Hewlett Packard Enterprise

HPE Network Node Manager iSPI Performance for Traffic Software

软件版本：10.20
适用于 Windows® 和 Linux® 操作系统

部署参考

文档发布日期：2016 年 7 月
软件发布日期：2016 年 7 月

法律声明

担保

Hewlett Packard Enterprise 产品和服务的唯一担保由相应产品和服务随附的明示担保声明加以规定。此处的任何内容均不构成额外担保。对于本文档中出现的技术或编辑上的错误或遗漏，HPE 不承担任何责任。

此处所含信息如有更改，恕不另行通知。

受限权利声明

机密计算机软件。必须拥有 HPE 授予的有效许可证，方可拥有、使用或复制本软件。按照 FAR 12.211 和 12.212，并根据供应商的标准商业许可的规定，商业计算机软件、计算机软件文档与商品技术数据授权给美国政府使用。

版权声明

商标声明

Adobe® 是 Adobe Systems Incorporated 的商标。

Microsoft® 和 Windows® 是 Microsoft Corporation 在美国的注册商标。

Red Hat® 是 Red Hat, Inc. 在美国和其他国家/地区的注册商标。

文档更新

此文档的标题页包含以下标识信息：

- 软件版本号，用于指示软件版本。
- 文档发布日期，该日期将在每次更新文档时更改。
- 软件发布日期，用于指示该版本软件的发布日期。

要检查最近是否有更新或要验证使用的文档是否为最新版本，请转到：https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword= 。

此网站需要 HP Passport 帐户。如果没有，请单击 HP Passport 登录页面上的**创建帐户**按钮。

支持

请访问 HPE 软件支持网站：**https://softwaresupport.hpe.com**

此网站提供联系信息和有关 HPE 软件提供的产品、服务和支持的详细信息。

HPE 软件支持提供客户自行解决功能。通过该联机支持，可快速高效地访问用于管理业务的各种交互式技术支持工具。作为尊贵的支持客户，您可以通过该支持网站获得下列支持：

- 搜索感兴趣的知识文档
- 提交并跟踪支持案例和改进请求
- 下载软件修补程序
- 管理支持合同
- 查找 HPE 支持联系人
- 查看有关可用服务的信息
- 参与其他软件客户的讨论
- 研究和注册软件培训

大多数提供支持的区域都要求您注册为 HP Passport 用户再登录，很多区域还要求用户提供支持合同。要注册以获取 HP passport ID，请访问 **https://softwaresupport.hpe.com**，然后单击**注册**。

要查找有关访问级别的详细信息，请访问：
https://softwaresupport.hpe.com/web/softwaresupport/access-levels

目录

第 1 章: 关于本指南

此指南包含用于部署 HP Network Node Manager i Software Smart Plug-in Performance for Traffic(在文档的其余部分为 NNM iSPI Performance for Traffic)的信息和最佳实践集合。此指南的目标读者是:

- NNM iSPI Performance for Traffic 和 Network Performance Server (NPS) 系统管理员
- 网络工程师
- 具有在大型安装中部署和管理流量部署的经验的工程师

文档约定

NNM iSPI Performance for Traffic 文档使用以下约定:

NNM iSPI Performance for Traffic 文档约定

符号	描述
%TrafficInstallDir% (对于 Windows) $TrafficInstallDir (对于 Linux)	当主收集器或叶收集器与 NNMi 未安装在同一个系统上时，NNM iSPI Performance for Traffic 的安装目录。 对于 Windows <驱动器>\Program Files\HP\HP BTO Software 对于 Linux /opt/OV
%TrafficDataDir% (对于 Windows) $TrafficDataDir(对于 Linux)	当主收集器或叶收集器与 NNMi 未安装在同一个系统上时，NNM iSPI Performance for Traffic 的数据目录。 对于 Windows <驱动器>\ProgramData\HP\HP BTO Software 对于 Linux /var/opt/OV/
%NnmInstallDir% (对于 Windows) $NnmInstallDir(对于 Linux)	NNMi 应用程序目录的环境变量。当主收集器或叶收集器与 NNMi 安装在同一个系统上时，NNM iSPI Performance for Traffic 将安装在此目录中。此变量由 NNMi 安装程序(针对 Windows)自动创建。 对于 Windows <驱动器>\Program Files\HP\HP BTO Software 对于 Linux /opt/OV
%NnmDataDir% (对于 Windows)	NNMi 数据目录的环境变量。当主收集器或叶收集器与 NNMi 安装在同一个系统上时，NNM iSPI Performance for Traffic 将安装在此目录中。此变量由

NNM iSPI Performance for Traffic 文档约定(续)

符号	描述
$NnmDataDir(对于 Linux)	NNMi 安装程序(针对 Windows)自动创建。 对于 Windows <驱动器>\ProgramData\HP\HP BTO Software 对于 Linux /var/opt/OV/

其他可用的环境变量

NNM iSPI Performance for Traffic 管理员可以通过运行一个脚本来设置许多用于导航到经常访问位置的环境变量。

要设置可用环境变量的扩展列表，请使用类似于以下示例的命令：

Windows：C:\Program Files\HP\HP BTO Software\bin\nnm.envvars.bat

UNIX/Linux：/opt/OV/bin/nnm.envvars.sh

要在 NNM iSPI Performance for Traffic 主收集器上设置环境变量，请使用类似于以下示例的命令：

Windows：C:\Program Files\HP\HP BTO Software\traffic-master\bin\traffic-master.envvars.bat

UNIX/Linux：/opt/OV/traffic-master/bin/traffic-master.envvars.sh

要在 NNM iSPI Performance for Traffic 叶收集器上设置环境变量，请使用类似于以下示例的命令：

Windows：C:\Program Files\HP\HP BTO Software\traffic-leaf\bin\traffic-leaf.envvars.bat

UNIX/Linux：/opt/OV/traffic-leaf/bin/traffic-leaf.envvars.sh

第 2 章: NNM iSPI Performance for Traffic 简介

NNM iSPI Performance for Traffic 会扩展从网络中的路由器导出的 IP 流数据记录中获得的数据。您可以使用经过扩展的数据了解并分析环境中的网络流量模式和趋势。

您可以使用 IP 流数据记录(由 NNM iSPI Performance for Traffic 处理和扩展)，借助 Network Performance Server (NPS) 生成报告。使用 NNM iSPI Performance for Traffic，您可以将数据导出为 CSV 格式，供其他数据分析工具使用。

IP 流数据和 NNM iSPI Performance for Traffic

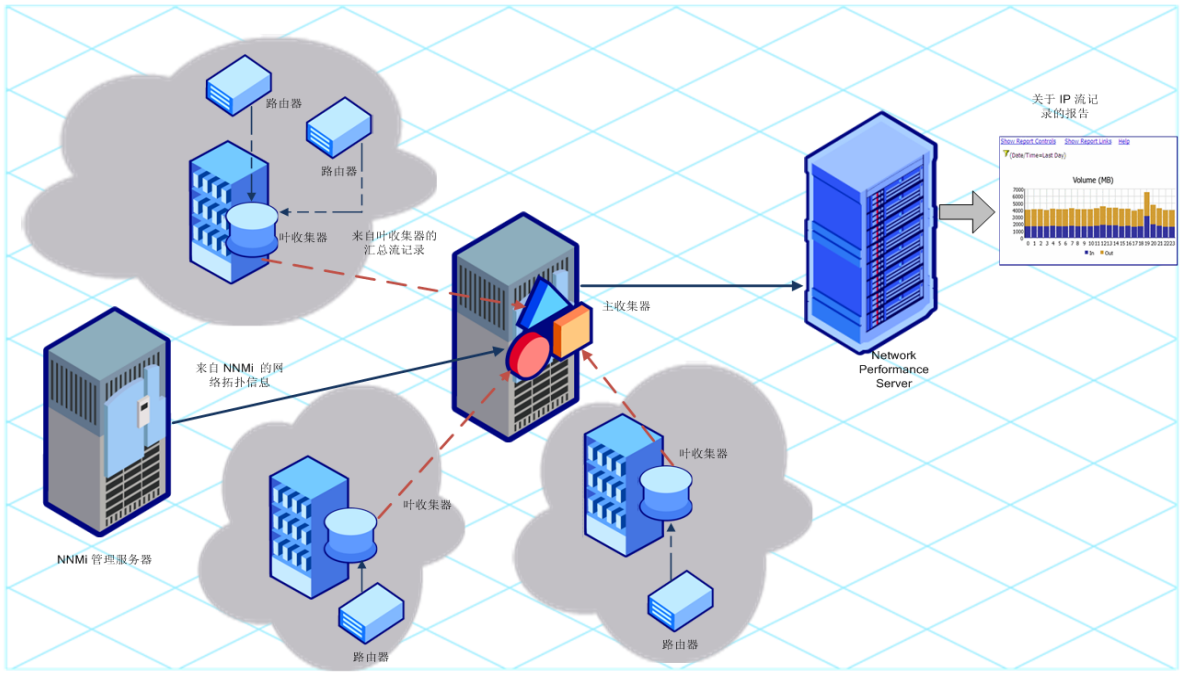
网络路由器能够导出 IP 流数据记录。IP 流数据记录包含诸如源和目标设备/系统的 IP 地址、源和目标设备/系统的端口、已发送数据字节数之类的详细信息。

NNM iSPI Performance for Traffic 识别、采集和处理特定接口上的入口和出口 IP 流数据记录。还可以在接口上同时启用入口和出口流时识别流向。NNM iSPI Performance for Traffic 为您提供了一组扩展的详细信息，其中流信息已使用 NNMi 中呈现的网络拓扑信息进行了增强。您还可以使用用户定义的筛选来筛选所采集的数据，或将流与用户定义的应用程序关联。

体系结构

NNM iSPI Performance for Traffic 由两个主要组件组成 - **叶收集器**和**主收集器**。叶收集器从不同的路由器采集 IP 流记录，然后将汇总数据转发到主收集器。主收集器会处理从叶收集器接收的汇总数据，并将拓扑上下文添加到 IP 流记录中。**HP NNMi Extension for iSPI Performance for Traffic** 安装在 NNMi 管理服务器上，包含基于主收集器处理的数据生成报告的规则和定义。

NNM iSPI Performance for Traffic 的体系结构



NNM iSPI Performance for Traffic 的工作流

1. 叶收集器会从配置为导出 IP 流记录的路由器采集 IP 流数据。
2. 叶收集器处理采集的数据。
   - 叶收集器借助聚合的内置规则聚合并扩展采集的数据，然后将聚合数据转发到主收集器。叶收集器可以每隔 5 分钟聚合一次原始数据。
   - 叶收集器也会原封不动地将所有**原始数据**[1]转发到主收集器。

   备注：可以配置 NNM iSPI Performance for Traffic 停止将原始数据转发到主收集器。
3. NNMi 会将网络拓扑信息发送到主收集器。
4. 主收集器会处理从叶收集器接收的数据，并将拓扑上下文添加到从叶收集器采集的数据中。此外，主收集器还执行 DNS 解析，应用 ToS 组配置、阈值等。
5. 主收集器会将处理后的数据记录到 NPS 数据库中。根据配置，主收集器可以将两种不同类型的数据样本记录到 NPS 数据库中：原始数据和每隔五分钟聚合的数据。
6. 借助 NPS 的帮助，您可以生成报告来分析网络流量。此外，将叶收集器采集的数据存储到 NPS 数据库中后，NNM iSPI Performance for Traffic 在 NNMi 控制台中显示不同的仪表板和图形。

[1]原始数据是由网络上的流量流导出路由器导出且由 NNM iSPI Performance for Traffic 叶收集器采集的 IP 流记录集。NNM iSPI Performance for Traffic 将原始数据直接记录到 NPS 数据库。在大型环境中，建议禁用将原始数据记录到 NPS 数据库。

第 3 章: 部署 NNM iSPI Performance for Traffic

《NNMi Ultimate Support Matrix》定义了 NNM iSPI Performance for Traffic 的以下部署环境：

- 入门
- 小
- 中
- 大

有关这些环境规模的更多信息，请参阅《NNMi Ultimate Support Matrix》。有关安装信息，请参阅《NNM iSPI Performance for Traffic 交互安装指南》。

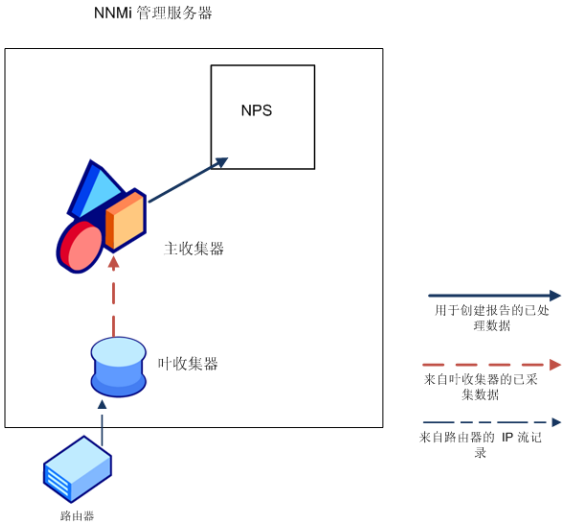
在入门级环境中部署

入门级环境适合用于评估目的。如果要创建环境来测试和演示 iSPI 的不同功能，则选择此类型的部署。不要在此环境中创建生产设置。

在此部署中，可以在 NNMi 管理服务器上安装主收集器和叶收集器，以及 HP NNMi Extension for iSPI Performance for Traffic。此部署中仅使用一个叶收集器。

在此环境中，可以在 NNMi 管理服务器上安装 NPS。

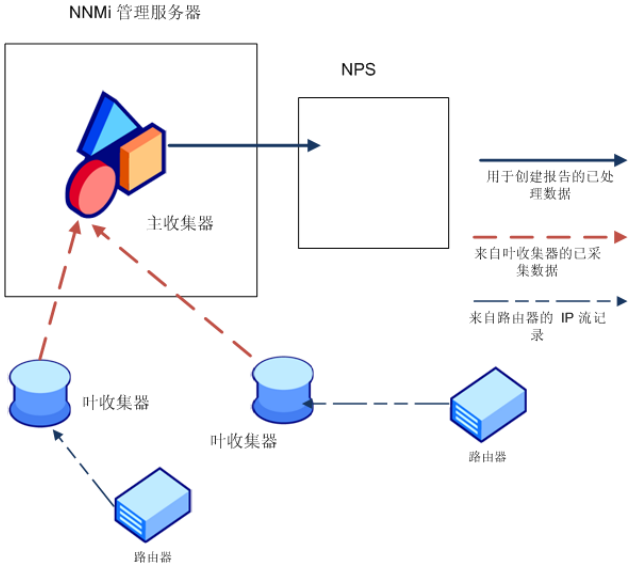
入门级部署



在小型或中型环境中部署

在此部署中，必须将主收集器和叶收集器安装在不同的系统中。可以选择在 NNMi 管理服务器上安装主收集器，在 NPS 系统上安装叶收集器。要确定您的环境所需的叶收集器数量，请参阅《NNMi Ultimate Support Matrix》。

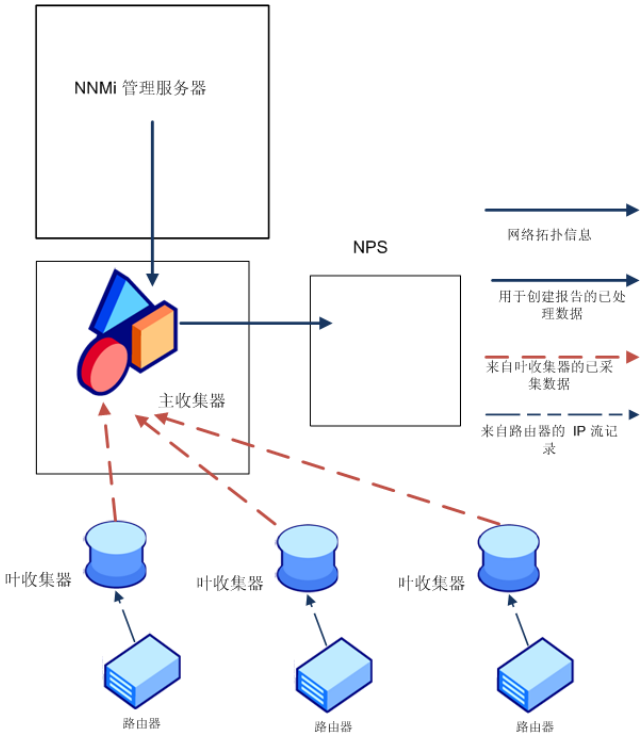
小型或中型部署



在大型环境中部署

此部署类型适合于大规模生产环境。此环境需要叶收集器的多个实例。要确定您的环境所需的叶收集器数量，请参阅《NNMi Ultimate Support Matrix》。

