

# vRealize Network Insight 常见问题解答

VMware vRealize Network Insight 5.0



vmware®

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

如果您对本文档有任何意见或建议, 请将反馈信息发送至:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**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 © 2019 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

# 目录

<b>1</b>	关于《vRealize Network Insight 常见问题解答指南》	<b>4</b>
<b>2</b>	常规	<b>5</b>
<b>3</b>	安装和配置	<b>7</b>
<b>4</b>	将 vCenter Server 作为数据源进行添加或配置	<b>11</b>
<b>5</b>	微分段和流	<b>13</b>
<b>6</b>	群集	<b>15</b>
	群集 - 常规	15
	群集 - 安装和配置	17
	群集 - 扩展	18
	群集 - 部署	19
<b>7</b>	数据管理和处理	<b>21</b>
<b>8</b>	IPFIX	<b>23</b>

# 关于《vRealize Network Insight 常见问题解答指南》

1

《vRealize Network Insight 常见问题解答指南》向用户介绍了有关 vRealize Network Insight 的常见问题解答。

## 目标读者

本信息面向使用 vRealize Network Insight 的用户。

## 常规

### 如何创建支持包？

请参阅《vRealize Network Insight 命令行参考指南》中的“支持包”部分。

### 如何在 Palo Alto Networks Panorama 中为 XML API 访问创建只读管理员角色？

要为 XML API 访问添加管理员角色，请执行以下操作：

- 1 选择 **Panorama** → **管理员角色**
- 2 单击**添加**以添加新的管理员角色并打开“管理员角色配置文件”对话框
- 3 在“管理员角色配置文件”对话框中
  - a 为角色指定名称（例如，`api-only-admin`）
  - b 选择**角色**作为 **Panorama**
  - c 禁用“Web UI”选项卡中的所有条目
  - d 启用“XML API”选项卡中除**提交**以外的所有条目
  - e 单击**确定**关闭该对话框，列表中将显示新**管理员角色**的名称
  - f 单击**提交**以将更改提交到 **Panorama**
- 4 将此**管理员角色**分配给管理帐户。

### 何时将服务视为共享？

以下端口配置为共享：

协议	端口
DNS	53
Bootpc	68
Kerberos	110
sunrpc	111
NTP	123
map	143

协议	端口
Imap3	220
SMTP	25
LDAP	389
IGMPv3Lite	465
syslog	514
Submission	587
syslog-conn	601
LDAPS	636
IMAPS	993
POP3S	995
NFS	2049
MSFT-GC	3268
MSFT-GC-SSL	3269

## 数据源上显示事件/错误“数据源身份信息（如证书或密钥）已更改（The data source identity information such as a certificate or the key has changed）”。这意味着什么？

vRealize Network Insight 从数据源收到了新证书，该证书与产品中存储的证书不同。vRealize Network Insight 自动接受数据源提供的证书。在此过程中，数据源上将显示一个事件，可以从中下载新旧证书。

## 在 vRealize Network Insight 中导入 DNS 记录的限制是多少？

导入 DNS 记录的限制为：

- Infobox DNS 数据源：可以从单个数据源导入 900K 记录。
- 手动导入 DNS 记录：可以使用多个 .csv 或 Bind 文件（打包为一个 zip 文件）导入 DNS 记录。可以导入的记录数量没有限制，但存在上载限制，如下所示：
  - 单个 zip 文件中的文件数 - 25 个
  - 单个 zip 文件的最大大小 - 10 MB。

## 安装和配置

### vRealize Network Insight 的资源要求？

有关资源要求，请参阅《vRealize Network Insight 安装指南》。

### 如果在 vRealize Network Insight 代理 OVA 部署期间输入不正确的密钥，会怎样？

在 vRealize Network Insight 代理 OVA 部署期间，不会验证密钥。即使密钥不正确，部署也会完成。但是，配对可能会失败，并且 vRealize Network Insight 代理在 vRealize Network Insight UI 上不会显示为已检测。

要更正共享密码，请登录到 vRealize Network Insight 代理 CLI，然后运行 `set-proxy-shared-secret` 命令以设置正确的密钥。此命令会将旧密钥替换为新密钥，因此 vRealize Network Insight 平台将检测到 vRealize Network Insight 代理并进行配对。

