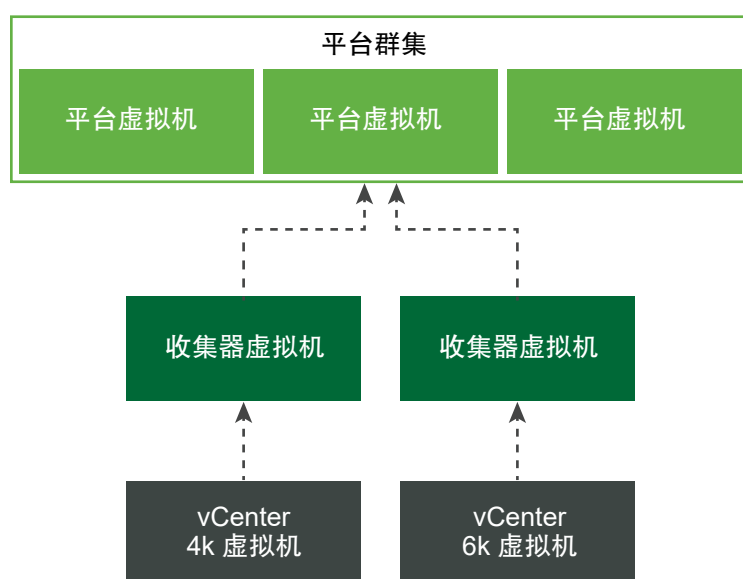
- 1 在 **EVAL NSX 评估模式**下，单击“分析流”页面中的**生成报告**。
- 2 在**非 EVAL 模式**下，单击**微分段**页面上的**流量分布 > 更多选项 > 评估报告**。



## 计划纵向扩展部署

如果设置中的虚拟机计数或活动流数量较高或预计会增加，则可以增加平台或收集器的大小。

可以使用以下架构更好地了解平台和收集器的分布情况：



本章讨论了以下主题：

- 计划纵向扩展平台群集
- 计划纵向扩展收集器
- 增加设置的块大小

### 计划纵向扩展平台群集

可以纵向扩展平台群集，以满足增加的负载。根据负载，可以通过增加块大小或者创建或扩展平台群集来纵向扩展。可以将三个 LARGE 平台块连接在一起，形成一个平台群集。如果平台为 LARGE 或 EXTRA LARGE 块大小，则必须通过创建平台群集进行纵向扩展。

要确定平台块大小和平台块数量，请参见[系统建议和要求](#)。

**注** 平台群集不支持高可用性配置。所有平台节点都需要启动且正在运行，群集才能以最佳性能运作。

## 平台群集纵向扩展场景

- 场景 1: 平台运行 5000 个虚拟机和 150 万个活动流

将平台从 MEDIUM 转换为 LARGE。请参见[增加设置的块大小](#)。

- 场景 2: 平台运行一个 LARGE 节点，其中具有 9000 个虚拟机和 200 万个活动流

再添加两个 LARGE 块节点以转换为 3 节点 LARGE 块群集。请参见《vRealize Network Insight 用户指南》中的“扩展群集”。

- 场景 3: 平台运行一个 3 节点 LARGE 群集，其中包含一个或多个收集器、15000 个虚拟机和 400 万个活动流。

将现有平台节点从 LARGE 转换为 EXTRA-LARGE。请参见[增加设置的块大小](#)。

- 场景 4: 平台运行一个 3 节点 EXTRA-LARGE 群集，其中包含一个或多个收集器、25000 个虚拟机和 800 万个活动流。

再添加两个 EXTRA-LARGE 块节点以转换为 5 节点 Extra-LARGE 群集。请参见《vRealize Network Insight 用户指南》中的“扩展群集”。

## 计划纵向扩展收集器

收集器容量基于块大小。可以添加到收集器的数据源取决于收集器的容量（虚拟机和流）。

请参见表 1-6. [收集器部署 - 最大容量](#)。收集器的块大小为 LARGE 后，必须添加更多收集器。可以将每个收集器纵向扩展到 EXTRA-LARGE 大小。