大型部署


NNMi 管理服务器
NPS
网络拓扑信息
用于创建报告的已处理数据
来自叶收集器的已采集数据
来自路由器的 IP 流记录
主收集器
叶收集器
叶收集器
叶收集器
路由器
路由器
路由器

第 4 章: 准备

安装 NNM iSPI Performance for Traffic 之前，请先阅读下表中描述的有关系统硬件和软件要求的信息：

软件和硬件预安装清单

文档类型	文档路径
HP Network Node Manager iSPI Performance for Traffic 交互安装指南	• 介质根目录 • 手册网站
《NNMi Ultimate Release Notes》	手册网站
《NNMi Ultimate Support Matrix》	手册网站

有关此处列出的所有文档的最新版本，请转到：

http://h20230.www2.hp.com/selfsolve/manuals

第 5 章: 管理安全性

使用 NNM iSPI Performance for Traffic，您可以配置单点登录 (SSO)，用于在维护访问的安全级别时从 NNMi 控制台访问 NNM iSPI Performance for Traffic 配置表单，如启用 NNM iSPI Performance for Traffic 的单点登录 (第 13 页)中所述。

还可配置 NNMi 将公钥基础结构 (PKI) 证书映射到 NNMi 用户帐户。这样您就可以登录到 NNMi 控制台，而无需在登录页面上输入 NNMi 用户名和密码。但是，在尝试启动 NNM iSPI Performance for Traffic 配置表单时，系统会再次提示您提供 NNMi 用户名和密码，除非您执行了其他步骤来协调与 iSPI 的映射，如配置使用公钥基础结构验证访问 (第 16 页)中所述。

备注：将 NNMi 和 NNM iSPI Performance for Traffic 配置为使用公钥基础结构 (PKI) 验证时，不要启用单点登录功能。

使用 NNM iSPI Performance for Traffic，您可以在 NNMi 管理服务器和 NPS 间进行安全通信。还可配置 NNM iSPI Performance for Traffic 确保主收集器和叶收集器间的安全通信。有关详细信息，请参阅启用安全性 (第 18 页)。

启用 NNM iSPI Performance for Traffic 的单点登录

此部分描述启用 NNM iSPI Performance for Traffic 的单点登录 (SSO) 所需的步骤。使用 SSO 后，在登录 NNMi 控制台时，您不必再次提供登录凭据即可访问 NNM iSPI Performance for Traffic 配置表单。

主收集器和 NNMi 安装在同一个系统中

如果已将主收集器安装在 NNMi 管理服务器上，请执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到主收集器系统。
2. 导航到以下目录：
   在 Windows 上

   ```
   %NnmDataDir%\shared\nnm\conf\props
   ```

   在 Linux 上

   ```
   /var/opt/OV/shared/nnm/conf/props
   ```
3. 使用文本编辑器打开 `nms-ui.properties` 文件。
4. 在 `nms-ui.properties` 文件中，将以下条目的值指定为 `true`：
   `com.hp.nms.ui.sso.isEnabled = true`
5. 运行以下命令：
   在 Windows 上

   ```
   %NnmInstallDir%\bin\nnmsso.ovpl -reload
   ```

   在 Linux 上

   ```
   /opt/OV/bin/nnmsso.ovpl -reload
   ```

6. 运行以下命令：
   在 Windows 上

   %NnmInstallDir%\traffic-master\bin\nmstrafficmasterssoreload.ovpl

   在 Linux 上

   /opt/OV/traffic-master/bin/nmstrafficmasterssoreload.ovpl

主收集器和 NNMi 安装在单独的系统中

如果已将主收集器安装在单独的系统(而非 NNMi 管理服务器)中，请执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到 NNMi 管理服务器。
2. 导航到以下目录：
   在 Windows 上

   %NnmDataDir%\shared\nnm\conf\props

   在 Linux 上

   /var/opt/OV/shared/nnm/conf/props
3. 使用文本编辑器打开 nms-ui.properties 文件。
4. 在 nms-ui.properties 文件中，将以下条目的值指定为 true：
   com.hp.nms.ui.sso.isEnabled = true
5. 运行以下命令：
   在 Windows 上

   %NnmInstallDir%\bin\nnmsso.ovpl -reload

   在 Linux 上

   /opt/OV/bin/nnmsso.ovpl -reload
6. 仅限 Windows：请执行以下步骤：
   - 确保已将 %NnmDataDir%\shared\nnm\conf\props\nms-ui.properties 文件中的 com.hp.nms.ui.sso.initString 属性和 %NnmDataDir%\shared\nnm\conf\lwssofmconf.xml 文件中的 initString 属性设置为相同的值。
   - 确保已将 %NnmDataDir%\shared\nnm\conf\props\nms-ui.properties 文件中的 com.hp.nms.ui.sso.protectedDomains 属性和 %NnmDataDir%\shared\nnm\conf\lwssofmconf.xml 文件中的 domain 元素设置为相同的值。
7. 仅限 Linux：请执行以下步骤：
   - 确保已将 /var/opt/OV/shared/nnm/conf/props/nms-ui.properties 文件中的 com.hp.nms.ui.sso.initString 属性和 /var/opt/OV/shared/nnm/conf/lwssofmconf.xml 文件中的 initString 属性设置为相同的值。
   - 确保已将 /var/opt/OV/shared/nnm/conf/props/nms-ui.properties 文件中的 com.hp.nms.ui.sso.protectedDomains 属性和 /var/opt/OV/shared/nnm/conf/lwssofmconf.xml 文件中的 domain 元素设置为相同的值。
8. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到主收集器系统。
9. 通过运行以下命令，停止主收集器：
   在 Windows 上

   %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl 或 %TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl

   在 Linux 上

/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl

10. 在主收集器系统上创建以下目录结构：
在 Windows 上

%TrafficDataDir%\shared\nnm\conf\props

在 Linux 上

/var/opt/OV/shared/nnm/conf/props

11. 仅限 Windows：请执行以下步骤：
- 将以下文件从 NNMi 管理服务器的 %NnmDataDir%\shared\nnm\conf 目录复制到主收集器系统上的 %TrafficDataDir%\shared\nnm\conf 目录中：
lwssofmconf.xml

- 将以下文件从 NNMi 管理服务器的 %NnmDataDir%\shared\nnm\conf\props 目录复制到主收集器系统上的 %TrafficDataDir%\shared\nnm\conf\props 目录中：
nms-ui.properties

12. 仅限 Linux：请执行以下步骤：
- 将以下文件从 NNMi 管理服务器的 /var/opt/OV/shared/nnm/conf 目录复制到主收集器系统上的 /var/opt/OV/shared/nnm/conf 目录中：
lwssofmconf.xml

- 将以下文件从 NNMi 管理服务器的 /var/opt/OV/shared/nnm/conf/props 目录复制到主收集器系统上的 /var/opt/OV/shared/nnm/conf/props 目录中：
nms-ui.properties

13. 导航到以下目录：
在 Windows 上

%TrafficDataDir%\shared\nnm\conf\props

在 Linux 上

/var/opt/OV/shared/nnm/conf/props

14. 使用文本编辑器打开 nms-ui.properties 文件。
15. 在主收集器上的 nms-ui.properties 文件中，将以下条目的值指定为 true：
com.hp.nms.ui.sso.isEnabled = true
16. 通过运行以下命令，启动主收集器：
在 Windows 上

%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl 或
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl

在 Linux 上

/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl

17. 在主收集器系统上运行以下命令：
在 Windows 上

%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterssoreload.ovpl

在 Linux 上

/opt/OV/traffic-master/bin/nmstrafficmasterssoreload.ovpl

18. 清除浏览器 Cookie，并以非系统用户身份使用新浏览器会话再次登录到 NNMi 控制台。
19. 启动 NNM iSPI Performance for Traffic 配置表单。启用 SSO 后，将不必提供登录凭据即可访问 NNM iSPI Performance for Traffic 配置表单。

配置使用公钥基础结构验证访问

此部分描述配置 NNM iSPI Performance for Traffic 使用 PKI 验证所需的步骤。使用 PKI 验证，不必提供登录凭据即可访问 NNM iSPI Performance for Traffic 控制台。

备注：当 NNMi 配置为使用 PKI 验证时，iSPI 也必须使用 PKI 验证。当 NNMi 继续使用基于凭据的验证时，不得配置为仅 iSPI 使用 PKI 验证。

将 iSPI 配置为使用 PKI 验证涉及以下步骤：

1. 配置 NNMi
2. 配置证书验证方法
3. 配置 NNM iSPI Performance for Traffic

备注：如果在主收集器处于 HA 群集中时将 NNM iSPI Performance for Traffic 配置为使用 PKI 验证，则必须在主(主动)和辅助(被动)服务器上执行所需的配置任务。

1. 配置 NNMi
   要将 NNMi 配置为使用 PKI 验证，请按《HPE Network Node Manager 部署参考》指南的“将 NNMi 配置为支持公钥基础结构验证”部分中的步骤操作。

   将 NNMi 配置为使用 PKI 验证后，如果不执行步骤 3，系统将在您尝试启动 NNM iSPI Performance for Traffic 配置表单时提示您提供 NNMi 用户名和密码。
2. 配置证书验证方法
   将 NNMi 配置为使用 PKI 验证后，必须阻止使用无效证书的未经授权访问。必须执行其他步骤将 NNMi 配置为使用证书验证方法 - 证书吊销列表 (CRL) 或在线证书状态协议 (OCSP)。

   按《HPE Network Node Manager 部署参考》指南的“证书验证(CRL 和 OCSP)”部分中的步骤操作。
3. 配置 NNM iSPI Performance for Traffic
   将 NNMi 配置为使用 PKI 验证必须更新 `nms-auth-config.xml` 文件，该文件位于 NNMi 配置数据目录中(在 Windows 上是 `%nnmdatadir%\nmsas\NNM\conf`；在 UNIX/Linux 上是 `/var/opt/OV/nmsas/NNM/conf`)。必须根据已更新的 `nms-auth-config.xml` 文件修改 iSPI 配置数据目录中的 `nms-auth-config.xml` 文件，以便 iSPI 使用 PKI 验证。

   主收集器和 NNMi 安装在同一个系统中

   要将 NNM iSPI Performance for Traffic 配置为使用 PKI 验证，请执行以下步骤：

   a. 确保已完成步骤 1 和步骤 2。
   b. 登录到主收集器系统。
   c. 导航到以下目录：
      在 Windows 上

      `%nnmdatadir%\nmsas\traffic-master\conf`

      在 Linux 上

      `/var/opt/OV/nmsas/traffic-master/conf`
   d. 使用文本编辑器打开 `nms-auth-config.xml` 文件。
   e. 在主收集器上修改 `nms-auth-config.xml` 文件以启用 PKI 验证。有关所需更改的信息，请参阅《HPE Network Node Manager 部署参考》中的“为 NNMi 配置 PKI(X.509 证书验证)”部分。

备注： 务必修改 iSPI nms-auth-config.xml 文件，以便与 NNMi 管理服务器上对 nms-auth-config.xml 文件所做的更改匹配。

f. 保存并关闭该文件。

g. 在命令提示符处运行以下命令：
在 Windows 上

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterauthreload.ovpl
```

在 Linux 上

```
/opt/OV/traffic-master/bin/nmstrafficmasterauthreload.ovpl
```

主收集器和 NNMi 安装在单独的系统中

备注： 如果在 HA 下进行文件修改，则必须在群集中的两个节点上进行修改。对于使用 HA 配置的主收集器，如果更改需要停止并重新启动主收集器系统，则必须在运行 nmstrafficmasterstop.ovpl 和 nmstrafficmasterstart.ovpl 命令之前，将节点置于维护模式。

要将 NNM iSPI Performance for Traffic 配置为使用 PKI 验证，请执行以下步骤：

a. 登录到主收集器系统。

b. 导航到包含 nnm.truststore 文件的目录：
在 Windows 上

```
%TrafficDataDir%\shared\nnm\certificates
```

在 Linux 上

```
/var/opt/OV/shared/nnm/certificates
```

c. 必须将受信任的 CA 证书(必要时为整个链)导入到 nnm.truststore 文件中。

d. 例如，mycompany_ca.cer 文件包含您必须使用的证书。运行以下命令将 CA 证书导入到 NNMi nnm.truststore 文件：
在 Windows 上

```
%TrafficInstallDir%\nonOV\jdk\hpsw\bin\keytool -importcert -noprompt -keystore
“%TrafficDataDir%\shared\nnm\certificates\nnm.truststore” -file mycompany_ca.cer
-storepass ovpass -alias <别名>
```

在 Linux 上

```
/opt/OV/nonOV/jdk/hpsw/bin/keytool -importcert -noprompt -keystore
"/var/opt/OV/shared/nnm/certificates/nnm.truststore" -file mycompany_ca.cer -
storepass ovpass -alias <别名>
```

e. 确保已完成步骤 1 和步骤 2。

f. 导航到以下目录：
在 Windows 上

```
%TrafficDataDir%\nmsas\traffic-master\conf
```

在 Linux 上

```
/var/opt/OV/nmsas/traffic-master/conf
```

g. 使用文本编辑器打开 nms-auth-config.xml 文件。

h. 在主收集器上修改 nms-auth-config.xml 文件以启用 PKI 验证。有关所需更改的信息，请参阅《HPE Network Node Manager 部署参考》中的“为 NNMi 配置 PKI(X.509 证书验证)”

部分。

备注： 务必修改 iSPI nms-auth-config.xml 文件，以便与 NNMi 管理服务器上对 nms-auth-config.xml 文件所做的更改匹配。

i. 保存并关闭该文件。

j. 在主收集器系统上运行以下命令：
在 Windows 上

```
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterauthreload.ovpl
```

在 Linux 上