### 如何在部署 vRealize Network Insight 代理 OVA 后配置 DNS？

登录到 vRealize Network Insight 代理 CLI，然后运行 `change-network-settings` 命令。此交互式命令将为用户提供添加或修改 DNS 的选项，之后，将使用新 DNS 重新配置 vRealize Network Insight 代理。

如果未正确配置任何网络参数，请使用 `change-network-settings` 命令修改网络配置参数。

### 如何从 UI 中找到 vRealize Network Insight 代理虚拟机 IP？

转到“设置”页面，然后选择“vRealize Network Insight 基础架构”菜单选项。将显示 vRealize Network Insight 平台和 vRealize Network Insight 代理虚拟机的 IP 地址。

### 如果在部署 vRealize Network Insight 代理 OVA 后的 5 分钟内未检测到 vRealize Network Insight 代理，该怎么办？

使用 `consoleuser` 登录到 vRealize Network Insight 代理（请参阅《vRealize Network Insight 命令行参考指南》），然后验证以下内容：

- 使用 CLI `show-connectivity-status` 验证 vRealize Network Insight 平台与 vRealize Network Insight 代理的配对状态。

- 如果配对状态显示为 **Passed**，请在新的浏览器窗口中打开平台 UI，然后登录以检查状态。
- 如果配对状态显示为 **Failed**，说明在 vRealize Network Insight 代理 OVA 部署期间指定的共享密钥可能错误。要修复此问题，请使用 `set-proxy-shared-secret` 命令设置正确的密钥。此命令会将旧密钥替换为新密钥，因此 vRealize Network Insight 平台可检测到 vRealize Network Insight 代理。
- 如果 `show-connectivity-status` 显示 vRealize Network Insight 平台的网络可访问性为 **Failed**，则通过使用 `ping` 命令验证是否可从 vRealize Network Insight 代理虚拟机访问 vRealize Network Insight 平台。
- 如果无法访问，请使用 `show-config` 命令验证 NTP、DNS、网关和其他网络参数是否配置正确。
- 如果未正确配置任何网络参数，请使用 `setup` 命令修改网络配置参数。

## 如果忘记登录凭据，该怎么办？

如果您是 UI 本地用户：联系 vRealize Network Insight UI 管理员以重置您的凭据。

如果您是管理员：从 vRealize Network Insight 3.4 开始，可以使用 CLI `modify-password` 更改 UI 凭据。有关详细信息，请参阅 CLI 指南。如果使用的是 3.4 之前的 vRealize Network Insight 版本，请联系支持部门。

## 如何更改登录密码？

要更改登录密码，请执行以下操作：

- 1 转到**管理员 > 设置**，然后在左侧窗格中单击**我的个人资料**。
- 2 在**更改密码**页面上，填写必填信息，然后单击**保存**。

## 如果在检测 vRealize Network Insight 代理虚拟机之前显示登录屏幕，该怎么办？

- 如果在检测代理之前刷新浏览器或在新窗口中打开 URL，会出现此行为。
- 使用在许可证激活期间为 `admin@local` 用户名设置的凭据登录。

## vRealize Network Insight 是否支持多个 vCenter Server/NSX Manager？

是，vRealize Network Insight 支持多个 vCenter Server 和 NSX Manager。



## 哪些 vRealize Network Insight 服务需要访问 Internet？为什么？

vRealize Network Insight 支持需要访问 Internet 的远程家庭呼叫功能。通过此功能或服务，vRealize Network Insight 团队可以更好地了解客户环境并主动排除故障或修复问题。以下服务需要访问 Internet：

- 1 升级服务 (svc.ni.vmware.com:443)：vRealize Network Insight 使用此服务访问远程升级主机，并拉入新发布的可用位。会定期使用升级主机收集并上载与 vRealize Network Insight 的关键服务和性能相关的某些衡量指标，以便 vRealize Network Insight 支持团队监控并发现环境中的任何异常，进而采取措施以免影响关键服务。
- 2 衡量指标服务 (svc.ni.vmware.com:443)：系统会定期收集并上载与 vRealize Network Insight 的关键服务和性能相关的某些衡量指标，以便 vRealize Network Insight 支持团队监控并发现环境中的任何异常，进而采取措施以免影响关键服务。可以在部署 vApp 时或稍后通过“telemetry”CLI 启用/禁用此服务。
- 3 支持服务 (support2.ni.vmware.com:443)：此服务可建立与 vRealize Network Insight 支持主机的远程安全隧道，从而授权人员可以远程访问和使用部署。默认情况下，此服务处于禁用状态，可以通过 UI 和“support-tunnel”CLI 进行启用/禁用。
- 4 注册服务 (reg.ni.vmware.com:443)：用于向所有外部服务注册设备。该服务支持在上述服务之间建立可信通信。当安装程序有权访问 Internet 时，将自动执行注册。在隔离环境中，可以使用“offline-registration”CLI 完成此操作（有关详细信息，请参阅 CLI 指南）。启用支持隧道时必须使用此服务。