可以根据支持的收集器容量将多个数据源添加到一个收集器。但是，不能将同一数据源添加到多个收集器。

## 收集器纵向扩展场景

- 场景 1: vCenter 中有 2000 个虚拟机。

安装一个中型收集器虚拟机。将该 vCenter 添加到此收集器。请参见[添加 vCenter Server](#)。

- 场景 2: vCenter1 中有 1000 个虚拟机，vCenter2 中有 2000 个虚拟机（全部都在一个数据中心内）。

安装一个中型收集器虚拟机。将这两个 vCenter 添加到此收集器。请参见[添加 vCenter Server](#)。

- 方案 3: vCenter1 中有 1000 台虚拟机（数据中心 1），vCenter2 中有 2000 台虚拟机（数据中心 2）。

在每个数据中心内安装一个中型收集器虚拟机。将 vCenter1 添加到同一数据中心内的收集器虚拟机，并将 vCenter2 添加到其数据中心内的收集器虚拟机。请参见[添加 vCenter Server](#)。

- 场景 4: 虚拟机计数超过 4000，活动流超过 250 万。

将收集器虚拟机从 MEDIUM 转换为 LARGE。请参见[增加设置的块大小](#)。

- 场景 5: vCenter1 中有 9,000 个不带流的虚拟机（数据中心 1）。

安装一个大型收集器虚拟机。将该 vCenter 添加到此收集器。请参见[添加 vCenter Server](#)。

- 场景 6: 虚拟机计数小于或等于 10000，但活动流超过 500 万。

将收集器虚拟机从 LARGE 转换为 EXTRA-LARGE。请参见[增加设置的块大小](#)。

- 场景 8: 两个 vCenter，vCenter1 具有 10000 个虚拟机和 900 万个活动流，vCenter2 具有 10000 个虚拟机和 400 万个活动流。

安装一个 EXTRA-LARGE 和一个 LARGE 代理。将 vCenter1 添加到 EXTRA-LARGE 代理并将 vCenter2 添加到 LARGE 代理。

- 场景 9: 一个 vCenter 运行 10000 个虚拟机和 900 万个活动流。

安装一个 EXTRA-LARGE 代理并将该 vCenter 添加到此代理。

## 增加设置的块大小

为了满足您的要求，您可以将平台或收集器设备的块大小从 MEDIUM 更改为 LARGE 或从 LARGE 更改为 EXTRA-LARGE。

### 步骤

- ◆ 执行与您的设置相关的步骤。

选项	描述
对于单节点平台或全新独立 OVA	<ol style="list-style-type: none"> <li>登录到 vCenter。</li> <li>关闭平台虚拟机。</li> <li>将虚拟机的磁盘、RAM、总 vCPU 和相应预留至少增加到与目标块大小匹配。有关详细信息，请参见“系统建议和要求”页面。</li> <li>重新启动平台虚拟机。</li> </ol>
对于群集平台	<ol style="list-style-type: none"> <li>登录到 vCenter。</li> <li>按时间倒序关闭平台虚拟机。例如：按从节点 3 到节点 1 的顺序关闭。</li> <li>增加磁盘、RAM、总 vCPU 和相应的预留。有关详细信息，请参见“系统建议和要求”。</li> <li>按时间顺序重新启动平台虚拟机。例如：按从节点 1 到节点 3 的顺序重新启动。</li> </ol>
对于收集器	<ol style="list-style-type: none"> <li>登录到 vCenter。</li> <li>关闭收集器虚拟机。</li> <li>将虚拟机的磁盘、RAM、总 vCPU 和相应预留至少增加到与目标块大小匹配。有关详细信息，请参见“系统建议和要求”页面。</li> <li>重新启动收集器虚拟机。</li> </ol>