```
/opt/OV/traffic-master/bin/nmstrafficmasterauthreload.ovpl
```

启用安全性

此部分描述在 NNM iSPI Performance for Traffic 上启用安全性所需的步骤。您可以启用以下设备间的安全通信：

- NNMi 管理服务器和 NNM iSPI Performance for Traffic
- NNM iSPI Performance for Traffic 和 NPS
- 主收集器和叶收集器

启用 NNMi 和 NNM iSPI Performance for Traffic 间的安全通信

主收集器和 NNMi 安装在同一个系统中

要在主收集器和 NNMi 管理服务器安装在同一个系统中时，启用 NNMi 和 NNM iSPI Performance for Traffic 间的安全通信，请执行以下步骤：

1. 登录到主收集器系统。
2. 使用以下命令停止主收集器进程：
在 Windows 上
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
在 Linux 上
/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl
3. 导航到以下目录：
在 Windows 上
%NnmDataDir%\nmsas\traffic-master\conf
在 Linux 上
/var/opt/OV/nmsas/traffic-master/conf
4. 用文本编辑器打开 nnm.extended.properties 文件。
5. 将以下属性的值设置为 true：
   - com.hp.ov.nms.spi.traffic-master.spi.isSecure
   - com.hp.ov.nms.spi.traffic-master.Nnm.isSecure

备注： 如果在安装 NNM iSPI Performance for Traffic 时已启用是否安全选项，则不必设置以上属性。

备注： 如果 NNMi 管理服务器已配置应用程序故障转移，则将 com.hp.ov.nms.spi.traffic-master.Nnm.secondary.isSecure 属性设置为 true。

6. 将以下属性的值设置为 https：
   - com.hp.ov.nms.spi.traffic-master.spi.secureprotocol
   - com.hp.ov.nms.spi.traffic-master.Nnm.secureprotocol

   备注： 如果 NNMi 管理服务器已配置应用程序故障转移，则将 com.hp.ov.nms.spi.traffic-master.Nnm.secondary.secureprotocol 设置为 https。
7. 将以下属性的值设置为 NNMi 管理服务器的 HTTPS 端口号：
   - com.hp.ov.nms.spi.traffic-master.Nnm.secureport
   - com.hp.ov.nms.spi.traffic-master.Nnm.https.port

   备注： 如果 NNMi 管理服务器已配置应用程序故障转移，则将以下属性的值设置为 NNMi 管理服务器的 HTTPS 端口号：
   - com.hp.ov.nms.spi.traffic-master.Nnm.secondary.secureport
   - com.hp.ov.nms.spi.traffic-master.Nnm.secondary.https.port
8. 导航到以下目录：
   在 Windows 上
   %NnmInstallDir%\traffic-master\server\conf
   在 Linux 上
   /opt/OV/traffic-master/server/conf
9. 使用文本编辑器打开 login-config.xml 文件。
10. 搜索以下字符串：
    <application-policy name="nnm">
11. 找到 <module-option name="nnmAuthUrl">http://<NNM 主机>:<NNM 端口>/spilogin/auth</module-option> 属性，并进行以下更改：
    - 将 http 更改为 https
    - 将 NNMi 管理服务器的 HTTP 端口号更改为 NNMi 管理服务器的 HTTPS 端口号
12. 保存并关闭该文件。
13. 使用以下命令重新启动主收集器进程：
    在 Windows 上
    %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
    在 Linux 上
    /opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl

主收集器和 NNMi 安装在单独的系统中

要在主收集器和 NNMi 管理服务器未安装在同一个系统中时，启用 NNMi 和 NNM iSPI Performance for Traffic 间的安全通信，请执行以下步骤：

1. 登录到主收集器系统。
2. 使用以下命令停止主收集器进程：
   在 Windows 上
   `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`
   在 Linux 上
   `/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl`
3. 导航到以下目录：
   在 Windows 上
   `%TrafficDataDir%\nmsas\traffic-master\conf`
   在 Linux 上
   `/var/opt/OV/nmsas/traffic-master/conf`
4. 用文本编辑器打开 `nnm.extended.properties` 文件。
5. 将以下属性的值设置为 `true`：
   - `com.hp.ov.nms.spi.traffic-master.spi.isSecure`
   - `com.hp.ov.nms.spi.traffic-master.Nnm.isSecure`

   备注： 如果在安装 NNM iSPI Performance for Traffic 时已启用是否安全选项，则不必设置以上属性。

   备注： 如果 NNMi 管理服务器已配置应用程序故障转移，则将 `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.isSecure` 属性设置为 `true`。
6. 将以下属性的值设置为 `https`：
   - `com.hp.ov.nms.spi.traffic-master.spi.secureprotocol`
   - `com.hp.ov.nms.spi.traffic-master.Nnm.secureprotocol`

   备注： 如果 NNMi 管理服务器已配置应用程序故障转移，则将 `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.secureprotocol` 设置为 `https`。
7. 将以下属性的值设置为 NNMi 管理服务器的 HTTPS 端口号：
   - `com.hp.ov.nms.spi.traffic-master.Nnm.secureport`
   - `com.hp.ov.nms.spi.traffic-master.Nnm.https.port`

   备注： 如果 NNMi 管理服务器已配置应用程序故障转移，则将以下属性的值设置为 NNMi 管理服务器的 HTTPS 端口号：

- com.hp.ov.nms.spi.traffic-master.Nnm.secondary.secureport
- com.hp.ov.nms.spi.traffic-master.Nnm.secondary.https.port

8. 导航到以下目录：
   在 Windows 上
   %TrafficInstallDir%\traffic-master\server\conf
   在 Linux 上
   /opt/OV/traffic-master/server/conf
9. 使用文本编辑器打开 login-config.xml 文件。
10. 搜索以下字符串：
    <application-policy name="nnm">
11. 找到 <module-option name="nnmAuthUrl">http://<NNM 主机>:<NNM 端口>/spilogin/auth</module-option> 属性，并进行以下更改：
    - 将 http 更改为 https
    - 将 NNMi 管理服务器的 HTTP 端口号更改为 NNMi 管理服务器的 HTTPS 端口号
12. 保存并关闭该文件。
13. 登录 NNMi 管理服务器。
14. 导航到以下目录：
    在 Windows 上
    %NNMDataDir%\shared\nnm\certificates
    在 Linux 上
    /var/opt/OV/shared/nnm/certificates
15. 将 nnm.cert 文件复制到主收集器系统的临时目录中。

    备注： 如果在 %NnmDataDir%\shared\nnm\certificates\ 文件夹中未找到 nnm.cert 文件，请执行以下步骤：

    a. 运行以下命令生成 nnm.cert 文件：
       在 Windows 上
       %NnmInstallDir%\bin\nnmkeytool.ovpl -export -file c:\nnm.cert -keystore nnm-key.p12 -storetype PKCS12 -storepass nnmkeypass -alias <nnmi_FQDN>.selfsigned
       在 Linux 上
       $NnmInstallDir/bin/nnmkeytool.ovpl -export -file /tmp/nnm.cert -keystore nnm-key.p12 -storetype PKCS12 -storepass nnmkeypass -alias <nnmi_FQDN>.selfsigned
       在本实例中，<NNMi FQDN> 是 NNMi 管理服务器的 FQDN。
    b. 将 nnm.cert 文件复制到主收集器系统的临时目录中。
16. 在主收集器上运行以下命令，将证书添加到信任库：
    在 Windows 上
    %TrafficInstallDir%\nonOV\jdk\hpsw\bin\keytool -importcert -file "<tmp>/nnm.cert" -

keystore "%TrafficDataDir%/shared/nnm/certificates/nnm.truststore" -storepass ovpass -noprompt -alias <NNMi FQDN>

在 Linux 上
/opt/OV/nonOV/jdk/hpsw/bin/keytool -importcert -file "<tmp>/nnm.cert" -keystore "/var/opt/OV/shared/nnm/certificates/nnm.truststore" -storepass ovpass -noprompt -alias <NNMi FQDN>

在本实例中，<NNMi FQDN> 是 NNMi 管理服务器的 FQDN。

17. 在主收集器上运行以下命令，验证证书已添加到信任库：
在 Windows 上
%TrafficInstallDir%\nonOV\jdk\hpsw\bin\keytool -list -keystore "%TrafficDataDir%\shared\nnm\certificates\nnm.truststore" -storepass ovpass

在 Linux 上
/opt/OV/nonOV/jdk/hpsw/bin/keytool -list -keystore "/var/opt/OV/shared/nnm/certificates/nnm.truststore" -storepass ovpass

18. 使用以下命令重新启动主收集器进程：
在 Windows 上
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl

在 Linux 上
/opt/OV/traffic-leaf/bin/nmstrafficmasterstart.ovpl

启用主收集器和 NPS 间的安全通信

要在 NPS 以安全模式运行时启用主收集器和 NPS 间的安全通信，请执行以下步骤：

1. 导出第三方 Cognos 证书

   要使用浏览器密钥库导出 Cognos 证书，请执行以下步骤：

   a. 通过在浏览器中输入以下 URL 直接登录到 NPS：
   https://<完全限定域名>:<NPS HTTPS 端口>

   在此实例中，<完全限定域名> 是 NPS 系统的完全限定域名，<NPS HTTPS 端口> 是 NPS 用于安全通信的 HTTPS 端口。NPS 用于安全通信的默认端口是 9305。

   b. 查看证书，并将它导出为 DER 编码的二进制文件。将该文件命名为 trafficcert.cer。

   备注： 忽略可能看到的任何警告消息。

   c. 将导出的证书复制到主收集器上的某个临时位置。

2. 将第三方 Cognos 证书导入到 nnm.truststore。

   要将证书导入到 nnm.truststore，请执行以下步骤：

   a. 使用以下命令停止主收集器进程：
   在 Windows 上
   %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl

   或

   %TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl

   在 Linux 上
   /opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl

   如果已将主收集器安装在 NNMi 管理服务器上，则必须在将该证书导入到 nnm.truststore 之前，通过运行 ovstop -c ovjboss 命令停止 NNMi 进程。

b. 将 Cognos 证书导入 nnm.truststore 文件。
例如，trafficcert.cer 文件包含您必须使用的证书。运行以下命令将 CA 证书导入到 nnm.truststore 文件：

在 Windows 上
```
%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool -importcert -noprompt -keystore "%NnmDataDir%\shared\nnm\certificates\nnm.truststore" -file trafficcert.cer -storepass ovpass -alias cognos
```
或
```
%TrafficInstallDir%\nonOV\jdk\hpsw\bin\keytool -importcert -noprompt -keystore "%TrafficDataDir%\shared\nnm\certificates\nnm.truststore" -file trafficcert.cer -storepass ovpass -alias cognos
```
在 Linux 上
```
/opt/OV/nonOV/jdk/hpsw/bin/keytool -importcert -noprompt -keystore "/var/opt/OV/shared/nnm/certificates/nnm.truststore" -file trafficcert.cer -storepass ovpass -alias cognos
```

备注：忽略可能看到的任何警告消息。

使用的 keytool 应当是 Oracle 实现，而不是 GNU 实现。

如果已在步骤 a 中停止了 NNMi 进程，则必须在将该证书导入到 nnm.truststore 之后，通过运行 ovstart -c ovjboss 命令启动 NNMi 进程。

c. 使用以下命令启动主收集器进程：
在 Windows 上
```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```
或
```
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```
在 Linux 上
```
/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl
```

启用主收集器和叶收集器间的安全通信

在叶收集器安装期间，安装脚本将为叶收集器系统创建自签名证书。此证书包含的别名含有节点的完全限定域名。安装脚本将此自签名证书添加到叶收集器系统上的 nnm.keystore、nnm.truststore 和 nnm.cert 文件中。

安装主收集器和叶收集器后，您可以通过使用叶收集器系统的自签名证书使主收集器使用 HTTPS 协议与叶收集器系统通信。

要启用主收集器和叶收集器间的安全通信，请执行以下步骤：

1. 将叶收集器证书添加为主收集器上的受信任证书。
当主收集器和叶收集器安装在同一个系统中时，将叶收集器证书添加为受信任证书不需要额外的步骤。

   当主收集器和叶收集器安装在单独的系统中时，请为每个叶收集器系统执行以下步骤：

   a. 登录到叶收集器系统。

   b. 导航到包含叶收集器证书文件 nnm.cert 的目录：
   在 Windows 上
   ```
   %NnmDataDir%\shared\nnm\certificates
   ```

或

%TrafficDataDir%\shared\nnm\certificates

在 Linux 上
/var/opt/OV/shared/nnm/certificates

c. 将叶收集器证书复制到主收集器系统中。

备注：如果在 HA 下进行文件修改，则必须在群集中的两个节点上进行修改。对于使用 HA 配置的主收集器，如果更改需要停止并重新启动主收集器系统，则必须在运行 nmstrafficmasterstop.ovpl 和 nmstrafficmasterstart.ovpl 命令之前，将节点置于维护模式。

d. 通过运行以下命令，停止主收集器：
在 Windows 上
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl

或

%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl

在 Linux 上
/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl

如果已将主收集器安装在 NNMi 管理服务器上，则必须在将该证书导入到 nnm.truststore 之前，通过运行 ovstop -c ovjboss 命令停止 NNMi 进程。

e. 将叶收集器证书导入 nnm.truststore 文件。
例如，leaf.cert 文件包含您必须使用的叶收集器证书。leaf.cert 文件可以是您需要导入的证书颁发机构的自签名证书或签名证书。
运行以下命令将 CA 证书导入到 nnm.truststore 文件：
在 Windows 上
%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool -importcert -noprompt -keystore "%NnmDataDir%\shared\nnm\certificates\nnm.truststore" -file leaf.cert -storepass ovpass -alias <叶收集器 FQDN>

或

%TrafficInstallDir%\nonOV\jdk\hpsw\bin\keytool -importcert -noprompt -keystore "%TrafficDataDir%\shared\nnm\certificates\nnm.truststore" -file leaf.cert -storepass ovpass -alias <叶收集器 FQDN>

在 Linux 上
/opt/OV/nonOV/jdk/hpsw/bin/keytool -importcert -noprompt -keystore "/var/opt/OV/shared/nnm/certificates/nnm.truststore" -file leaf.cert -storepass ovpass -alias <叶收集器 FQDN>

如果已在步骤 d 中停止了 NNMi 进程，则必须在将证书导入 nnm.truststore 后启动 NNMi 进程。

f. 通过运行以下命令，启动主收集器：
在 Windows 上
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl

或

%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl

在 Linux 上
/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl

2. 使用系统用户帐户登录到 NNM iSPI Performance for Traffic 配置 UI，启用主收集器和叶收集器间的安全通信。执行《HP Network Node Manager iSPI Performance for Traffic Software 联机帮助》中的“配置叶收集器系统”部分列出的步骤。

使用证书颁发机构的签名证书

要在主收集器上使用证书颁发机构的签名证书而不是自签名证书，请执行以下步骤：

1. 登录到主收集器系统。
2. 通过运行以下命令，停止主收集器：
   在 Windows 上
   `%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`
   或
   `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`
   在 Linux 上
   `/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl`
3. 执行类似于《HPE Network Node Manager i Software 部署参考》的“生成证书颁发机构证书”部分中所列的步骤。
4. 在主收集器上导航到以下目录：
   在 Windows 上
   `%NnmDataDir%\nmsas\traffic-master`
   或
   `%TrafficDataDir%\nmsas\traffic-master`
   在 Linux 上
   `/var/opt/OV/nmsas/traffic-master`
5. 使用文本编辑器打开 `server.properties` 文件。
6. 添加以下属性：
   `nmsas.server.security.keystore.alias=<新别名>`
   在此实例中，<新别名> 是在导入签名证书时提供的别名。
7. 保存并关闭该文件。
8. 通过运行以下命令，启动主收集器：
   在 Windows 上
   `%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl`
   或
   `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl`
   在 Linux 上
   `/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl`

要在叶收集器上使用证书颁发机构的签名证书而不是自签名证书，请执行以下步骤：

1. 登录到叶收集器系统。
2. 通过运行以下命令，停止叶收集器：
   在 Windows 上
   `%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl`
   或
   `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl`

在 Linux 上
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl

3. 执行类似于《HPE Network Node Manager i Software 部署参考》的“生成证书颁发机构证书”部分中所列的步骤。
4. 在叶收集器上导航到以下目录：
在 Windows 上

   %NnmDataDir%\nmsas\traffic-leaf

   或

   %TrafficDataDir%\nmsas\traffic-leaf

   在 Linux 上

   /var/opt/OV/nmsas/traffic-leaf
5. 使用文本编辑器打开 server.properties 文件。
6. 添加以下属性：
nmsas.server.security.keystore.alias=<新别名>
在此实例中，<新别名>是在导入签名证书时提供的别名。
7. 保存并关闭该文件。
8. 通过运行以下命令，启动叶收集器：
在 Windows 上
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl

   或

   %TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl

   在 Linux 上
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl

第 6 章: 在高可用性群集中部署 NNM iSPI Performance for Traffic

可以在高可用性 (HA) 环境中安装 NNM iSPI Performance for Traffic，以便在监视设置中实现冗余。由于 NNM iSPI Performance for Traffic 由可安装在不同系统上的多个组件组成，您可以从多个部署场景选择 NNM iSPI Performance for Traffic 的 HA 实现。

支持的 HA 产品

HP Network Node Manager iSPI Performance for Traffic Software 提供的用于配置和运行 HA 下的 NNM iSPI Performance for Traffic 的命令将用于指定操作系统的以下 HA 产品：

- Veritas Cluster Server (VCS) V5.0
- Veritas Cluster Server (VCS) V5.1
- Windows 2008 和 2008 R2 的 Microsoft 群集服务

虽然可以按照本章中的操作步骤将 NNM iSPI Performance for Traffic 配置为在其他 HA 产品下运行，但 HPE 不对其他配置的群集配置问题提供支持。

为 NNM iSPI Performance for Traffic 配置 HA 的先决条件

要作为节点包含在 NNM iSPI Performance for Traffic HA 群集中的任何系统都必须满足以下要求：

- 支持使用虚拟 IP 地址。
- 支持使用共享磁盘。
- 满足 NNM iSPI Performance for Traffic 的所有要求，如《NNMi Ultimate Support Matrix》中所述。
- 满足计划运行 NNM iSPI Performance for Traffic 的 HA 产品的文档中描述的所有要求。
- 在开始为 NNM iSPI Performance for Traffic 配置 HA 之前，使用针对您的 HA 产品的命令配置和测试 HA 群集。HA 群集提供诸如检查应用程序检测信号和启动故障转移之类的功能。
  HA 群集配置必须至少包含以下各项：
  - (仅限 Linux) ssh
  - (仅限 Linux) remsh
- HA 群集的可 DNS 解析的虚拟 IP 地址
- HA 群集的可 DNS 解析的虚拟主机名

HA 安装环境

在 NNM iSPI Performance for Traffic 的三个组件中，只有主收集器可以安装在 HA 群集下。在将 NNMi 安装在 HA 群集下的环境中，可以选择将主收集器安装在同一个群集或不同群集中。

要在 HA 群集中安装主收集器，可以选择以下选项之一：

- NNMi 和主收集器在同一个群集中
- 只有主收集器在 HA 群集中

如果将 NNMi 安装在 HA 群集中，则必须在该群集中的所有 NNMi 管理服务器上安装 NNMi Extension for iSPI Performance for Traffic。

NNMi 和主收集器在同一个 HA 群集中

在此场景中，可选择在 NNMi 管理服务器上将主收集器作为加载项产品安装。

备注： NPS 可安装在 HA 中，也可不安装在 HA 中。但是，要确保未在 NNMi 管理服务器上安装 NPS。NPS 和主收集器不能同时作为 HA 产品存在于同一个 HA 群集中。

在具有 NNMi 和主收集器的一组系统中配置 HA 群集

如果将 NNMi 和主收集器安装在至少两个系统上，则可以创建 HA 群集，并将 NNMi 和收集器配置为在 HA 环境下运行。

可以在 HA 环境中的主节点和辅助节点上配置 NNMi 和 主收集器。有关如何在 HA 环境中安装 NNMi 的详细信息，请参阅《NNMi 部署参考》指南。

在主节点上配置主收集器涉及以下任务：

1. 安装 NNMi 和主收集器
   在每个系统上安装 NNMi 和主收集器。有关详细信息，请参阅《NNMi 交互安装指南》和HP Network Node Manager iSPI Performance for Traffic 交互安装指南。
2. 在 HA 群集中的每个服务器上安装 HPE NNMi Extension for iSPI Performance for Traffic。安装 HPE NNMi Extension for iSPI Performance for Traffic 时，请将 NNMi 服务器的虚拟 FQDN 指定为主收集器系统的 FQDN。
3. 将 NNMi 配置为在 HA 环境下运行
   在系统上配置 HA 软件，并将 NNMi 配置为在 HA 环境下运行。有关将 NNMi 配置为在 HA 环境下运行的信息，请参阅《NNMi 部署参考》指南。
4. 在主(主动)节点上配置主收集器
   要在主(主动)节点上配置主收集器，请执行以下步骤：
   a. 运行以下命令查找虚拟主机名：
      `nnmofficialfqdn.ovpl`
   b. 修改 `%NnmInstallDir%\traffic-master\server\conf%NnmInstallDir%\conf\traffic-master` 或 `/opt/OV/traffic-master/server/conf/opt/OV/conf/traffic-master` 目录中的 `login-config.xml` 文件以反映 NNMi 管理服务器的虚拟 FQDN：

c. 用文本编辑器打开 login-config.xml 文件。
d. 查找元素 <module-option name="nnmAuthUrl">。
e. 修改元素中包含的字符串，使之反映 NNMi 管理服务器的虚拟 FQDN。
f. 保存该文件。
g. 转到以下目录：
在 Windows 上

%NnmDataDir%\nmsas\traffic-master\conf

在 Linux 上

/var/opt/OV/nmsas/traffic-master/conf

h. 在 nnm.extended.properties 文件中，将 com.hp.ov.nms.spi.traffic-master.Nnm.perfspidatapath 属性设置为 nnmenableperfspi.ovpl 脚本显示的值。

备注： 在 NNMi 系统上，nnmenableperfspi.ovpl 脚本会在 nnmenableperfspi_log.txt 文件(位于 %NnmDataDir%\log 或 /var/opt/OV/log 目录中)中记录所有详细信息，可供您参考。

i. 默认值为：
在 Windows 上

%HA_MOUNT_POINT%\NNM\dataDir\shared\perfSpi\datafiles

在 Linux 上

$HA_MOUNT_POINT/NNM/dataDir/shared/perfSpi/datafiles

备注： 安装点是装载 NNMi 共享磁盘的目录位置。此安装点必须在各个系统间保持一致。(即每个节点必须使用相同的安装点名称。)例如：

Windows：S:\
确保完整地指定驱动器。S 和 S: 不是可接受的格式，不能对共享磁盘进行访问。

Linux：/nnmmount

j. 如果不想在主收集器处于 HA 群集中时将 NNM iSPI Performance for Traffic 配置为使用 PKI 验证，请转到步骤 n。
如果在主收集器处于 HA 群集中时将 NNM iSPI Performance for Traffic 配置为使用 PKI 验证，则必须在主(主动)服务器上执行所需的配置更改。

备注： 对于使用 HA 配置的主收集器，如果更改需要停止并重新启动主收集器系统，则必须在运行 nmstrafficmasterstop.ovpl 和 nmstrafficmasterstart.ovpl 命令之前，将主动节点置于维护模式。

k. 导航到以下目录：
在 Windows 上

%nnmdatadir%\nmsas\traffic-master\conf

在 Linux 上

/var/opt/OV/nmsas/traffic-master/conf

l. 使用文本编辑器打开 nms-auth-config.xml 文件。

m. 在主收集器上修改 nms-auth-config.xml 文件以启用 PKI 验证。有关所需更改的信息，请参阅《HPE Network Node Manager 部署参考》指南中的“为 NNMi 配置 PKI(X.509 证书验证)”部分。

备注： 务必修改 iSPI nms-auth-config.xml 文件，以便与 NNMi 管理服务器上对 nms-auth-config.xml 文件所做的更改匹配。

n. 运行以下命令，将主收集器配置为在 HA 群集下运行：
对于 Windows