**注** 如果 vRealize Network Insight 平台位于 Internet 代理后面，请将以下域名和端口列入白名单：

**表 3-1.**

服务	URL	端口
升级服务/衡量指标服务	svc.ni.vmware.com	443
支持隧道服务	support2.ni.vmware.com	443
注册服务	reg.ni.vmware.com	443

## 什么是端口聚合以及执行此操作的机制是什么？

端口聚合功能已内置于系统中，可聚合临时端口流，如动态 FTP、Oracle、MS-RPC 等。这有助于减少系统中的流数，并为基本上用于同一服务的大量流提供聚合视图。

执行此操作的机制如下所示：

- 在通告 destination\_ip 的前三天，会将该特定 IP 上的目标端口聚合到 10K 存储桶中，并开始为该 IP 构建端口配置文件（每个目标 IP 构建一个端口配置文件）。
- 三天后，已经构建了配置文件，如果端口密度较高，将开始聚合端口范围（反映临时端口打开模式）。范围本身为动态大小（如 100、1,000、10,000），并且将根据打开的端口数以及在给定聚合范围内的分布情况进行创建。

**注** 会对每个服务器 IP 地址单独制定此决策。

- 这将允许在没有批量端口打开活动的情况下报告高端口流，但不会进行聚合，此外，还允许在发生此类活动时应用动态聚合。
- 配置文件会按时间衰减的方式不断更新，以说明正在打开新端口或不再使用旧端口。

## 如何在部署 vRealize Network Insight OVA 后更改 IP 地址/网关/网络掩码？

要更改 vRealize Network Insight 平台/代理网络设置，请登录到 CLI 并运行 `change-network-settings` 命令。此交互式命令将为用户提供修改 IP 地址、网关、网络掩码等的选项，之后，将使用新的详细信息重新配置 vRealize Network Insight 设备。

### 注

- 必须使用虚拟机控制台会话完成此任务，因为设备最后会重新引导。
- 如果 vRNI 平台 IP 已修改且已与代理配对，则在每个代理虚拟机上运行以下 CLI 命令：

```
vrni-proxy set-platform --ip-or-fqdn <New_Platform_IP>
```

## 如何将评估许可证更改为永久许可证？

请参阅《vRealize Network Insight 用户指南》中的“更改许可证”部分。

## vRealize Network Insight 中的许可证有什么特点？

表 3-2.

许可证名称	许可证类型	功能
企业	完全/生产：可以是永久型，也可以是时限型。	将启用以下功能： <ul style="list-style-type: none"> <li>■ AWS 作为数据提供程序</li> <li>■ 可调整数据保留策略</li> <li>■ Infoblox DNS 数据源</li> <li>■ 物理 IP 和 DNS 映射</li> <li>■ 分析</li> </ul>
高级	完全/生产：可以是永久型，也可以是时限型。	不适用

**注** 所有许可证的容量均按 CPU 插槽数和 CCU（并发用户）数计算。可以通过 **UI -> 设置 -> 关于** 使用更新的密钥续订评估许可证或将其转换为生产。有关更多详细信息，请参阅用户指南。

## 如何在 vRealize Network Insight 中备份虚拟机？

请参阅《VMware 最佳做法》，了解如何备份虚拟机，例如 VMware VADP/VDP API。建议在创建或扩展群集之前执行备份。

## 将 vCenter Server 作为数据源进行添加或配置

# 4

### 如果使用 IP 地址添加 vCenter Server 时收到“请求超时 (Request timed out)”消息，该怎么办？

- 验证是否可从 vRealize Network Insight 代理虚拟机访问 vCenter Server IP 地址。
- 登录到 vRealize Network Insight 代理 CLI，然后使用 ping 确保可访问 IP，并使用 telnet 确保可在端口 443 上访问 vCenter Server。
- 如果可访问 vCenter Server，则重试添加。
- 如果 IP 地址不可访问，则使用命令 show-config 验证是否已从 vRealize Network Insight 代理虚拟机正确配置网关。
- 如果网关不正确，则使用 setup 命令对其进行更正。