# 升级 vRealize Network Insight

# 5

可以将当前的 vRealize Network Insight 环境升级到最新版本。

升级之前需要注意的要点：

- 升级后，vRealize Network Insight 大约需要 12 到 24 小时的时间来处理在升级操作期间位于管道中的数据，并反映在 UI 上。
- vRealize Network Insight 不支持回滚或产品降级。在继续升级之前，必须先执行备份。有关备份和还原过程的详细信息，请参见 <https://kb.vmware.com/s/article/55829> 知识库文章。
- 在群集环境中，必须仅在平台 1 节点上执行升级操作。
- 升级到 vRealize Network Insight 5.1 后，某些防火墙规则 ID 可能会更改为 VMware Cloud on AWS 1.9 API 返回的新 ID。如果存在已附加到流的任何 VMware Cloud on AWS 1.8 防火墙规则：
  - 升级之后，将立即为所有活动流附加正确的或相应的 VMware Cloud on AWS 1.9 防火墙规则。
  - 对于在从 1.8 升级到 1.9 版之前不活动持续时间超过 24 小时的流，防火墙规则将引用不存在的规则。

---

**注** 如果在执行集中升级时出现上载失败或 UI 故障等问题，请联系 VMware 技术支持。

---

## 迁移到 Foundation 数据库

要将配置数据分布在群集中的数据存储上，vRealize Network Insight 5.1 会将 PostgreSQL 替换为 Foundation 数据库，以存储配置数据。这样有助于 vRealize Network Insight：

- 减少平台 1 节点上的负载
- 避免单点故障
- 提高弹性
- 增强性能
- 在群集节点之间共享同一磁盘

迁移过程将自动执行以下动作：

- 关闭所有服务
- 启动从 PostgreSQL 到 Foundation 数据库的表到表迁移

- 在平台 1 UI 上显示动态迁移进度信息

将数据从 PostgreSQL 移至 Foundation 数据库的迁移时间取决于磁盘速度和节点计数（节点越多，提供的 Foundation 数据库写入吞吐量也就越大）

完成迁移过程所需的时间取决于数据库的大小。

设置大小	数据大小	节点计数	通常迁移时间
小型	20 GB 至 40 GB	1 个节点	1 至 2 个小时
中型	60 GB 至 100 GB	3 个节点	7 至 10 个小时
一个大型云设置	500GB	10 节点群集	15 至 20 个小时
XL（超大型）	1 TB	10 节点群集	35 至 40 个小时

请注意，迁移将在 vRealize Network Insight 升级过程中执行。因此，升级时间可能更长，在操作过程中屏幕上会显示相关信息。

vRealize Network Insight 提供不同的升级模式。

本章讨论了以下主题：

- [联机升级](#)
- [一键式脱机升级](#)
- [CLI 升级](#)

## 联机升级

只要推出 vRealize Network Insight 的新版本，您就会收到通知。

### 前提条件

- 如果 /tmp 目录中的空间不足，则升级步骤可能会失败。确认满足平台和收集器服务器的以下磁盘空间要求：
  - /tmp - 6 GB
  - /home - 2 GB
- 确认满足平台服务器的以下磁盘空间要求：
  - / - 6 GB（仅适用于平台 1 节点）
  - /var - 40 GB
- 确认您满足最小带宽要求 500 KB/秒，以便从服务器下载升级包。如果下载带宽不足，则[安装和支持](#)页面将抛出错误。
- 确保所有节点都处于联机状态。如果有任何节点处于非活动状态，则不允许触发升级。
- 生成虚拟机的快照。
- 记下以下值以便在迁移后进行验证：
  - 虚拟机计数

- 快照计数 > 0 的虚拟机
- 防火墙规则计数
- 安全组计数
- NSX 防火墙计数

## 步骤

- 1 推出更新时，您会看到**更新可用**消息通知。

### 注

- 如果未显示更新通知，请通过运行 `show-connectivity-status` 命令验证 vRealize Network Insight 平台虚拟机和收集器虚拟机是否通过端口 443 连接到 `reg.ni.vmware.com` 以及通过端口 443 连接到 `svc.ni.vmware.com`。如果此连接需要 http proxy，请使用 `set-web-proxy` 命令在每个虚拟机上进行配置。确保输出中包含的升级连接状态为 `Passed`。
- 提交支持请求，并提供产品 UI 中的服务标记。服务标记显示在**设置 > 关于**下。
- 登录到设备并运行 `show-connectivity-status` 命令。提供每个 vRealize Network Insight 平台虚拟机和收集器虚拟机的命令输出屏幕截图。