```
%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon TRAFFIC
```

对于 Linux

```
/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon TRAFFIC
```

5. 在辅助(被动)节点上配置主收集器
要在辅助(被动)节点上配置主收集器，请执行以下步骤：

a. 在辅助节点上安装 NNMi 与主收集器。确保辅助节点在安装期间有单独的完全限定域名(FQDN)。有关详细信息，请参阅《NNMi 交互安装指南》和HP Network Node Manager iSPI Performance for Traffic 交互安装指南。

b. 运行以下命令查找虚拟主机名：
nnmofficialfqdn.ovpl

c. 修改 %NnmInstallDir%\traffic-master\server\conf%NnmInstallDir%\conf\traffic-master 或 /opt/OV/traffic-master/server/conf/opt/OV/conf/traffic-master 目录中的 login-config.xml 文件以反映 NNMi 管理服务器的虚拟 FQDN：

d. 用文本编辑器打开 login-config.xml 文件。

e. 查找元素 <module-option name=”nnmAuthUrl”>。

f. 修改元素中包含的字符串，使之反映 NNMi 管理服务器的虚拟 FQDN。

g. 保存该文件。

h. 转到以下目录：
在 Windows 上

```
%NnmDataDir%\nmsas\traffic-master\conf
```

在 Linux 上

```
/var/opt/OV/nmsas/traffic-master/conf
```

i. 在 nnm.extended.properties 文件中，将 com.hp.ov.nms.spi.traffic-master.Nnm.perfspidatapath 属性设置为 nnmenableperfspi.ovpl 脚本显示的值。
在 NNMi 系统上，nnmenableperfspi.ovpl 脚本会在 nnmenableperfspi_log.txt 文件(位于 %NnmDataDir%\log 或 /var/opt/OV/log 目录中)中记录所有详细信息，可供您参考。
默认值为：

在 Windows 上： %HA_MOUNT_POINT%\NNM\dataDir\shared\perfSpi\datafiles

在 Linux 上： $HA_MOUNT_POINT/NNM/dataDir/shared/perfSpi/datafiles

j. 如果不想在主收集器处于 HA 群集中时将 NNM iSPI Performance for Traffic 配置为使用 PKI 验证，请转到步骤 p。

k. 如果在主收集器处于 HA 群集中时将 NNM iSPI Performance for Traffic 配置为使用 PKI 验证，则必须在辅助(被动)服务器上执行所需的配置更改。

l. 对于使用 HA 配置的主收集器，如果更改需要停止并重新启动主收集器系统，则必须在运行 nmstrafficmasterstop.ovpl 和 nmstrafficmasterstart.ovpl 命令之前，将被动节点

置于维护模式。

m. 导航到以下目录：
在 Windows 上

```
%nnmdatadir%\nmsas\traffic-master\conf
```

在 Linux 上

```
/var/opt/OV/nmsas/traffic-master/conf
```

n. 使用文本编辑器打开 nms-auth-config.xml 文件。

o. 在主收集器上修改 nms-auth-config.xml 文件以启用 PKI 验证。有关所需更改的信息，请参阅《HPE Network Node Manager 部署参考》中的“为 NNMi 配置 PKI(X.509 证书验证)”部分。

备注：务必修改 iSPI nms-auth-config.xml 文件，以便与 NNMi 管理服务器上对 nms-auth-config.xml 文件所做的更改匹配。

p. 运行以下命令，将辅助节点上的 主收集器 配置为在 HA 群集下运行：
对于 Windows

```
%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon TRAFFIC
```

对于 Linux

```
/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon TRAFFIC
```

6. 在 HA 群集中配置每个被动节点
在 HA 群集中的每个被动节点上重复步骤 4。

取消配置 HA 群集中的 NNM iSPI Performance for Traffic

从 HA 群集删除 NNM iSPI Performance for Traffic 节点的过程涉及撤销该 NNM iSPI Performance for Traffic 主收集器实例的 HA 配置。然后，可以将该 NNM iSPI Performance for Traffic 主收集器实例作为独立系统运行，或从该节点卸载 NNM iSPI Performance for Traffic 主收集器。

如果要保持为 NNM iSPI Performance for Traffic 配置高可用性，HA 群集必须包含一个主动运行 NNM iSPI Performance for Traffic 主收集器的节点和至少一个被动 NNM iSPI Performance for Traffic 主收集器节点。

如果要从 HA 群集完全删除 NNM iSPI Performance for Traffic 主收集器，请在该群集中的所有节点上取消配置 HA 功能。

要完全取消配置 HA 群集中的 NNM iSPI Performance for Traffic，请执行以下步骤：

1. 确定该 HA 群集中哪个节点是主动节点。在任何节点上，运行以下命令：
在 Windows 上

```
%NNMInstallDir%\traffic-master\misc\nnm\ha\nnmhaclusterinfo.ovpl -group <资源组> -activeNode 或 %TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhaclusterinfo.ovpl -group <资源组> -activeNode
```

在 Linux 上

```
/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -group <资源组> -activeNode
```

2. 在每个被动节点上，取消配置 HA 群集中的 NNMi：

%NnmInstallDir%\traffic-master\misc\nnm\ha\nnmhaunconfigure.ovpl TRAFFIC <资源组> 或 %TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhaunconfigure.ovpl TRAFFIC <资源组>

/opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl TRAFFIC <资源组>

此命令删除对共享磁盘的访问，但不取消配置磁盘组或卷组。

3. 在每个被动节点上，删除特定于资源组的文件：
删除以下目录中的所有文件：

在 Windows 上

%NnmInstallDir%\traffic-master\hacluster\<资源组>\ 或 %TrafficInstallDir%\traffic-master\hacluster\<资源组>\

在 Linux 上

/opt/OV/traffic-master/hacluster/<资源组>

4. 在主动节点上，通过创建以下维护文件，禁用 HA 资源组监视：
%NnmInstallDir%\traffic-master\hacluster\<资源组>\maintenance 或 %TrafficInstallDir%\traffic-master\hacluster\<资源组>\maintenance

/opt/OV/hacluster/<资源组>/maintenance

文件可以为空。

5. 使用以下命令停止 Traffic 主收集器：

nmstrafficmasterstop.ovpl --HA

为防止数据损坏，请确保没有 Traffic 主收集器实例在运行并且在访问共享磁盘。

6. 在主动节点上运行以下命令：
nnmhadisk.ovpl TRAFFIC -from <安装点>
7. 从共享磁盘上删除所有文件。
8. 删除维护文件。

在 Windows 上

del %NnmDataDir%\hacluster\<资源组>\maintenance 或 del %TrafficDataDir%\hacluster\<资源组>\maintenance

在 Linux 上

rm -rf /opt/OV/hacluster/<资源组>/maintenance

9. 在主动节点上，停止 NNM iSPI Performance for Traffic 主收集器 HA 资源组：

在 Windows 上

%NnmInstallDir%\traffic-master\misc\nnm\ha\nnmhastoprg.ovpl TRAFFIC <资源组> 或 %TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhastoprg.ovpl TRAFFIC <资源组>

在 Linux 上

/opt/OV/misc/nnm/ha/nnmhastoprg.ovpl TRAFFIC <资源组>

10. 在主动节点上，取消配置 HA 群集中的 NNM iSPI Performance for Traffic：

在 Windows 上

%NnmInstallDir%\traffic-master\misc\nnm\ha\nnmhaunconfigure.ovpl TRAFFIC <资源组> 或 %TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhaunconfigure.ovpl TRAFFIC <资源组>

在 Linux 上

/opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl TRAFFIC <资源组>

此命令删除对共享磁盘的访问，但不取消配置磁盘组或卷组。

11. 在主动节点上，删除特定于资源组的文件。

    删除以下目录中的所有文件：

    在 Windows 上

    `%NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\` 或
    `%TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\`

    在 Linux 上

    `/var/opt/OV/hacluster/<资源组>/`

12. 卸载共享磁盘。
    - 如果需要在某个时候重新配置 NNM iSPI Performance for Traffic HA 群集，可以使磁盘保持当前状态。
    - 如果要将该共享磁盘用于其他用途，请复制要保留的所有数据(如下一个操作步骤中所述)，然后使用 HA 产品命令取消配置磁盘组和卷组。

13. 取消配置 HA 中的所有节点后，修改以下文件，将主收集器的主机名从虚拟 IP 更改为该节点的实际主机名：

    在 Windows 上

    `%NnmDataDir%\shared\traffic-master\conf\nnm.extended.properties` 或
    `%TrafficDataDir%\shared\traffic-master\conf\nnm.extended.properties`

    在 Linux 上

    `/var/opt/OV/shared/traffic-master/conf/nnm.extended.properties`

14. 对于加载项主收集器，更改以下两个参数：
    - `com.hp.ov.nms.spi.traffic-master.spi.hostname=`<localhost 的 FQDN>
    - `com.hp.ov.nms.spi.traffic-master.Nnm.hostname=`<NNM 服务器的 FQDN>

    对于独立主收集器，更改以下参数：
    - `com.hp.ov.nms.spi.traffic-master.spi.hostname=`<localhost 的 FQDN>
    - `com.hp.ov.nms.spi.traffic-master.Nnm.hostname=`<NNM 服务器的 FQDN>

15. 使用以下命令启动主收集器：
    `nmstrafficmasterstart.ovpl`

取消配置 NNMi HA 群集中的 NNM iSPI Performance for Traffic

在并存设置中，要完全取消配置 HA 群集中的 NNM iSPI Performance for Traffic，请执行以下步骤：

1. 确定该 HA 群集中哪个节点是主动节点。在任何节点上，运行以下命令：

   在 Windows 上：

   `%NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -group <资源组> -activeNode`

在 Linux 上：

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl -group <资源组> -activeNode
```

2. 在每个被动节点上，取消配置 HA 群集中的 NNM iSPI Performance for Traffic 加载项。要取消配置，请运行以下命令：

   在 Windows 上：

   ```
   %NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM -addon TRAFFIC
   ```

   在 Linux 上：

   ```
   $NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM -addon TRAFFIC
   ```

3. 验证是否已在所有群集被动节点上取消配置 NNM iSPI Performance for Traffic 加载项。要进行验证，请运行以下命令：

   在 Windows 上：

   ```
   %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_
   PRODUCTS
   ```

   在 Linux 上：

   ```
   $NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS
   ```

   如果输出中显示任何带 NNM iSPI Performance for Traffic 加载项的被动群集节点，请在该节点上重复执行步骤 2。

4. 现在可以从 HA 群集的活动节点上取消配置 NNM iSPI Performance for Traffic。要取消配置，请运行以下命令：

   在 Windows 上：

   ```
   %NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM -addon TRAFFIC
   ```

   在 Linux 上：

   ```
   $NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM -addon TRAFFIC
   ```

5. 确保 NNMi 正在主动节点上运行。

在 HA 环境中修补 NNM iSPI Performance for Traffic 主收集器

此部分描述当主收集器在 HA 中配置时，安装和卸载 NNM iSPI Performance for Traffic 主收集器补丁程序所需的步骤。此部分提供的步骤适用于 HA 安装环境 (第 28 页)中描述的两个选项。