### 如果在添加 vCenter Server 时收到“IP/FQDN 无效 (IP/FQDN is invalid)”消息，该怎么办？

- 验证为 vCenter Server 提供的 IP/FQDN 是否正确。
- 通过使用 ping 命令验证是否可从 vRealize Network Insight 代理虚拟机访问 FQDN。
- 如果不可访问，请使用 nslookup FQDN 和 show-config 命令验证是否已在 vRealize Network Insight 代理虚拟机上正确配置 DNS。
- 如果 DNS 不正确，则使用 setup 命令对其进行更正。

### vRealize Network Insight 安全和操作平台需要哪些特权？

vRealize Network Insight 需要具有以下特权的 VMware vCenter Server 凭据：

- 分布式交换机：修改
- dvPort 组：修改

## 如果在 vCenter Server 数据源页面上启用 IPFIX 时收到错误“用户没有所需特权 (User does not have required privileges)。”该怎么办？

vRealize Network Insight 需要具有以下特权的 VMware vCenter Server 凭据才能启用 IPFIX：

- 分布式交换机：修改
- dvPort 组：修改

请确保提供的 VMware vCenter Server 用户对 vCenter Server 的根文件夹及其所有子实体（如所有文件夹和所有数据中心）具有权限。

## 从环境中获取数据的频率如何？

vRealize Network Insight 代理每 10 分钟从环境中获取一次数据。

## 添加 vCenter Server 后多久将开始分析数据？

添加 vCenter Server 后，立即开始分析数据。产品 UI 将在几分钟内显示部分数据分析情况，可能需要两个小时才能全部完成。

---

**注** 流量数据不断变化，其分析中至少包含 24 小时的数据。

---

## 如果删除 vRealize Network Insight OVA，如何清除 vCenter Server 中的 IPFIX 设置？

- 使用 VMware vSphere Web Client：转到主页 > 网络 > **VDS (名称)** > **Netflow** 设置。从“收集器”设置中移除 vRealize Network Insight 代理 IP。
- 使用 VMware vSphere Windows 客户端：转到主页 > 清单 > 网络 > **VDS (名称)** > **编辑** 设置。从“Netflow”选项卡上的“收集器”设置中移除 vRealize Network Insight 代理 IP。对于已启用 IPFIX 的每个 VDS，都需要执行此步骤。

## 如何清除 vRealize Network Insight 中的 IPFIX 配置？

在 vRealize Network Insight UI 中，转到 **设置 > 数据源**，删除 vCenter server。这将移除 vRealize Network Insight 执行的 IPFIX 配置。

## 微分段和流

### 流量分布看板项中的数字表示什么？

百分比值提供了基于流分析的流量分布概况。

表 5-1.

流量	描述
东西向 (EW)	东西向流量，表示为组总流量的百分比
已交换 (占东西向流量的百分比)	已交换流量，表示为东西向流量的百分比
已路由 (占东西向流量的百分比)	已路由流量，表示为东西向流量的百分比 (%)
在主机内 (占虚拟机-虚拟机流量的百分比)	源和目标位于同一主机上的流量，表示为虚拟机到虚拟机流量的百分比
虚拟机到虚拟机 (占东西向流量的百分比)	虚拟机到虚拟机流量，表示为东西向流量的百分比
Internet	Internet 流量，表示为组总流量的百分比

### 如何在流中聚合端口？

端口聚合功能已内置于系统中，可聚合临时端口流，如动态 FTP、Oracle、MS-RPC 等。这有助于减少系统中的流数，并为基本上用于同一服务的大量流提供聚合视图。执行此操作的机制如下所示：

- 在通告 `destination_ip` 的前三天，会将该 IP 上的目标端口聚合到 10K 存储桶中，并开始为该 IP 构建端口配置文件。
- 三天后，已经构建了可以放心使用的配置文件，如果端口密度较高，将开始聚合端口范围（换句话说，反映临时端口打开模式）。范围本身为动态大小（100、1,000、10,000），并且将根据打开的端口数以及在给定聚合范围内的分布情况进行创建。
- 这将允许在没有批量端口打开活动的情况下报告高端口流，但不会进行聚合；此外，还允许在发生此类活动时应用动态聚合。
- 配置文件会按时间衰减的方式不断更新，以说明正在打开新端口或不再使用旧端口。