- 2 在更新可用消息通知中，单击**查看详细信息**以查看更新的详细信息。

此时将显示“vRealize Network Insight 升级”屏幕。

- 3 阅读**继续操作之前**说明，然后单击**继续**。

- 4 等待预检查完成，预检查会验证：

- 磁盘空间，包括迁移所需的空间
- 版本
- NTP 同步状态
- 带宽

可以查看基于您的设置完成升级过程所需的大概时间（包括迁移持续时间）。

- 5 单击**立即安装**。

## 6 升级过程开始后，“vRealize Network Insight 升级”屏幕将提供升级过程的状态。

### 注

- 如果某个节点变为非活动状态，则升级过程不会继续。节点再次变为活动状态后，升级才会恢复。
- 平台 1 将成为升级服务器。如果平台 1 处于脱机状态，则不升级其他节点。
- 平台升级后，可以恢复正常的 vRealize Network Insight 操作，即使收集器升级并行执行也可如此。如果升级过程未完全结束，“安装和支持”页面中会显示 Node Version Mismatch detected 消息。

- 升级服务后，Nginx 将重新启动以显示迁移过程。因此，可能在短时间（一到两分钟）内无法访问 UI。
- vRealize Network Insight 开始将数据迁移到 Foundation 数据库。在“数据迁移状态”屏幕上，您会看到：
  - 整体状态
  - 已用时间
  - 按表状态显示的表
  - 迁移的记录数

如有任何问题，可以使用[导出迁移日志](#)选项与 VMware 技术支持团队分享。

- 在升级过程中，收集器上的 PostgreSQL 数据也会迁移到 Foundation 数据库。但是，UI 上不显示收集器迁移状态。

## 7 升级过程完成后，您将看到确认消息。

所有平台和收集器节点都已升级。

### 后续步骤

- 登录到 vRealize Network Insight，然后执行您的任务。
- 两三天后，删除快照以节省磁盘空间。

## 一键式脱机升级

vRealize Network Insight 支持对产品版本 3.7 和更高版本执行一键式脱机升级。

### 前提条件

- 如果 /tmp 目录中的空间不足，则升级步骤可能会失败。确认满足平台和收集器服务器的以下磁盘空间要求：
  - /tmp - 6 GB
  - /home - 2 GB

- 确认满足平台服务器的以下磁盘空间要求：

- /- 12 Gb（仅适用于平台 1 节点）
- /var - 40 GB

---

**注** 如果 /tmp 目录中的空间不足，则包上载和后续升级步骤可能会失败。

---

- 为避免 UI 会话超时，请转到**设置 > 系统配置 > 用户会话超时**，然后将**用户会话超时**至少增加到 2 小时。更改会话超时持续时间后，必须重新登录到系统。
- 确保所有节点都处于联机状态。如果有任何节点处于非活动状态，则不允许触发升级。
- 生成虚拟机的快照。
- 记下以下值以便在迁移后进行验证：
  - 虚拟机计数
  - 快照计数 > 0 的虚拟机
  - 防火墙规则计数
  - 安全组计数
  - NSX 防火墙计数

#### 步骤

- 1 从 [My VMware](#) 下载所需的升级包文件，并将更新软件包保存在本地磁盘。
- 2 检查并确保下载包的 MD5SUM 值与在 VMware 网站中指定的 MD5SUM 值一致。
- 3 在**安装和支持**页面的**软件版本**下，选择**单击此处**。
- 4 单击**浏览**以选择文件，然后单击**上载**。

上载完成后，vRealize Network Insight 将在 2-3 分钟内显示包上载完成消息通知，并在后台进行包处理。

---

#### 注

- 上载软件包之前，请确保会话未关闭。如果会话结束，必须重新启动上载过程。
  - 包上载后，如果未显示更新可用消息通知，请勿刷新页面。
- 

- 5 在更新可用消息通知中，单击**查看详细信息**。

此时将显示“vRealize Network Insight 升级”屏幕。

- 6 阅读**继续操作之前**说明，然后单击**继续**。
- 7 等待预检查完成，预检查会验证：
  - 磁盘空间，包括迁移所需的空间
  - 版本
  - NTP 同步状态