在 HA 环境中应用主收集器补丁程序的先决条件

在开始主收集器补丁程序安装过程之前，请确保已满足以下先决条件：

- 必须将 NNMi、NNM iSPI Performance for Metrics、NNMi Extension for iSPI Performance for Traffic 和 NNM iSPI Performance for Traffic 叶收集器升级到最新可用的补丁程序。
- 确保将主主收集器节点配置为主动节点。
- 必须先在每个被动主收集器上安装补丁程序，然后在主动主收集器上安装补丁程序。

在 HA 环境中应用主收集器补丁程序

要安装主收集器补丁程序，请按照下面的顺序执行下方列出的步骤：

1. 在被动主收集器上安装主收集器补丁程序 (第 35 页)
2. 在主动主收集器上安装主收集器补丁程序 (第 36 页)
3. 在 HA 环境中重新配置被动主收集器 (第 37 页)

在被动主收集器上安装主收集器补丁程序

要在 HA 环境中的被动主收集器上安装主收集器补丁程序，请执行以下步骤：

1. 通过在每个被动主收集器上创建以下文件将 HA 群集移入维护模式：
   在 Windows 上

   %NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance 或
   %TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance

   %NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM 或
   %TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM

   在 Linux 上

   /var/opt/OV/hacluster/<资源组>/maintenance

   /var/opt/OV/hacluster/<资源组>/maint_NNM
2. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到每个被动主收集器。
3. 运行以下命令将主收集器临时从 HA 群集中删除：
   在 Windows 上
   - NNMi 和主收集器在同一个群集中
     %NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM –addon TRAFFIC

     备注： 当 NNMi 和主收集器处于同一群集中时，确保以下命令不在列表中显示被动主收集器：

     %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS

   - 主收集器在独立 HA 群集中
     %TrafficInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl TRAFFIC <资源组>

     备注： 当主收集器安装在独立 HA 群集中时，确保以下命令不在列表中显示被动主收集器：

     %TrafficInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl –group <资源组> -nodes

   在 Linux 上
   - NNMi 和主收集器在同一个群集中
     /opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl NNM –addon TRAFFIC

备注：当 NNMi 和主收集器处于同一群集中时，确保以下命令不在列表中显示被动主收集器：

```
/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS
```

- 主收集器在独立 HA 群集中
  /opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl TRAFFIC <资源组>

备注：当主收集器安装在独立 HA 群集中时，确保以下命令不在列表中显示被动主收集器：

```
/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl –group <资源组> -nodes
```

4. 如补丁程序文本中所述应用主收集器补丁程序。

备注：在此补丁程序安装到主动主收集器上之前，不要在此被动主收集器上重新配置 HA。

在主动主收集器上安装主收集器补丁程序

1. 要在 HA 环境中的主动主收集器上安装主收集器补丁程序，请执行以下步骤：
2. 通过在主动主收集器上创建以下文件将 HA 群集移入维护模式：
   在 Windows 上

   %NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance 或
   %TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance

   %NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM 或
   %TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM

   在 Linux 上

   /var/opt/OV/hacluster/<资源组>/maintenance

   /var/opt/OV/hacluster/<资源组>/maint_NNM
3. 运行以下命令停止主动主收集器上的主收集器进程：
   在 Windows 上

   %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl --HA 或
   %TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl --HA

   %NnmInstallDir%\nonOV\traffic-master\bin\nmstrafficmasterstop.ovpl --HA 或
   %TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl --HA

   在 Linux 上

   /opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl --HA

   /opt/OV/nonOV/traffic-master/bin/nmstrafficmasterstop.ovpl --HA
4. 如补丁程序文本中所述安装主收集器补丁程序。

备注：不要取消主动主收集器上的 HA 配置。

5. 运行以下命令启动主动主收集器上的主收集器进程：
   在 Windows 上

%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl --HA 或
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl --HA

%NnmInstallDir%\nonOV\traffic-master\bin\nmstrafficmasterstart.ovpl --HA 或
%TrafficInstallDir%\nonOV\traffic-master\bin\nmstrafficmasterstart.ovpl --HA

在 Linux 上

/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl --HA

/opt/OV/nonOV/traffic-master/bin/nmstrafficmasterstart.ovpl --HA

在 HA 环境中重新配置被动主收集器

要在 HA 环境中重新配置被动主收集器，请执行以下步骤：

1. 在每个被动主收集器上，运行以下命令重新配置 HA。
   在 Windows 上
   - NNMi 和主收集器在同一个群集中
     %NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM –addon TRAFFIC

     备注： 当 NNMi 和主收集器处于同一群集中时，确保以下命令在列表中显示被动主收集器：

     %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS

   - 主收集器在独立 HA 群集中
     %TrafficInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl TRAFFIC

     备注： 当主收集器安装在独立 HA 群集中时，确保以下命令在列表中显示被动主收集器：

     %TrafficInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl –group <资源组> -nodes

   对于 Linux
   - NNMi 和主收集器在同一个群集中
     /opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM –addon TRAFFIC

     备注： 当 NNMi 和主收集器处于同一群集中时，确保以下命令在列表中显示被动主收集器：

     /opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS

   - 主收集器在独立 HA 群集中
     /opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl TRAFFIC

     备注： 当主收集器安装在独立 HA 群集中时，确保以下命令在列表中显示被动主收集器：

     /opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl –group <资源组> -nodes

2. 删除以下文件将被动主收集器移出维护模式：
   在 Windows 上

   %NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance 或
   %TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance

   %NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM 或
   %TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM

   在 Linux 上

   /var/opt/OV/hacluster/<资源组>/maintenance

   /var/opt/OV/hacluster/<资源组>/maint_NNM
3. 删除以下文件将主动主收集器移出维护模式：
   在 Windows 上

   %NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance 或
   %TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance

   %NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM 或
   %TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM

   在 Linux 上

   /var/opt/OV/hacluster/<资源组>/maintenance

   /var/opt/OV/hacluster/<资源组>/maint_NNM

卸载 HA 环境中的主收集器补丁程序

要卸载主收集器补丁程序，请按照下面的顺序执行下方列出的步骤：

1. 从被动主收集器卸载主收集器补丁程序 (第 38 页)
2. 从主动主收集器卸载主收集器补丁程序 (第 39 页)
3. 在 HA 环境中重新配置被动主收集器 (第 40 页)

从被动主收集器卸载主收集器补丁程序

要从 HA 环境中的被动主收集器上卸载主收集器补丁程序，请执行以下步骤：

1. 通过在每个被动主收集器上创建以下文件将 HA 群集移入维护模式：
   在 Windows 上

   %NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance 或
   %TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance

   %NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM 或
   %TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM

   在 Linux 上

   /var/opt/OV/hacluster/<资源组>/maintenance

   /var/opt/OV/hacluster/<资源组>/maint_NNM
2. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到每个被动主收集器。
3. 运行以下命令将主收集器临时从 HA 群集中删除：
   在 Windows 上

- NNMi 和主收集器在同一个群集中
  %NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM –addon TRAFFIC

  备注： 当 NNMi 和主收集器处于同一群集中时，确保以下命令不在列表中显示被动主收集器：

  %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS

- 主收集器在独立 HA 群集中
  %TrafficInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl TRAFFIC <资源组>

  备注： 当主收集器安装在独立 HA 群集中时，确保以下命令不在列表中显示被动主收集器：

  %TrafficInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl –group <资源组> -nodes

在 Linux 上

- NNMi 和主收集器在同一个群集中
  /opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl NNM –addon TRAFFIC

  备注： 当 NNMi 和主收集器处于同一群集中时，确保以下命令不在列表中显示被动主收集器：

  /opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS

- 主收集器在独立 HA 群集中
  /opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl TRAFFIC <资源组>

  备注： 当主收集器安装在独立 HA 群集中时，确保以下命令不在列表中显示被动主收集器：

  /opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl –group <资源组> -nodes

4. 如补丁程序文本中所述卸载主收集器补丁程序。

   备注： 在此补丁程序卸载成功之前，不要在此被动主收集器上重新配置 HA。

从主动主收集器卸载主收集器补丁程序

要从 HA 环境中的主动主收集器上卸载主收集器补丁程序，请执行以下步骤：

1. 通过在主动主收集器上创建以下文件将 HA 群集移入维护模式：
   在 Windows 上

   %NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance 或
   %TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance

   %NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM 或
   %TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM

在 Linux 上

/var/opt/OV/hacluster/<资源组>/maintenance

/var/opt/OV/hacluster/<资源组>/maint_NNM

2. 运行以下命令停止主动主收集器上的主收集器进程：
在 Windows 上

%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl --HA 或
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl --HA

%NnmInstallDir%\nonOV\traffic-master\bin\nmstrafficmasterstop.ovpl --HA 或
%TrafficInstallDir%\nonOV\traffic-master\bin\nmstrafficmasterstop.ovpl --HA

在 Linux 上

/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl --HA

/opt/OV/nonOV/traffic-master/bin/nmstrafficmasterstop.ovpl --HA

3. 如补丁程序文本中所述卸载主收集器补丁程序。

备注：不要取消主动主收集器上的 HA 配置。

4. 运行以下命令启动主动主收集器上的主收集器进程：
在 Windows 上

%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl --HA 或
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl --HA

%NnmInstallDir%\nonOV\traffic-master\bin\nmstrafficmasterstart.ovpl --HA 或
%TrafficInstallDir%\nonOV\traffic-master\bin\nmstrafficmasterstart.ovpl --HA

在 Linux 上

/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl --HA

/opt/OV/nonOV/traffic-master/bin/nmstrafficmasterstart.ovpl --HA

在 HA 环境中重新配置被动主收集器

1. 要在 HA 环境中重新配置被动主收集器，请执行以下步骤：
2. 在每个被动主收集器上，运行以下命令重新配置 HA。
在 Windows 上
   - NNMi 和主收集器在同一个群集中
   %NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM –addon TRAFFIC

     备注：当 NNMi 和主收集器处于同一群集中时，确保以下命令在列表中显示被动主收集器：

     %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS

   - 主收集器在独立 HA 群集中
   %TrafficInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl TRAFFIC

备注：当主收集器安装在独立 HA 群集中时，确保以下命令在列表中显示被动主收集器：

```
%TrafficInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl –group <资源组> -nodes
```

对于 Linux

- NNMi 和主收集器在同一个群集中
  `/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM –addon TRAFFIC`

  备注：当 NNMi 和主收集器处于同一群集中时，确保以下命令在列表中显示被动主收集器：

  ```
  /opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS
  ```

- 主收集器在独立 HA 群集中
  `/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl TRAFFIC`

  备注：当主收集器安装在独立 HA 群集中时，确保以下命令在列表中显示被动主收集器：

  ```
  /opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl –group <资源组> -nodes
  ```

3. 删除以下文件将被动主收集器移出维护模式：
   在 Windows 上

   `%NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance` 或
   `%TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance`

   `%NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM` 或
   `%TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM`

   在 Linux 上

   `/var/opt/OV/hacluster/<资源组>/maintenance`

   `/var/opt/OV/hacluster/<资源组>/maint_NNM`
4. 删除以下文件将主动主收集器移出维护模式：
   在 Windows 上

   `%NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance` 或
   `%TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maintenance`

   `%NnmDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM` 或
   `%TrafficDataDir%\nmsas\traffic-master\hacluster\<资源组>\maint_NNM`

   在 Linux 上

   `/var/opt/OV/hacluster/<资源组>/maintenance`

   `/var/opt/OV/hacluster/<资源组>/maint_NNM`

第 7 章: 在应用程序故障转移环境中部署 NNM iSPI Performance for Traffic

NNM iSPI Performance for Traffic 无法配置为支持应用程序故障转移。但是，它可以存在于在应用程序故障转移环境中安装 NNMi 的环境。在配置 NNMi 用于应用程序故障转移后，NNM iSPI Performance for Traffic 主收集器将尝试建立与主 NNMi 管理服务器的连接。当主收集器无法连接到主 NNMi 管理服务器时，它会尝试使用 `nnm.extended.properties` 文件中提供的凭据连接到辅助 NNMi 管理服务器。

支持以下部署配置：

- NNMi 安装在应用程序故障转移环境中，作为两个独立系统上的主实例和辅助实例。
- NNM iSPI Performance for Traffic 主收集器和叶收集器安装在独立的非并存系统上。
- 主和辅助 NNMi 管理服务器上都必须安装 NNMi Extension for iSPI Performance for Traffic。
- 在主和辅助 NNMi 管理服务器上都必须将主收集器配置为指向以下内容：
  - NNMi 实例(提供物理 FQDN)
  - 共享 HA 系统上的 NNM iSPI Performance for Metrics 数据文件文件夹的网络共享驱动器。

在应用程序故障转移中配置 NNM iSPI Performance for Traffic

可以在安装 NNM iSPI Performance for Traffic 前或安装 NNM iSPI Performance for Traffic 后，通过主收集器系统上提供的主和辅助 NNMi 管理服务器的详细信息，配置 NNMi 用于故障转移。

场景 1：在配置 NNMi 用于应用程序故障转移之后安装 NNM iSPI Performance for Traffic

如果在配置 NNMi 用于应用程序故障转移后安装 NNM iSPI Performance for Traffic，请执行以下步骤：

1. 在主和辅助 NNMi 管理服务器上安装 NNMi Extension for iSPI Performance for Traffic。
   要在辅助 NNMi 管理服务器上安装 NNMi Extension for iSPI Performance for Traffic，必须使用辅助 NNMi 管理服务器上提供的主收集器 FQDN。
2. 安装主收集器，然后提供主和辅助 NNMi 管理服务器的详细信息。

备注：如果要启用主收集器和 NNMi 管理服务器间的安全通信 (HTTPS)，请参阅启用安全性 (第 18 页)。

场景 2：在安装 NNMi 和 NNM iSPI Performance for Traffic 之后配置 NNMi 用于应用程序故障转移

如果先安装 NNM iSPI Performance for Traffic 再配置 NNMi 用于应用程序故障转移，请在配置 NNMi 用于应用程序故障转移后执行以下步骤：

1. 在辅助 NNMi 管理服务器上安装 NNMi Extension for iSPI Performance for Traffic。
   要在辅助 NNMi 管理服务器上安装 NNMi Extension for iSPI Performance for Traffic，必须使用辅

助 NNMi 管理服务器上提供的主收集器 FQDN。

2. 登录到主收集器系统。
3. 运行以下命令停止主收集器进程：
   在 Windows 上
   `%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl` 或
   `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`
   在 Linux 上
   `/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl`
4. 导航到以下目录：
   在 Windows 上
   `%NnmDataDir%\nmsas\traffic-master\conf`
   在 Linux 上
   `/var/opt/OV/nmsas/traffic-master/conf`
5. 使用文本编辑器打开 `nnm.extended.properties` 文件。
6. 将 `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.hostname` 属性设置为辅助 NNMi 管理服务器的 FQDN。
7. 修改以下属性：
   - 将 `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.port` 属性设置为主收集器的 HTTP 端口号。默认的 HTTP 端口号是 `12080`。
   - 将 `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.isSecure` 属性的值设置为 `com.hp.ov.nms.spi.traffic-master.spi.isSecure` 属性中设置的值。
   - 将 `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.present` 属性设置为 `true`。将此属性设置为 true 指示将 NNMi 管理服务器配置用于应用程序故障转移。
   - 将 `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.protocol` 属性的值设置为 `com.hp.ov.nms.spi.traffic-master.Nnm.protocol` 属性中设置的值。

     备注： 如果要启用主收集器和 NNMi 管理服务器间的安全通信 (HTTPS)，请参阅启用安全性 (第 18 页)。

   - 将 `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.username` 属性设置为 `com.hp.ov.nms.spi.traffic-master.Nnm.username` 属性中提供的 WS 客户端用户名。确保在辅助 NNMi 管理服务器上创建与在主 NNMi 管理服务器上创建的相同的用户(具有相同的用户名和密码)。
   - 将 `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.https.port` 属性设置为 `com.hp.ov.nms.spi.traffic-master.Nnm.https.port` 属性中设置的 NNMi 管理服务器的 HTTPS 端口号。默认的 HTTPS 端口号是 `443`。
   - 将 `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.perfspidatapath` 属性设置为辅助 NNMi 管理服务器上的共享文件夹的数据路径。
   - 将 `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.jndi.port` 属性设置为 `com.hp.ov.nms.spi.traffic-master.Nnm.jndi.port` 属性中设置的 NNMi 管理服务器的 JNDI 端口号。默认的 JNDI 端口号是 `1099`。
8. 保存并关闭该文件。