## 240.240.240.240 IP 地址在 vRealize Network Insight 中表示什么？

240.240.240.240 是 vRealize Network Insight 中的占位 IP 地址。如果有大量 IP 地址 (> 5000) 命中某个特定 IP 地址，则使用此 IP 地址。可以将该服务端点的所有后续入站 Internet IP（自第 5001 个 IP 起）替换为此占位 IP 240.240.240.240。

这是为了限制系统中的流数，因为单独记录每个 Internet 客户端的公开服务可能会导致出现大量流，从而增加系统负载。

对于已替换为此占位 IP 的所有流，所有衡量指标都汇总在具有此 IP 地址的相应流中，因此在汇总级别不会丢失任何统计信息。

流视图中报告的流的所有目标 IP 均显示为源自 240.240.240.240，实际上，由大量 Internet IP (> 5000) 命中。

## 群集

本章讨论了以下主题：

- 群集 - 常规
- 群集 - 安装和配置
- 群集 - 扩展
- 群集 - 部署

### 群集 - 常规

#### 是否可以将代理虚拟机或收集器虚拟机加入群集？

否。不支持将收集器/代理虚拟机加入群集。

#### vRealize Network Insight 是否需要 vRealize Log Insight 等负载均衡器？

vRealize Network Insight 群集是一种横向扩展解决方案，不是 HA 解决方案。如果主平台虚拟机/主节点发生故障，则整个服务将变得不可用。

#### 如果远程代理和平台之间的连接断开，会怎样？

如果平台和代理虚拟机之间的连接断开，则代理虚拟机将在本地存储数据（具体取决于磁盘空间），并在恢复连接后发送数据。

#### vRealize Log Insight 是否与 vRealize Network Insight 集成？

是，vRealize Log Insight 已与 vRealize Network Insight 3.4 集成。这些警示将发送到 syslog（可以为 vRealize Log Insight）。

#### 如果节点重新引导，会怎样？

如果节点重新引导，将自动加入群集并可继续运行。如果该节点为主节点，则服务会在节点关闭期间完全丧失。

## 如何更改群集中任何平台节点或代理的 IP？

在 N 节点群集中，可以使用 `change-network-settings` CLI 更改任何平台节点的 IP。需要使用 `update-IP-change` CLI 在群集中的所有其他平台节点上反映新的 IP。必须使用虚拟机控制台会话完成此操作，因为设备最后会重新引导。

**注** 如果更改了平台 1（从其触发群集操作的主平台）的 IP，还需要使用 `vrni-proxy` CLI 在所有代理上反映新的 IP。

例如，假设有一个 3 节点群集：

- 用例 1：仅更改平台 2 的 IP
  - a 在平台 2 上运行 `change-network-settings` 以更改其 IP。
  - b 在平台 1 和平台 3 上运行 `update-IP-change` 以反映新的平台 2 IP
- 用例 2：仅更改平台 1 的 IP
  - a 在平台 1 上运行 `change-network-settings` 以更改其 IP。
  - b 在平台 2 和平台 3 上运行 `update-IP-change` 以反映新的平台 1 IP
  - c 在所有代理上运行 `vrni-proxy` 以反映新的平台 1 IP
- 用例 3：更改平台 1 和代理 X 的 IP
  - a 运行用例 2 中所述的所有步骤。
  - b 在代理 X 上运行 `change-network-settings` 以更改其 IP。有关每个命令的详细信息，请参阅 CLI 指南。