- 包

## 8 单击立即安装。

可以查看基于您的设置完成升级过程所需的大概时间。

## 9 升级过程开始后，“vRealize Network Insight 升级”屏幕将提供升级过程的状态。

### 注

- 如果某个节点变为非活动状态，则升级过程不会继续。节点再次变为活动状态后，升级才会恢复。
- 平台 1 将成为升级服务器。如果平台 1 处于脱机状态，则不升级其他节点。
- 平台升级后，可以恢复正常的 vRealize Network Insight 操作，即使收集器升级并行执行也可如此。如果升级过程未完全结束，“安装和支持”页面中会显示 Node Version Mismatch detected 消息。

- 升级服务后，Nginx 将重新启动以显示迁移过程。因此，可能在短时间（一到两分钟）内无法访问 UI。
- vRealize Network Insight 开始将数据迁移到 Foundation 数据库。在“数据迁移状态”屏幕上，您会看到：
  - 整体状态
  - 已用时间
  - 按表状态显示的表
  - 迁移的记录数

如有任何问题，可以使用**导出迁移日志**选项与 VMware 技术支持团队分享。

- 在升级过程中，收集器上的 PostgreSQL 数据也会迁移到 Foundation 数据库。但是，UI 上不显示收集器迁移状态。

## 10 升级过程完成后，您将看到确认消息。

所有平台和收集器节点都已升级。

### 后续步骤

- 登录到 vRealize Network Insight，然后执行您的任务。
- 两三天后，删除快照以节省磁盘空间。

## CLI 升级

仅当联机升级或一键式脱机升级不起作用时，才考虑 CLI 升级。必须先升级平台虚拟机，然后再升级收集器虚拟机。但是，在使用 CLI 启动脱机升级之前，必须先联系 VMware 技术支持。

在群集环境中，只能从平台 1 (P1) 节点执行升级操作，群集中的其他平台节点会自动升级。但您必须单独升级每个收集器。

## 前提条件

- 如果 /tmp 目录中的空间不足，则升级步骤可能会失败。确认满足平台和收集器服务器的以下磁盘空间要求：
  - /tmp - 6 GB
  - /home - 2 GB
  - /var - 40 GB
- 确保所有节点都处于联机状态。如果有任何节点处于非活动状态，则不允许触发升级。
- 生成虚拟机的快照。
- 记下以下值以便在迁移后进行验证：
  - 虚拟机计数
  - 快照计数 > 0 的虚拟机
  - 防火墙规则计数
  - 安全组计数
  - NSX 防火墙计数

## 步骤

- 1 从 [My VMware](#) 下载所需的升级包文件。
- 2 检查并确保下载包的 MD5SUM 值与在 VMware 网站中指定的 MD5SUM 值一致。
- 3 将升级包复制到 vRealize Network Insight 平台 1 虚拟机和所有收集器虚拟机。
  - 要将文件从 Linux 虚拟机复制到 vRealize Network Insight 虚拟机，请运行命令 `scp <filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/`。
  - 要将文件从 Windows 虚拟机复制到 vRealize Network Insight 虚拟机，请运行命令 `pscp -scp <SOURCE_PATH>\<filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/`。

---

**注** 使用 <https://the.earth.li/~sgtatham/putty/latest/w64/pscp.exe> 中的 pscp 实用程序。

---

- 4 通过 CLI 使用 consoleuser 登录到 vRealize Network Insight 平台 1，并运行以下命令：
  - `package-installer copy --host localhost --user consoleuser --path /home/consoleuser/<filename>.upgrade.bundle`
  - `package-installer upgrade --name <filename>.upgrade.bundle`