9. 运行以下命令将 com.hp.ov.nms.spi.traffic-master.Nnm.secondary.password 属性设置为 com.hp.ov.nms.spi.traffic-master.Nnm.password 属性中输入的加密密码：
   在 Windows 上
   %NnmInstallDir%\traffic-master\bin\encrypttrafficpassword.ovpl --nnmEncrypt=<辅助服务器上的 WS 用户密码字符串> --secondary 或 %TrafficInstallDir%\traffic-master\bin\encrypttrafficpassword.ovpl --nnmEncrypt=<辅助服务器上的 WS 用户密码字符串> --secondary
   在 Linux 上
   /opt/OV/traffic-master/bin/encrypttrafficpassword.ovpl --nnmEncrypt=<辅助服务器上的 WS 用户密码字符串> --secondary
10. 保存并关闭该文件。
11. 运行以下命令以启动主收集器进程：
    在 Windows 上
    %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl 或 %TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
    在 Linux 上
    /opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl
12. 导航到以下目录：
    在 Windows 上
    %NnmInstallDir%\traffic-master\server\conf\
    在 Linux 上
    /opt/OV/traffic-master/server/conf/
13. 用文本编辑器打开 login-config.xml 文件。
14. 搜索以下字符串：
    <application-policy name="nnm">
15. 在以下属性中修改 NNM 辅助管理服务器的主机名：
    login-module code="com.hp.ov.nms.as.server.security.NmsSPILoginModule" flag="sufficient"> <module-option name="nnmAuthUrl">http://<辅助 NNM 主机名>:<NNM 端口>/spilogin/auth</moduleoption><module-option name="password-stacking">useFirstPass</moduleoption></login-module>
16. 保存并关闭该文件。

第 8 章：调整NNM iSPI Performance for Traffic

HPE 建议在安装后，通过调整参数集对 NNM iSPI Performance for Traffic 进行配置以优化其在小型、中型和大型层环境中的性能。HPE 还建议为主收集器生成的流数据配置报告数据保留期限。

增强主收集器和叶收集器的性能

NNM iSPI Performance for Traffic 为您提供了一组参数，您可以通过配置它们以在大型环境中实现最佳 iSPI 性能。这些调整参数位于以下文件中：

- 在主收集器系统上
  在 Windows 上

  `%NnmDataDir%\nmsas\traffic-master\conf\%NnmDataDir%\shared\traffic-master\conf\nms-traffic-master.address.properties` 或 `%TrafficDataDir%\nmsas\traffic-master\conf\%TrafficDataDir%\shared\traffic-master\conf\nms-traffic-master.address.properties`

  在 Linux 上

  `/var/opt/OV/nmsas/traffic-master/conf//var/opt/OV/shared/traffic-master/conf/nms-traffic-master.address.properties`
- 在叶收集器系统上
  在 Windows 上

  `%NnmDataDir%\nmsas\traffic-leaf\conf\%NnmDataDir%\shared\traffic-leaf\conf\nms-traffic-leaf.address.properties` 或 `%TrafficDataDir%\nmsas\traffic-leaf\conf\%TrafficDataDir%\shared\traffic-leaf\conf\nms-traffic-leaf.address.properties`

  在 Linux 上

  `/var/opt/OV/nmsas/traffic-leaf/conf//var/opt/OV/shared/traffic-leaf/conf/nms-traffic-leaf.address.properties`

《NNMi Ultimate Support Matrix》定义了以下类型的环境：

- 入门
- 小
- 中
- 大

要在安装之后配置 NNM iSPI Performance for Traffic 的调整参数，请执行以下步骤：

备注：在安装之后，必须执行这些步骤。

1. 确定环境的类型 - 入门、小型、中型或大型(请参阅《NNM iSPI Performance for Traffic Support Matrix》)。要确定网络中流记录的速率，请运行 `nmstrafficflowanalysistool.ovpl` 命令。有关详细信息，请参阅此工具的参考页。
2. 记下《NNM iSPI Performance for Traffic Support Matrix》的 Table 4 中调整参数的建议值。
3. 在每个叶收集器系统上执行以下步骤：
   a. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到叶收集器系统。
   b. 使用文本编辑器打开 `nms-traffic-leaf.address.properties` 文件。

      备注： HPE 建议不要修改叶收集器系统上的 `nms-traffic-leaf.address.properties` 文件中的以下属性：

      - 收集器名称`.flowrecord.pool.size`
      - 收集器名称`.topn.flowrecord.pool.size`

      在此实例中，收集器名称是叶收集器实例的名称。在安装 NNM iSPI Performance for Traffic 9.20 Patch 1 以及叶收集器开始从其他路由器接收 IP 流数据后属性收集器名称`.flowrecord.pool.size`和收集器名称`.topn.flowrecord.pool.size`可能会增加。

   c. 将 `flowrecord.pool.size` 属性设置为《NNM iSPI Performance for Traffic Support Matrix》的 Table 4 中对应于您所用环境的流记录的建议值。HPE 建议仅将此属性设置为该建议值一次。

      备注：

      - 如果同一叶收集器系统上有多个叶收集器实例，则必须为各个叶收集器实例划分所需的池大小。然后可以在相应的 nms-traffic-leaf.address.properties 文件中为每个叶收集器实例设置 flowrecord.pool.size 和 topn.flowrecord.pool.size 属性。例如，如果叶收集器系统流记录所需的对象池大小为 100K，同时您有两个叶收集器实例，则必须将 flowrecord.pool.size 属性设置为 50K。
      - 增大流记录池大小需要额外内存。流记录池大小每增加 100K，就必须提供 200 MB 额外内存。例如，如果流记录池大小增加了 200K，则必须为叶收集器的 Xmx 值添加额外的 400 MB。有关如何更改 Xmx 值的信息，请参阅修改 JVM 参数 (第 49 页)。

   d. 将 `topn.flowrecord.pool.size` 属性设置为《NNM iSPI Performance for Traffic Support Matrix》的 Table 4 中对应于您所用环境的前 N 个流记录的建议值。HPE 建议仅将此属性设置为该建议值一次。

      备注： 增大前 N 名流记录池大小需要额外内存。前 N 名流记录池大小每增加 100K，就必须提供 200 MB 额外内存。例如，如果前 N 名流记录池大小增加了 500K，则必须为叶收集器的 Xmx 值添加额外的 1 GB。有关如何更改 Xmx 值的信息，请参阅修改 JVM 参数 (第 49 页)。

   e. 在大型层环境中，如果 NNM iSPI Performance for Traffic 监视 4000 个以上的接口至少需要 20 个阈值，则必须将 `thresold.objectpool.size` 属性至少设置为 `1000000` 个。
   f. 保存该文件。
   g. 通过运行以下命令，重新启动叶收集器：
      在 Windows 上

`%NnmInstallDir%\traffic-leaf\bin\%NnmInstallDir%\nonOV\traffic-leaf\bin\nmstrafficleafstart.ovpl` 或 `%TrafficInstallDir%\traffic-leaf\bin\%TrafficInstallDir%\nonOV\traffic-leaf\bin\nmstrafficleafstart.ovpl`

在 Linux 上

`/opt/OV/traffic-leaf/bin//opt/OV/nonOV/traffic-leaf/bin/nmstrafficleafstart.ovpl`

备注：在操作期间，NNM iSPI Performance for Traffic 会自动更新这些参数的值。每次自动更新调整参数时，NNM iSPI Performance for Traffic 都会在 NNMi 控制台的“流处理状态”视图中创建一个新条目。

4. 在主收集器系统上执行以下步骤：
   a. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到主收集器系统。
   b. 用文本编辑器打开 `nms-traffic-master.address.properties` 文件。
   c. 将 `nms.traffic-master.maxflowrecord.inqueue` 属性设置为《NNM iSPI Performance for Traffic Support Matrix》的 Table 4 中对应于您所用环境的主队列大小的建议值。
   d. 保存该文件。
   e. 通过运行以下命令，重新启动主收集器：
   在 Windows 上

   `%NnmInstallDir%\traffic-master\bin\%NnmInstallDir%\nonOV\traffic-master\bin\nmstrafficmasterstart.ovpl` 或 `%TrafficInstallDir%\traffic-master\bin\%TrafficInstallDir%\nonOV\traffic-master\bin\nmstrafficmasterstart.ovpl`

   在 Linux 上

   `/opt/OV/traffic-master/bin//opt/OV/nonOV/traffic-master/bin/nmstrafficmasterstart.ovpl`

其他调整参数

NNM iSPI Performance for Traffic 在没有足够可用磁盘空间或每种报告有大量要写入 NNMi 系统的待处理文件时，无法在 NNMi 系统上写入文件。

备注：NNM iSPI Performance for Traffic 将文件写入 NNMi 系统的 `%NnmDataDir%\shared\perfSpi\datafiles` 目录 (Windows) 或 `/var/opt/OV/shared/perfSpi/datafiles` 目录 (Linux)。

为了确保 NNM iSPI Performance for Traffic 将文件成功写入 NNMi 系统，NNM iSPI Performance for Traffic 将检测 NNMi 系统上可用的磁盘空间量，以及要写入 NNMi 系统的每种待处理文件数。将文件写入 NNMi 系统之前，NNM iSPI Performance for Traffic 将从主收集器配置读取这些值。默认情况下，主收集器将文件写入 NNMi 系统所需的 NNMi 系统最小磁盘空间量为 1 GB，将文件写入 NNMi 系统时可排队的每种待处理文件的最大数是 100 个。

要修改 NNM iSPI Performance for Traffic 中设置的默认值，请在主收集器系统上执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到主收集器系统。
2. 通过运行以下命令，停止主收集器：
   在 Windows 上

%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl 或
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl

在 Linux 上

/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl

3. 用文本编辑器打开 nms-traffic-master.address.properties 文件。
4. 根据您的需求设置以下属性：
   a. nnm.shared.drive.size：定义主收集器将文件写入 NNMi 系统所需的 NNMi 系统最小磁盘空间量。
   b. nps.max.pending.files：定义将文件写入 NNMi 系统时可排队的每种待处理文件的最大数。
5. 保存该文件。
6. 通过运行以下命令，启动主收集器：
   在 Windows 上

   %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl 或
   %TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl

   在 Linux 上

   /opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl

禁用对象池调整

NNM iSPI Performance for Traffic 根据您环境中设置的池大小值自动调整叶收集器的池大小。如果不想内存使用情况变化，可以禁用此功能。

要禁用叶收集器实例池大小的自动调整，请执行以下步骤：

1. 登录到叶收集器系统。
2. 通过运行以下命令，停止叶收集器进程：
   在 Windows 上

   %NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl 或
   %TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl

   在 Linux 上

   /opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl

3. 导航到以下目录：
   在 Windows 上

   %NnmDataDir%\nmsas\traffic-leaf\conf\nms-traffic-leaf.address.properties 或
   %TrafficDataDir%\nmsas\traffic-leaf\conf\nms-traffic-leaf.address.properties

   在 Linux 上

   /var/opt/OV/nmsas/traffic-leaf/conf/nms-traffic-leaf.address.properties

4. 使用文本编辑器打开 nms-traffic-leaf.address.properties 文件。
5. 添加以下属性：
   leaf.collector.object.pool.tuner.disable=true
   添加上述属性将禁用所有实例的池大小自动调整。
6. 保存并关闭该文件。
7. 通过运行以下命令，启动叶收集器进程：
   在 Windows 上

%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl 或
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl

在 Linux 上

/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl

修改 JVM 参数

可以通过修改主收集器和叶收集器的 JVM 参数更改初始 Java 堆大小 (-Xms) 和最大 Java 堆大小 (-Xmx)。

要更改主收集器的初始 Java 堆大小 (-Xms) 和最大 Java 堆大小 (-Xmx)，请执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到主收集器系统。
2. 通过运行以下命令，停止主收集器：
   在 Windows 上

   %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl 或
   %TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl

   在 Linux 上

   /opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl
3. 导航到以下目录：
   在 Windows 上

   %NnmDataDir%\nmsas\traffic-master\conf

   或

   %TrafficDataDir%\nmsas\traffic-master\conf

   在 Linux 上

   /var/opt/OV/nmsas/traffic-master/conf
4. 使用文本编辑器打开 nms-traffic-master.jvm.properties 文件。
5. 将 -Xms 属性设置为《NNMi Ultimate Support Matrix》的 Master Collector Size 表中对应于您所用环境的初始 Java 堆大小 (-Xms) 的建议值。默认情况下，初始 Java 堆大小设置为 128 MB。
6. 将 -Xmx 属性设置为《NNMi Ultimate Support Matrix》的 Master Collector Size 表中对应于您所用环境的初始 Java 堆大小 (-Xmx) 的建议值。默认情况下，最大 Java 堆大小设置为 4,096 MB。
7. 保存并关闭该文件。
8. 通过运行以下命令，启动主收集器：
   在 Windows 上

   %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl 或
   %TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl

   在 Linux 上

   /opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl

要更改叶收集器的初始 Java 堆大小 (-Xms) 和最大 Java 堆大小 (-Xmx)，请执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到叶收集器系统。
2. 通过运行以下命令，停止叶收集器：
   在 Windows 上

%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl 或
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl

在 Linux 上

/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl

3. 导航到以下目录：
在 Windows 上

%NnmDataDir%\nmsas\traffic-leaf\conf

或

%TrafficDataDir%\nmsas\traffic-leaf\conf

在 Linux 上

/var/opt/OV/nmsas/traffic-leaf/conf

4. 使用文本编辑器打开 nms-traffic-leaf.jvm.properties 文件。
5. 将 -Xms 属性设置为《NNMi Ultimate Support Matrix》的 Leaf Collector Size 表中对应于您所用环境的初始 Java 堆大小 (-Xms) 的建议值。默认情况下，初始 Java 堆大小设置为 128 MB。
6. 将 -Xmx 属性设置为《NNMi Ultimate Support Matrix》的 Leaf Collector Size 表中对应于您所用环境的最大 Java 堆大小 (-Xmx) 的建议值。默认情况下，最大 Java 堆大小设置为 4,096 MB。
7. 保存并关闭该文件。
8. 通过运行以下命令，启动叶收集器：
在 Windows 上

%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl 或
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl

在 Linux 上

/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl

调整保留期限

保留期限是指主收集器生成的详细数据和汇总数据存储在 NPS 系统上用于报告的时间。存储数据将占用 NPS 系统磁盘使用情况。在 NPS 系统上，数据库占用部分磁盘后，将无法减少数据库 (*.db) 文件，从而将该磁盘空间重用于操作系统。要减少磁盘的使用，可以修改 NPS 提供的 ExtensionPack 或 NNM iSPI Performance for Traffic 提供的单独 ExtensionPack 的保留期限。为 NNM iSPI Performance for Traffic 提供的 ExtensionPack 设置的保留期限值将覆盖为 NPS 提供的 ExtensionPack 设置的保留期限值。有关更改 NPS 保留期限的信息，请参阅《HPE Network Node Manager iSPI Performance for Metrics 安装指南》。

NNM iSPI Performance for Traffic 提供的每个 ExtensionPack 在安装时为详细数据和汇总数据定义了不同的保留期限。以下参数定义这些保留期限：

- PRSPI_DataRetention_Raw：详细数据存储的天数。NNM iSPI Performance for Traffic 的详细数据仅存储在原始表中。因此，要更改保留期限，必须修改 PRSPI_DataRetention_Raw 参数。下表列出的是 NNM iSPI Performance for Traffic ExtensionPack 提供的默认保留期限：

保留期限默认值

ExtensionPack	默认值
Interface_Traffic	3
Interface_Traffic_1_minute	30
Interface_Traffic _Aggregated	400

备注：默认禁用 1 分钟接口流量报告。有关如何启用这些报告的信息，请参阅《HP Network Node Manager iSPI Performance for Traffic Software 联机帮助》中的"配置主收集器"部分。

- PRSPI_DataRetention_Hour：每小时汇总的数据存储的天数。

  备注：NNM iSPI Performance for Traffic 不在摘要表中存储数据。修改此参数不会更改保留期限。

- PRSPI_DataRetention_Day：每天汇总的数据存储的天数。

  备注：NNM iSPI Performance for Traffic 不在摘要表中存储数据。修改此参数不会更改保留期限。

- PRSPI_SUMMARY_Policy：ExtensionPack 的汇总策略。HPE 建议不要为 NNM iSPI Performance for Traffic 的任何 ExtensionPack 设置此参数。