## 平台 1 需要多少磁盘空间？

平台 1 需要比群集中其他节点更多的磁盘空间，因为某些配置数据仅存储在平台 1 上。

## 如果任何节点的磁盘空间不足，会怎样？

当任何特定平台节点上的磁盘空间达到特定阈值时，UI 开始显示错误消息。可以通过登录到 vCenter，增加平台节点的磁盘空间

。

## 可以在群集中复制多少次数据？

数据复制机制取决于平台节点中存在的组件。



## 群集 - 安装和配置

### 所有平台虚拟机是否必须位于同一 L2/L3 分段上？

否。不过，最好将所有平台节点都置于一个公用网络上，以降低节点之间的延迟。这是因为许多分布式组件在节点之间复制数据，高延迟可能会引起系统性能和稳定性问题。

### 是否可以使用产品内升级功能升级群集？

在版本 3.7 之前，不支持对群集执行联机升级。从 3.8 和后续版本开始，可以使用联机升级方法升级群集。

### 如果在群集创建过程中出现故障，会怎样？

最佳做法是首先生成主平台和代理的快照，然后再启动群集创建过程。如果出现故障，请删除辅助平台节点，然后从快照恢复主平台和代理虚拟机。

### 将单节点部署扩展到群集时，现有数据和配置会发生什么情况？

所有数据和配置都保持不变。创建群集后，将可访问数据。

### 平台虚拟机是否可以分布在不同区域中？

否，平台节点需要位于同一站点中。代理服务器可以异地分布。

### 是否可以将平台托管在 vSAN 延伸群集（2 个数据中心...）上？

是，同一数据中心内或跨不同数据中心的 vSAN 群集仍可确保一定的 IO 性能（如本地存储）。

### 是否可以在不同的 vSAN 群集上托管群集节点？

是，平台群集的不同节点可以托管在不同的底层数据存储中。

### 是否需要备份平台节点？

是，应使用 VMware 建议的快照/备份技术（截至目前）进行备份。vRNI 群集高可用性功能正在规划中，届时将无需执行外部备份。

### 如何估算某一区域上的群集代理虚拟机与另一区域上的平台虚拟机群集之间的带宽？

在一些大型部署中，我们发现此值的范围为 1 mbps 到 20 mbps。在将数据发送到平台虚拟机之前，代理虚拟机中会执行大量的去重和压缩操作。

### 群集节点之间的网络流量是多少？

流量通常取决于群集大小和数据中心环境的类型。

对于具有 30-50k 虚拟机的安装：

- 在群集之间：约为 50-400 Mbps。
- 在代理与平台之间：约为 100 Kbps-15 Mbps。

## 群集中节点之间的最大允许延迟是多少？

平台节点必须位于同一站点中。在这种情况下，延迟最低。如果平台节点托管在 vSAN 延伸群集（两个数据中心）上，同一数据中心内或跨不同数据中心的 vSAN 群集可确保一定的 IO 性能（如本地存储）。在数据中心上运行的应用程序（如 vRealize Network Insight）可正常运行。可以在不同的底层数据存储上托管平台群集的不同节点。但是，需要确保群集中的所有平台虚拟机都位于同一站点中。

## 某一区域上的代理虚拟机与另一区域上的平台虚拟机群集之间的最大允许延迟是多少？

您的设置中可能具有异地分布的代理。代理虚拟机到平台虚拟机之间采用 HTTPS 连接，因此从高延迟到数秒级均可容许。vRealize Network Insight 支持一个群集中最多包含 10 个节点（30,000 个带流的虚拟机或 50,000 个不带流的虚拟机）。

## 代理/平台虚拟机的大小应为多少？

使用大型块配置：请参阅“安装指南”。

## 群集 - 扩展

### 是否可以扩展已创建的群集？

是，支持最多将一个群集扩展到 10 个节点。

### 如果非主平台虚拟机变得不可用，会怎样？

内部服务应对非主节点故障的复原能力有限。通常，发生节点故障后，NI 会失去计算能力。

### 支持何种类型的负载平衡？

修复了代理到平台的映射。任何代理虚拟机中的数据到达任何平台虚拟机后，其处理将在所有平台虚拟机间实现内部负载平衡。

### 创建平台群集是否会增加带宽消耗？

代理虚拟机或收集器虚拟机仅继续与主虚拟机或平台虚拟机进行通信。平台虚拟机群集通信的带宽要求最小。因此，带宽消耗不会显著增加。

### 代理虚拟机到平台虚拟机之间的数据传输频率是多少？

代理虚拟机会持续不断地将过去重或压缩的数据发送到平台虚拟机。

## 是否在代理虚拟机中进行任何数据优化？

会在代理虚拟机中执行各种去重、压缩、缩减或批处理步骤。当平台虚拟机与代理虚拟机之间的连接断开时，代理虚拟机会在本地存储数据（具体取决于磁盘空间），并在恢复连接时发送数据。