---

**注** 必须先执行平台升级，然后再启动收集器更新。

---

- 5 在操作系统升级过程中重新引导安装后再次运行 `package-installer upgrade` 命令。

---

**重要事项** 如果收到 SSH 会话超时错误，则必须查看 `/var/log/arkin/centralized_upgrade.log` 以了解是否已进行重新引导。如果重新引导成功，必须再次运行 `package-installer upgrade` 命令。

---

- 6 通过 CLI 登录到每个收集器节点，然后使用平台升级所用的相同命令执行升级。

---

**注** 您可以同时升级所有收集器。

---

- 7 使用 `show-version` 命令验证升级后的版本。

# 卸载 vRealize Network Insight

# 6

必须通过 vSphere Web Client 卸载 vRealize Network Insight。

## 步骤

1 如果可以访问 vRealize Network Insight Web 门户，请执行以下操作：

- a 登录到 vRealize Network Insight Web 门户。
- b 转到 **设置 > 帐户和数据源**。
- c 关闭并删除所有数据源。

删除 vCenter 数据源将移除 VDS 上的 IPFIX 设置（如果已配置）。同样，删除 NSX Manager 数据源会从 NSX 流监控器中移除 IPFIX 设置。

2 如果无法访问 vRealize Network Insight Web 门户，请执行以下操作：

- a 如果在 vCenter 上启用了 Netflow (IPFIX)，请从 VDS/DVPG IPFIX 设置中移除 vRealize Network Insight 收集器 IP。请参见在 [vCenter 中启用 Netflow 时移除收集器 IP](#)。
- b 如果在 NSX 上启用了 IPFIX，请移除 vRealize Network Insight 收集器 IP 流监控设置。请参见在 [NSX 中启用 Netflow 时移除收集器 IP](#)。
- c 如果在物理交换机上将 Netflow 配置为将 Netflow 发送到 vRealize Network Insight Netflow 收集器，请修改交换机中的配置以停止发送 NetFlow 信息。

3 如果创建了任何特定的防火墙或路由规则以允许或路由进出 vRealize Network Insight 虚拟机的流量，请移除这些防火墙/路由规则。

4 出于安全原因，请清理用于在 vRealize Network Insight 中配置数据源的访问凭据。

5 关闭并删除所有 vRealize Network Insight 收集器和平台虚拟机。

## 在 vCenter 中启用 Netflow 时移除收集器 IP

如果在 vCenter 中启用了 Netflow (IPFIX)，请使用此过程从虚拟专用服务器 (VDS)/分布式虚拟端口组 (DVPG) IPFIX 设置中移除 vRealize Network Insight 收集器 IP。

## 步骤

- 1 登录到 vSphere Web Client。
- 2 转到 **主页 > 网络**。

- 3 在左侧窗格中，选择 **VDS**，然后单击 **配置 > 编辑**。
- 4 在 **收集器 IP 地址** 字段中，移除 vRealize Network Insight 收集器 IP 详细信息。
- 5 在 **收集器端口** 字段中，移除端口详细信息。
- 6 单击 **确定**。  
在继续执行下一步之前，必须等待两分钟左右。
- 7 选择此 VDS 的 DVPG，然后单击 **配置 > 策略 > 编辑**。
- 8 在 **Netflow** 字段中，从下拉菜单中选择 **禁用**。
- 9 验证设置，然后单击 **应用**。

#### 后续步骤

对已启用 IPFIX 的每个 VDS 及其 DVPG 重复执行这些步骤，以移除 vRealize Network Insight 收集器 IP。

## 在 NSX 中启用 Netflow 时移除收集器 IP

如果在 NSX 中启用了 Netflow (IPFIX)，请使用此过程移除 vRealize Network Insight (vRealize Network Insight) 收集器 IP 流监控设置。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **主页 > 网络和安全 > 工具 > 流监控 > 配置**。
- 3 在 **全局流收集状态** 中，单击 **禁用**。
- 4 要禁用流连接，请单击 **IPFIX**。
- 5 在 **IPFIX** 选项卡中，选择 **收集器 IP**，然后单击 **删除**。
- 6 如果已经没有 IP 了，请单击 **编辑** 并清除 **启用 IPFIX 配置** 复选框。
- 7 单击 **保存**。