要更改某个 ExtensionPack 的默认保留期限，请执行以下步骤：

1. 登录到 NPS 系统。
2. 停止 ETL 进程。
3. 用文本编辑器打开 customConfig.cfg 文件：
   在 Windows 上

   <NPS 数据目录>\NNMPerformanceSPI\rconfig\<ExtensionPack 名称>\customConfig.cfg

   在此实例中，<NPS 数据目录> 是安装 NPS 后存储 NPS 配置和数据文件的目录。

   在 Linux 上

   /var/opt/OV/NNMPerformanceSPI/rconfig/<ExtensionPack 名称>/customConfig.cfg
4. 将 customConfig.cfg 文件的内容传输到新的 userConfig.cfg 文件，然后在同一位置保存新文件。
5. 在新的 userConfig.cfg 文件中，设置参数 PRSPI_DataRetention_Raw 修改详细数据存储的天数。

   备注：修改保留期限可能对磁盘使用情况产生重大影响。

6. 保存并关闭 customConfig.cfg 文件。
7. 重新启动 ETL 进程。

增强 NPS 性能

NPS 处理 NNM iSPI Performance for Traffic 文件速度慢会导致写入 NNMi 系统的每种报告的待处理文件数增加。可以通过调整 ETL 增强 NPS 系统的性能。有关详细信息，请参阅调整 NPS 的 ETL (第 52 页)。

还可以通过调整硬件增强 NPS 的性能。当需要处理大量数据才能减少磁盘延迟和 I/O 等待时间以便优化记录处理和报告时，请优化磁盘和文件系统。有关详细信息，请参阅磁盘使用情况建议 (第 53 页)。

调整 NPS 的 ETL

要调整 NPS 的 ETL，请执行以下步骤：

1. 登录到 NPS 系统。
2. 停止 ETL 进程。
3. 用文本编辑器打开 customConfig.cfg 文件：
   在 Windows 上

   <NPS 数据目录>\NNMPerformanceSPI\rconfig\<ExtensionPack 名称>\customConfig.cfg

   在此实例中，<NPS 数据目录> 是安装 NPS 后存储 NPS 配置和数据文件的目录。

   在 Linux 上

   /var/opt/OV/NNMPerformanceSPI/rconfig/<ExtensionPack 名称>/customConfig.cfg
4. 在同一位置创建新的 userConfig.cfg 文件，然后将 customConfig.cfg 文件的内容传输到新的 userConfig.cfg 文件。
5. 在新的 userConfig.cfg 文件中，通过为每个 ExtensionPack 设置以下参数调整 NPS 的 ETL：

   备注：将 NPS 的 ETL 进程的调整参数增大为下表中列出的值会明显提高 CPU 的利用率。在增大这些参数之前，请确保有足够可用的 CPU 带宽。

   在此实例中，<NPS 数据目录> 是安装 NPS 后存储 NPS 配置和数据文件的目录。

   NPS 的 ETL 进程的子进程数，NPS 的 ETL 进程适用于基于不同 ExtensionPack 的中型和大型流量数据层 (ETL_MaxChildProcs)：

近似被管环境层	Interface_Traffic	Interface_Traffic_1_Minute	Interface_Traffic_Aggregated
中	5	10	10
大	10	50	20

   NPS 的 ETL 进程的每个子进程最大记录数，NPS 的 ETL 进程适用于基于不同 ExtensionPack 的中型和大型流量数据层 (ETL_MaxRecordsPerChild)：

近似被管环境层	Interface_Traffic	Interface_Traffic_1_ Minute	Interface_Traffic_ Aggregated
中	100k	100k	100k
大	100k	200k	200k

NPS 的 ETL 进程的每批次文件数，NPS 的 ETL 进程适用于基于不同 ExtensionPack 的中型和大型流量数据层 (ETL_MaxMetricsFilesPerBatch)：

近似被管环境层	Interface_Traffic	Interface_Traffic_1_ Minute	Interface_Traffic_ Aggregated
中	20	25	20
大	30	50	30

6. 保存并关闭 userConfig.cfg 文件。
7. 重新启动 ETL 进程。

磁盘使用情况建议

要减少磁盘延迟和 I/O 等待时间，请遵循以下建议：

- 在 SAN 的不同磁盘上创建存储位置 /var/opt/OV、IQ_SYSTEM_TEMP 和 USER_MAIN。运行以下命令设置这些存储位置的位置和大小：
  对于 Windows

  <NPS 安装目录>\NNMPerformanceSPI\bin\dbsize.ovpl

  对于 Linux

  /opt/OV/NNMPerformanceSPI/bin/dbsize.ovpl
- 将 IQ_SYSTEM_TEMP 设置为最小值 100 GB。
- 将磁盘缓存率设置为 50/50 读/写
- 存储位置使用原始磁盘

有关详细信息，请联系存储区域网络管理员。

第 9 章: 维护报告

使用 NNM iSPI Performance for Traffic，您可以查看可深入了解网络流量的报告，并通过分析流量流监视网络性能。默认情况下，所有的报告都不可用，因为启用任何报告都会增大 NNM iSPI Performance for Traffic 和 NPS 上的负载。此部分描述如何基于您的需求启用或禁用这些报告以增强 NNM iSPI Performance for Traffic 的性能。

启用流量报告上的子网详细信息

使用 NNM iSPI Performance for Traffic，您可以查看流量报告中的源子网地址和目标子网地址。但是，默认情况下这些子网详细信息在流量报告中不显示。必须执行其他配置步骤才能在 NNM iSPI Performance for Traffic 报告中查看子网详细信息。启用子网详细信息可能会增大 NNM iSPI Performance for Traffic 和 NPS 的负载。因此，您可能需要其他系统资源，如 CPU、内存和磁盘空间。

在以下报告中，子网详细信息位于**分组依据**列表中的"报告选项"中。

- 接口流量报告：最大变化、前 N 名、前 N 名图表和前 N 名表
- 聚合接口流量和 1 分钟接口流量报告：前 N 名分析、前 N 名图表分析和前 N 名表分析的排名靠前的接口报告

备注：默认禁用 1 分钟接口流量报告。有关如何启用这些报告的信息，请参阅《HP Network Node Manager iSPI Performance for Traffic Software 联机帮助》中的"配置主收集器"部分。

禁用子网详细信息后，"源子网地址"和"目标子网地址"选项将位于**分组依据**列表中。但是，子网地址在报告中将显示为 `0.0.0.0/0`。

要查看流量报告中的子网详细信息，请在叶收集器系统上执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到叶收集器系统。
2. 使用文本编辑器打开 `nms-traffic-leaf.address.properties` 文件。
3. 添加 `enable.subnet.report` 属性，并将其设置为 `true`。
4. 保存并关闭该文件。
5. 通过运行以下命令，启动叶收集器：
   在 Windows 上

   `%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl` 或
   `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl`

   在 Linux 上

   `/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl`

为排名靠前的目标端口的报告启用数据采集

默认禁用以下报告的数据采集：

- 聚合接口流量 - 目标端口的排名靠前的源
- 聚合接口流量 - 目标端口的排名靠前的目标
- 聚合接口流量 - 目标端口的排名靠前的会话
- 1 分钟接口流量 - 目标端口的排名靠前的源
- 1 分钟接口流量 - 目标端口的排名靠前的目标
- 1 分钟接口流量 - 目标端口的排名靠前的会话

备注：启用这些报告可能会增大 NNM iSPI Performance for Traffic 和 NPS 上的负载。因此，您可能需要其他系统资源，如 CPU、内存和磁盘空间。

备注：默认禁用 1 分钟接口流量报告。有关如何启用这些报告的信息，请参阅《HP Network Node Manager iSPI Performance for Traffic Software Software 联机帮助》中的“配置主收集器”部分。

要启用排名靠前的目标端口报告的数据采集，请执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到叶收集器系统。
2. 通过运行以下命令，停止叶收集器：
   在 Windows 上

   `%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl` 或
   `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl`

   在 Linux 上

   `/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl`
3. 导航到以下目录：
   在 Windows 上

   `%TrafficDataDir%\nmsas\traffic-leaf\conf`

   或

   `%NNMDataDir%\nmsas\traffic-leaf\conf`

   在 Linux 上

   `/var/opt/OV/nmsas/traffic-leaf/conf`
4. 使用文本编辑器打开 `nms-traffic-leaf.address.properties` 文件。
5. 添加以下行：
   `topn.subtypes.dstport=true`

   添加此行后，将启用 `Top Conversations for Destination Port` 报告的数据采集。
6. 添加以下行：
   `enable.srcordst.dstport=true`

添加此行后，将启用 Top Sources for Destination Port 和 Top Destinations for Destination Port 报告的数据采集。

7. 保存并关闭 nms-traffic-leaf.address.properties 文件。
8. 通过运行以下命令，启动叶收集器：

   在 Windows 上

   %NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl 或 %TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl

   在 Linux 上

   /opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl

要禁用排名靠前的目标端口报告的数据采集，请执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到叶收集器系统。
2. 通过运行以下命令，停止叶收集器：
   在 Windows 上

   %NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl 或 %TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl

   在 Linux 上

   /opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
3. 导航到以下目录：
   在 Windows 上

   %TrafficDataDir%\nmsas\traffic-leaf\conf

   或

   %NNMDataDir%\nmsas\traffic-leaf\conf

   在 Linux 上

   /var/opt/OV/nmsas/traffic-leaf/conf
4. 使用文本编辑器打开 nms-traffic-leaf.address.properties 文件。
5. 执行以下某项操作：
   - 删除以下代码行：
     topn.subtypes.dstport=true
   - 将 topn.subtypes.dstport 属性设置为 false。
6. 保存并关闭 nms-traffic-leaf.address.properties 文件。
7. 通过运行以下命令，启动叶收集器：
   在 Windows 上

   %NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl 或 %TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl

   在 Linux 上

   /opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl

禁用接口流量报告的数据生成

在大型环境中配置 NNM iSPI Performance for Traffic 时，必须禁用接口流量报告的数据生成以便实现最佳性能。

要禁用接口流量报告的数据生成，请执行以下步骤：

1. 登录到 NNM iSPI Performance for Traffic 配置表单。
2. 单击主收集器。将打开主收集器详细信息页面。
3. 找到 Interface Traffic Data Flush 参数并单击 

编辑。
4. 将接口流量数据清除参数的值字段设置为禁用清除。
5. 单击 

保存。
6. 通过运行以下命令，启动叶收集器：
   在 Windows 上

   %NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl 或
   %TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl

   在 Linux 上

   /opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
7. 通过运行以下命令，启动主收集器：
   在 Windows 上

   %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl 或
   %TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl

   在 Linux 上

   /opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl

第 10 章：维护 NNM iSPI Performance for Traffic

使用 NNM iSPI Performance for Traffic，您可以备份和恢复主收集器和叶收集器上的配置文件和嵌入式数据库。本章介绍了 NNM iSPI Performance for Traffic 提供的用于备份和恢复主收集器和叶收集器的数据库和配置文件的脚本。

本章还描述了更改 NNMi 管理服务器、主收集器、叶收集器或 NPS 的主机名后需要执行的更改。

升级收集器系统的操作系统

执行叶收集器和主收集器系统的就地操作系统升级之前，请停止收集器进程。

在主收集器系统上：

1. 以根用户或管理员身份登录。
2. 运行以下命令停止收集器：

   在 Windows 上

   `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`

   在 Linux 上

   `/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl`

在叶收集器系统上：

1. 以根用户或管理员身份登录。
2. 运行以下命令停止收集器：

   在 Windows 上

   `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl`

   在 Linux 上

   `/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl`

操作系统升级完成之后，运行以下命令启动收集器：

- 要启动主收集器，请执行以下操作：

  在 Windows 上

  `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`

  在 Linux 上

  `/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl`
- 要启动叶收集器，请执行以下操作：

  在 Windows 上

  `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl`

在 Linux 上

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

更改主机名

可以更改 NNMi 管理服务器、主收集器、叶收集器和 NPS 的主机名。每次更改其中一个服务器的主机名时，相关服务器必须进行相应更改。例如，如果更改了 NNMi 管理服务器的主机名，则必须将主收集器和 NPS 更新为该新主机名。以下部分描述更改其中一个主机名时需要进行的更改。

更改 NNMi 主机名

如果更改 NNMi 主机名，则必须更新以下 NNM iSPI Performance for Traffic 组件：

- NNMi Extension for iSPI Performance for Traffic
- 主收集器
- 叶收集器

在 NNMi Extension for iSPI Performance for Traffic 系统上，执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到 NNMi 管理服务器。
2. 运行以下命令：
   在 Windows 上
   `%NnmInstallDir%\bin\nnmsetofficialfqdn.ovpl`
   在 Linux 上
   `/opt/OV/bin/nnmsetofficialfqdn.ovpl`

在 主收集器 系统上，执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到主收集器系统。
2. 导航到以下目录：
   在 Windows 上
   `%NnmDataDir%\nmsas\traffic-master\conf` 或 `%TrafficDataDir%\nmsas\traffic-master\conf`
   在 Linux 上
   `/var/opt/OV/nmsas/traffic-master/conf`
3. 用文本编辑器打开 `nms-traffic-master.address.properties` 文件。
4. 将 `jboss.nnm.host` 属性的值修改为 NNMi 管理服务器的主机名。
5. 保存并关闭该文件。
6. 用文本编辑器打开 `nnm.extended.properties` 文件。
7. 将 `com.hp.ov.nms.spi.traffic-master.nnm.hostname` 属性的值修改为 NNMi 管理服务器的主机名。

   备注： 如果 NNMi 管理服务器已配置应用程序故障转移，则将 `com.hp.ov.nms.spi.traffic-master.nnm.secondary.hostname` 属性的值修改为 NNMi 管理服务器的主机名并重新启动主收集器。

8. 保存并关闭该文件。

9. 导航到以下目录：
   在 Windows 上
   %NnmInstallDir%\traffic-master\server\conf\ 或 %TrafficDataDir%\traffic-master\server\conf\
   在 Linux 上
   /opt/OV/traffic-master/server/conf/
10. 用文本编辑器打开 login-config.xml 文件。
11. 搜索以下字符串：
    <application-policy name="nnm">
12. 在以下属性中修改 NNMi 管理服务器的主机名：
    - <login-module code="com.hp.ov.nms.as.server.security.NmsSPILoginModule" flag="sufficient"> <module-option name="nnmAuthUrl">http://<NNM 主机名>:<NNM 端口>/spilogin/auth</module-option><module-option name="password-stacking">useFirstPass</module-option> </login-module>

    - <login-module code="com.hp.ov.nms.as.server.security.NmsSPILoginModule" flag="sufficient"><module-option name="nnmAuthUrl">https://<NNM 安全主机名>:<NNM 安全端口>/spilogin/auth</module-option><module-option name="password-stacking">useFirstPass</module-option></login-module>

13. 保存并关闭该文件。
14. 如果主收集器与 NNMi 未安装在同一个系统中，则将以下目录内容移到其他目录路径中：
    在 Windows 上
    %NnmDataDir%\shared\nnm\certificates
    在 Linux 上
    /var/opt/OV/shared/nnm/certificates
15. 如果主收集器与 NNMi 未安装在同一个系统中，则使用以下命令再次生成新证书：
    在 Windows 上
    a. “%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool" -genkey -alias <主收集器 FQDN>.selfsigned -keyalg rsa -sigalg SHA1withRSA -keysize 2048 -dname cn=<主收集器 FQDN> -keypass nnmkeypass -validity 36500 -keystore “%TrafficDataDir%\shared\nnm\certificates\nnm.keystore" -storepass nnmkeypass
    b. “%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool" -export -file “%TrafficDataDir%\shared\nnm\certificates\nnm.cert" -keystore “%TrafficDataDir%\shared\nnm\certificates\nnm.keystore" -alias <主收集器 FQDN>.selfsigned -storepass nnmkeypass
    c. “%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool" -importcert -file “%TrafficDataDir%\shared\nnm\certificates\nnm.cert" -keystore “%TrafficDataDir%\shared\nnm\certificates\nnm.truststore" -storepass ovpass -noprompt

    备注：如果主收集器已配置安全通信，则必须再次将证书从 NNMi 管理服务器添加到 nnm.truststore。有关详细信息，请参阅启用 NNMi 和 NNM iSPI Performance for Traffic 间的安全通信 (第 18 页)。