## 是否对网络带宽进行了任何优化？

是，会在代理虚拟机中执行各种去重/压缩/缩减/批处理步骤。

## 是否可以在代理服务器上建立群集？

否。不能在代理服务器上建立群集。

## vCenter 如何将流量发送到代理服务器？

vCenter 不向代理服务器发送流量。代理服务器实际上连接到指定的 vCenter 以获取信息。

## 部署群集时，vCenter 如何将流量发送到各个代理服务器？

实际上，代理连接到 vCenter 获取信息。相应的代理将连接到指定的 vCenter 并获取信息。代理上没有可用的群集。

## 群集 - 部署

### 如何在横向扩展群集后访问 UI？

只能从平台 1 访问 UI。

### 什么是平台 1，为何需要记住此节点？

启动群集创建过程的平台节点视为平台 1。在群集的 n 个节点中，只能从此节点访问 UI。

### 如果只能从平台 1 访问 UI，那么如何从群集中的其他节点检索数据？

数据中心的数据分布在群集中的所有节点上。当 UI 层在平台 1 上请求数据时，平台 1 节点会获取存储在所有节点上的数据并向 UI 发送响应。

### 是否可以使用部署在不同数据中心的平台节点创建群集？

群集中的所有节点之间相互交换数据。因此，为了避免出现延迟问题，建议使用部署在同一数据中心的平台节点创建群集。

### 横向扩展平台节点时，现有平台上的数据会怎样？

现有平台节点上的数据将保留并分布在群集中的所有节点上。

## 代理虚拟机数量在确定所需的平台块数量方面是否重要？

否。仅所有 vCenter 的虚拟机总数和流的状态（已启用或已禁用）才会影响所需的块数量。请参阅《vRealize Network Insight 安装指南》中的块模型表。

## vCenter 数量或者物理设备（如路由器）或任何其他类型数据源的数量是否影响所需的平台块数量？

否。仅所有 vCenter 的虚拟机总数和流的状态（已启用或已禁用）才会影响所需的块数量。请参阅《vRealize Network Insight 安装指南》中的块模型表。

## vRNI 是否支持平台群集分布在两个数据中心以实现 HA？

否。平台群集不支持分散在多个数据中心。所有平台群集虚拟机应位于同一站点中。目前，平台群集不支持 HA。此功能正在规划中。客户可以跨 2 个站点使用 SRM 执行灾难恢复，以实现 HA。

## vRNI 是否支持具有 6000 多个虚拟机且已启用流的单个 vCenter？

版本 3.5 之前，vRNI 代理不支持从包含 6000 多个带流的虚拟机的单个大型 vCenter 收集数据。此功能正在规划中。

## 平台 1 需要多少磁盘空间？

平台 1 需要比群集中其他节点更多的磁盘空间，因为某些配置数据仅存储在平台 1 上。

## 如果任何节点的磁盘空间不足，会怎样？

当任何特定平台节点上的磁盘空间达到特定阈值时，UI 开始显示错误消息。可以通过登录到 vCenter，增加平台节点的磁盘空间。

## 可以在群集中复制多少次数据？

数据复制机制取决于平台节点中存在的组件。

## 群集的工作原理是什么？

- 部署中的所有代理都连接到一个平台（平台 1）。平台和代理之间的连接使用端口 443 通过 https 实现。因此，仅平台 1 中的端口 443 对代理可见。
- 收到代理发出的请求后，平台 1 节点会以循环方式将请求负载平衡到群集中的其他平台节点。
- 平台节点将数据规范化并置于消息队列，以由计算引擎进行处理。
- 计算引擎使用数据复制机制将数据分布在群集中的所有节点上。这样，如果群集中的任何节点（平台 1 除外）出现故障，则不会丢失任何数据。
- 某些配置数据显式存储在平台 1 节点上，这些数据不会进行复制。这就是为什么不支持高可用性解决方案的原因。

## 数据管理和处理

### 在边界条件下，例如，平台-代理服务器通信中断时，数据处理管道的表现如何？

- 默认保留期是多长？

30 天。可以使用企业许可证从 UI 增加保留期。注意：增加时，请确保遵循磁盘准则。

- 如何在代理上处理数据？

代理上的所有数据将转换为 **SDM**（自描述消息），然后再发送到平台（包括流数据）。包括任何数据源的所有配置、清单和衡量指标数据。如果无法访问平台或 **SDM** 上载到 **Kafka** 队列失败，则会将这些数据写入代理虚拟机上的磁盘（写入 `/var/BLOB_STORE` 下）。

- 何时开始在代理上清除数据？

对于非流数据：分配了 10 GB 空间用于在磁盘 (**BLOB\_STORE**) 上存储 **SDM**。当此存储填满时，收集器将开始删除较旧的 **SDM**，然后将新的 **SDM** 添加到磁盘。这取决于从所有数据源收集的数据大小以及超出此限制的速度。

对于流数据：分配了 15 GB 空间用于存储原始流（存储在 `/var/flow/vds/nfcapd` 下）。此空间用尽后，流处理器便开始删除较旧的流文件。进站原始流速率约为 2M/分钟时，大约需要 10 小时才会开始进行轮换。

- 清除逻辑是什么？

首先删除最旧的 **SDM**。

- 何时在代理中停止处理新数据？

只要服务正常运行，就永久不会停止。

- 假设平台和代理之间断开连接，并且未满足任何清除条件，则在重新连接时是否会在平台上协调所有数据？

存储在磁盘上的所有数据都将发送到平台。除非平台上存在数据丢失情况（详细信息见下文），否则应完全进行协调。

- 在平台上可能会发生数据丢失的情况有哪些？

平台开始删除 **Kafka** 队列中超过 6 小时（3 节点群集的情况下为 18 小时）的 **SDM**。另一种可能的情况是队列达到饱和状态。系统中出现滞后且进站数据速率较高时，可能会发生这种情况。

- 最新的 **SDM** 是先发布还是按照该顺序为最早的一个？

先发送最旧的 **SDM**。在 **v3.9** 之前，存在一个已知问题，该问题会导致一些数据丢失。有关详细信息，请联系 **GSS**。

- 数据是否先存储在代理中的磁盘上，然后不存在通信问题时再推送到平台？

如果不存在通信问题，则 **SDM** 不会存储在磁盘上。这些数据从内存本身发送到平台。仅当代理收到 **SDM** 发送过程中出现问题时，才将其存储在磁盘上。

- 如果出现任何问题，代理如何了解哪个是最后处理的流文件？

流处理器会在数据库中保留上次处理 **nfcapd** 文件的书签。

- 在没有任何问题的情况下可以处理的最大 **SDM** 大小是多少？用户如何了解是否违反此限制？

**SDM** 大小上限为 **15 MB**。从 **v3.9** 开始，每当平台放入大型 **SDM** 时都会引发事件。

# IPFIX

## 什么是 IPFIX？

IPFIX 是用于导出流信息的 IETF 协议。流定义为在特定时间段内传输且共享 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。这通常称为 Netflow。但是，IPFIX 是标准的 IETF 协议。

## VDS 导出哪些流信息？

可以将 vSphere 环境中的 VDS 配置为使用 IPFIX 导出流信息。在连接到 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。每条流记录的方向设置为“输出”。

## vRealize Network Insight 如何使用 IPFIX？

vRealize Network Insight 使用 VMware VDS IPFIX 收集网络流量数据。每个会话都有两个路径。例如：会话 A↔C 具有 A→C 数据包和 C→A 数据包。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。

## 如何对 vRealize Network Insight 流收集进行故障排除？

- 1 请确保特定 VDS 及其 DVPG 和上行链路属性已启用 Netflow 监控，且收集器 IP 地址为 vRealize Network Insight 收集器的 IP 地址。
- 2 IPFIX Netflow 数据包被防火墙（NSX、虚拟或物理）丢弃。请确保在 ESXi 主机和 vRealize Network Insight 收集器之间的路由中可能存在的任何防火墙都允许传输至 vRealize Network Insight 收集器 IP 上 UDP 端口 2055 的 Netflow 数据包。
- 3 ESXi 主机停止发送 IPFIX Netflow 数据包。如果无法访问 UDP 端口 2055，ESXi 主机将在一段时间后停止发送 Netflow 数据包。这种情况可能是由防火墙丢弃数据包所致。
- 4 由于网络路由问题，ESXi 主机无法访问 vRealize Network Insight 收集器。请确保 ESXi 主机与 vRealize Network Insight 收集器之间存在正确的路由。

## 应了解哪些与 IPFIX 相关的 VMware 知识库文章？

VMware ESXi 6.0 Update 1:

[2135956](#)