    在 Linux 上
    a. “/opt/OV/nonOV/jdk/nnm/bin/keytool" -genkey -alias <主收集器 FQDN>.selfsigned -keyalg rsa -sigalg SHA1withRSA -keysize 2048 -dname cn=<主收集器 FQDN> -keypass

```
nnmkeypass -validity 36500 -keystore
“/var/opt/OV/shared/nnm/certificates/nnm.keystore" -storepass nnmkeypass
```

b.
```
“/opt/OV/nonOV/jdk/nnm/bin/keytool" -export -file
“/var/opt/OV/shared/nnm/certificates/nnm.cert" -keystore
“/var/opt/OV/shared/nnm/certificates/nnm.keystore" -alias <主收集器
FQDN>.selfsigned -storepass nnmkeypass
```

c.
```
“/opt/OV/nonOV/jdk/nnm/bin/keytool" -importcert -file
“/var/opt/OV/shared/nnm/certificates/nnm.cert" -keystore
“/var/opt/OV/shared/nnm/certificates/nnm.truststore" -storepass ovpass -noprompt
```

备注：如果主收集器已配置安全通信，则必须再次将证书从 NNMi 管理服务器添加到 `nnm.truststore`。有关详细信息，请参阅启用 NNMi 和 NNM iSPI Performance for Traffic 间的安全通信 (第 18 页)。

16. 重新启动主收集器系统。

在 NNMi 管理服务器上安装的叶收集器系统中，执行以下步骤：

备注：当 NNMi 管理服务器上未安装叶收集器时，无需对叶收集器系统进行更改。

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到叶收集器系统。
2. 导航到以下目录：
   在 Windows 上
   `%NnmDataDir%\nmsas\traffic-leaf\conf`
   在 Linux 上
   `/var/opt/OV/nmsas/traffic-leaf/conf`
3. 使用文本编辑器打开 `nms-traffic-leaf.address.properties` 文件。
4. 将 `leaf.host` 属性的值修改为 NNMi 管理服务器的主机名。
5. 保存并关闭该文件。
6. 导航到以下文件：
   在 Windows 上
   `%NnmDataDir%\nmsas\traffic-leaf\` 或 `%TrafficInstallDir%\nmsas\traffic-leaf\`
   在 Linux 上
   `/var/opt/OV/nmsas/traffic-leaf`
7. 打开 `server.properties` 文件。
8. 将 `java.rmi.server.hostname` 属性的值修改为 NNMi 管理服务器的主机名。
9. 保存并关闭该文件。
10. 重新启动叶收集器系统。

更改主收集器主机名

如果更改主收集器主机名，则必须更新以下 NNM iSPI Performance for Traffic 组件：

- NNMi Extension for iSPI Performance for Traffic
- 主收集器

在 NNMi Extension for iSPI Performance for Traffic 系统上，执行以下步骤：

1. 登录 NNMi 管理服务器。
2. 导航到以下目录：
   在 Windows 上
   %NnmInstallDir%\support
   在 Linux 上
   /opt/OV/support
3. 运行以下命令：
   a. nnmtwiddle.ovpl -host <NNM 主机名> -port 80 -u system -p <密码> invoke com.hp.ov.nms.topo:service=NetworkApplication removeApplication traffic
   b. nnmtwiddle.ovpl -host <NNM 主机名> -port 80 -u system -p <NNMi 系统用户密码> invoke com.hp.ov.nms.topo:service=NetworkApplication setApplicationService traffic <新的主收集器主机名> http 12080
   c. nnmtwiddle.ovpl -u system -p <NNM 系统密码> invoke com.hp.ov.nms.topo:service=NetworkApplication printConfiguration
4. 重新启动 NNMi 管理服务器。

在 主收集器 系统上，执行以下步骤：

1. 登录到主收集器系统。
2. 导航到以下目录：
   在 Windows 上
   %NnmDataDir%\nmsas\traffic-master 或 %TrafficDataDir%\nmsas\traffic-master
   在 Linux 上
   /var/opt/OV/nmsas/traffic-master
3. 用文本编辑器打开 server.properties 文件。
4. 将 java.rmi.server.hostname 属性的值修改为主收集器的主机名。
5. 保存并关闭该文件。
6. 导航到以下目录：
   在 Windows 上
   %trafficinstalldir%\traffic-master\server 或 %nnminstalldir%\traffic-master\server
   在 Linux 上
   /opt/OV/traffic-master\server
7. 用文本编辑器打开 server.properties 文件。
8. 将 java.rmi.server.hostname 属性的值修改为主收集器的主机名。
9. 保存并关闭该文件。
10. 导航到以下目录：
    在 Windows 上
    %NnmDataDir%\nmsas\traffic-master\conf 或 %TrafficDataDir%\nmsas\traffic-master\conf
    在 Linux 上
    /var/opt/OV/nmsas/traffic-master/conf
11. 用文本编辑器打开 nnm.extended.properties 文件。
12. 将 com.hp.ov.nms.spi.traffic-master.spi.hostname 属性的值修改为主收集器的主机名。
13. 保存并关闭该文件。
14. 如果主收集器与 NNMi 未安装在同一个系统中，则将 <NNM 数据目录>\shared\nnm\certificates 的内容移到其他目录路径。

15. 如果主收集器与 NNMi 未安装在同一个系统中，则使用以下命令再次生成新证书：
在 Windows 上
    a. “%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool" -genkey -alias <主收集器 FQDN>.selfsigned -keyalg rsa -sigalg SHA1withRSA -keysize 2048 -dname cn=<主收集器 FQDN> -keypass nnmkeypass -validity 36500 -keystore “%TrafficDataDir%\shared\nnm\certificates\nnm.keystore" -storepass nnmkeypass
    b. “%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool" -export -file “%TrafficDataDir%\shared\nnm\certificates\nnm.cert" -keystore “%TrafficDataDir%\shared\nnm\certificates\nnm.keystore" -alias <主收集器 FQDN>.selfsigned -storepass nnmkeypass
    c. “%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool" -importcert -file “%TrafficDataDir%\shared\nnm\certificates\nnm.cert" -keystore “%TrafficDataDir%\shared\nnm\certificates\nnm.truststore" -storepass ovpass -noprompt

    备注：如果已启用主收集器和 NNMi 管理服务器间的安全通信 (HTTPS)，请参阅启用 NNMi 和 NNM iSPI Performance for Traffic 间的安全通信 (第 18 页)。

    在 Linux 上
    a. “/opt/OV/nonOV/jdk/nnm/bin/keytool" -genkey -alias <主收集器 FQDN>.selfsigned -keyalg rsa -sigalg SHA1withRSA -keysize 2048 -dname cn=<主收集器 FQDN> -keypass nnmkeypass -validity 36500 -keystore “/var/opt/OV/shared/nnm/certificates/nnm.keystore" -storepass nnmkeypass
    b. “/opt/OV/nonOV/jdk/nnm/bin/keytool" -export -file “/var/opt/OV/shared/nnm/certificates/nnm.cert" -keystore “/var/opt/OV/shared/nnm/certificates/nnm.keystore" -alias <主收集器 FQDN>.selfsigned -storepass nnmkeypass
    c. “/opt/OV/nonOV/jdk/nnm/bin/keytool" -importcert -file “/var/opt/OV/shared/nnm/certificates/nnm.cert" -keystore “/var/opt/OV/shared/nnm/certificates/nnm.truststore" -storepass ovpass -noprompt

    备注：如果已启用主收集器和 NNMi 管理服务器间的安全通信 (HTTPS)，请参阅启用 NNMi 和 NNM iSPI Performance for Traffic 间的安全通信 (第 18 页)。

16. 重新启动主收集器。

更改叶收集器主机名

如果更改叶收集器主机名，请在叶收集器系统上执行以下步骤：

1. 登录到叶收集器系统。
2. 导航到以下目录：
在 Windows 上
%NnmDataDir%\nmsas\traffic-leaf\conf 或 %TrafficDataDir%\nmsas\traffic-leaf\conf
在 Linux 上
/var/opt/OV/nmsas/traffic-leaf/conf
3. 使用文本编辑器打开 nms-traffic-leaf.address.properties 文件。
4. 将 leaf.host 属性的值修改为叶收集器的主机名。

5. 保存并关闭该文件。
6. 导航到以下目录：
   在 Windows 上
   %NnmInstallDir%\nmsas\traffic-leaf\conf 或 %TrafficInstallDir%\nmsas\traffic-leaf\conf
   在 Linux 上
   /opt/OV/traffic-leaf\conf
7. 使用文本编辑器打开 nms-traffic-leaf.address.properties 文件。
8. 将 leaf.host 属性的值修改为叶收集器的主机名。
9. 保存并关闭该文件。
10. 导航到以下目录：
    在 Windows 上
    %NnmDataDir%\nmsas\traffic-leaf 或 %TrafficDataDir%\nmsas\traffic-leaf
    在 Linux 上
    /var/opt/OV/nmsas/traffic-leaf
11. 用文本编辑器打开 server.properties 文件。
12. 将 java.rmi.server.hostname 属性的值修改为 NNMi 管理服务器的主机名。
13. 保存并关闭该文件。
14. 如果叶收集器已配置为与主收集器安全通信，则将以下目录内容移到其他目录路径中：
    在 Windows 上
    %NnmDataDir%\shared\nnm\certificates
    在 Linux 上
    /var/opt/OVshared/nnm/certificates
15. 如果叶收集器已配置为与主收集器安全通信，则使用以下命令再次生成新证书：
    在 Windows 上
    a. “%NnmInstallDir%>\nonOV\jdk\nnm\bin\keytool" -genkey -alias <叶收集器 FQDN>.selfsigned -keyalg rsa -sigalg SHA1withRSA -keysize 2048 -dname cn=<叶收集器 FQDN> -keypass nnmkeypass -validity 36500 -keystore “%NnmDataDir%\shared\nnm\certificates\nnm.keystore" -storepass nnmkeypass
    b. “%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool" -export -file “%NnmDataDir%\shared\nnm\certificates\nnm.cert" -keystore “%NnmDataDir%\shared\nnm\certificates\nnm.keystore" -alias <叶收集器 FQDN>.selfsigned -storepass nnmkeypass
    c. “%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool" -importcert -file “%NnmDataDir%\shared\nnm\certificates\nnm.cert" -keystore “%NnmDataDir%\shared\nnm\certificates\nnm.truststore" -storepass ovpass -noprompt

       备注：如果叶收集器已配置安全通信，则必须再次将证书从叶收集器导入到 nnm.truststore。有关详细信息，请参阅启用主收集器和叶收集器间的安全通信 (第 23 页)。

    在 Linux 上
    a. “/opt/OV/nonOV/jdk/nnm/bin/keytool" -genkey -alias <叶收集器 FQDN>.selfsigned -keyalg rsa -sigalg SHA1withRSA -keysize 2048 -dname cn=<叶收集器 FQDN> -keypass nnmkeypass -validity 36500 -keystore “/var/opt/OV/shared/nnm/certificates/nnm.keystore" -storepass nnmkeypass

b. “/opt/OV/nonOV/jdk/nnm/bin/keytool" -export -file “/var/opt/OV/shared/nnm/certificates/nnm.cert" -keystore “/var/opt/OV/shared/nnm/certificates/nnm.keystore" -alias <叶收集器 FQDN>.selfsigned -storepass nnmkeypass

c. “/opt/OV/nonOV/jdk/nnm/bin/keytool" -importcert -file “/var/opt/OV/shared/nnm/certificates/nnm.cert" -keystore “/var/opt/OV/shared/nnm/certificates/nnm.truststore" -storepass ovpass -noprompt

备注：如果叶收集器已配置安全通信，则必须再次将证书从叶收集器导入到 nnm.truststore。有关详细信息，请参阅启用主收集器和叶收集器间的安全通信 (第 23 页)。

16. 重新启动叶收集器系统。
17. 以管理员特权登录到 NNMi 控制台。
18. 转到**配置**工作区。
19. 双击 **NNM iSPI Performance for Traffic 配置**。此时会打开 NNM iSPI Performance for Traffic 表单。
20. 使用主收集器安装过程中创建的系统用户帐户登录到 NNM iSPI Performance for Traffic 表单。
21. 删除叶收集器实例和叶收集器系统。有关详细信息，请参阅《HP Network Node Manager iSPI Performance for Traffic Software 联机帮助》中的“配置叶收集器实例”和“配置叶收集器系统”部分。
22. 添加叶收集器实例和叶收集器系统。有关详细信息，请参阅《HP Network Node Manager iSPI Performance for Traffic Software 联机帮助》中的“配置叶收集器实例”和“配置叶收集器系统”部分。

更改 NPS 主机名

如果更改 NPS 主机名，则必须更新：

- NNMi 管理服务器
- 主收集器

有关 NPS 系统上所需的更改，请参阅《NNM iSPI Performance for Metrics 部署参考》中的“维护 NPS”部分。

在 NNMi 管理服务器上，执行以下步骤：

1. 登录 NNMi 管理服务器。
2. 导航到以下目录：
   在 Windows 上
   %NnmInstallDir%\bin
   在 Linux 上
   /opt/OV/bin
3. 在命令提示符处，运行 nnmenableperfspi.ovpl -disable 命令。
4. 出现提示时，运行 nnmenableperfspi.ovpl 命令并提供主机名。
5. 在网络上对具有 Web 服务器客户端角色的用户再次共享 %NnmDataDir%\shared\perfSpi\datafiles 目录。确保该用户拥有此目录的读取/写入访问权

限。有关详细信息，请参阅《HP Network Node Manager iSPI Performance for Traffic Software 交互安装指南》的“安装主收集器”部分中的“预安装任务”。

在主收集器系统上，执行以下步骤：

1. 登录到主收集器系统。
2. 导航到以下目录：
   在 Windows 上
   `%NnmDataDir%\nmsas\traffic-master\conf` 或 `%TrafficDataDir%\nmsas\traffic-master\conf`
   在 Linux 上
   `/var/opt/OV/nmsas/traffic-master/conf`
3. 用文本编辑器打开 `nps.extended.properties`。
4. 修改以下属性的值：
   `com.hp.ov.nms.spi.traffic-master.nps.hostname`
5. 保存并关闭该文件。

备份和恢复命令

NNM iSPI Performance for Traffic 提供了以下脚本用于备份和恢复数据库和配置文件：

- `nmstrafficmasterbackup.ovpl`：创建所有主收集器数据库和配置文件的完整备份。
- `nmstrafficmasterresetdb.ovpl`：删除现有主收集器数据库并重新创建主收集器数据库和表。
- `nmstrafficmasterrestore.ovpl`：恢复使用 `nmstrafficmasterbackup.ovpl` 脚本创建的备份。
- `nmstrafficleafbackup.ovpl`：创建所有叶收集器数据库和配置文件的完整备份。
- `nmstrafficleafresetdb.ovpl`：删除现有叶收集器数据库并重新创建叶收集器数据库和表。
- `nmstrafficleafrestore.ovpl`：恢复使用 `nmstrafficleafbackup.ovpl` 脚本创建的备份。

有关详细信息，请参阅相应的参考页。

备注：使用 NNM iSPI Performance for Traffic 提供的脚本，您可以在 NNMi 和主收集器或叶收集器未安装在同一个系统中时备份和恢复文件。要在 NNMi 和主收集器或叶收集器安装在同一个系统中时备份和恢复文件，请参阅《HPE Network Node Manager i Software 部署参考》指南。

备份主收集器

要备份主收集器，请执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到主收集器系统。
2. 通过运行以下命令，停止主收集器：
   在 Windows 上
   `%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl` 或
   `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`
   在 Linux 上
   `/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl`

3. 运行以下命令启动主收集器数据库和配置文件的备份：
   `nmstrafficmasterbackup.ovpl -target <目标存档文件的完整路径> -scope [all|db]`
   在此实例中，<目标存档文件的完整路径>是用于存储备份文件的目录。
   选项 `all` 可以备份数据库和配置文件。
   选项 db 仅可备份数据库。
   备份脚本可创建备份数据的 tar 文件。
4. 通过运行以下命令，启动主收集器：
   在 Windows 上
   `%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl` 或
   `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl`
   在 Linux 上
   `/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl`

重置主收集器数据库

要重置主收集器数据库，请执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到主收集器系统。
2. 通过运行以下命令，停止主收集器：
   在 Windows 上
   `%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl` 或
   `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`
   在 Linux 上
   `/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl`
3. 运行以下命令重置主收集器数据库：
   `nmstrafficmasterresetdb.ovpl -start`
4. 通过运行以下命令，启动主收集器：
   在 Windows 上
   `%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl` 或
   `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl`
   在 Linux 上
   `/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl`

恢复主收集器

备注： 恢复主收集器数据库之前，必须先重置主收集器数据库，如重置主收集器数据库 (第 67 页)中所述。

要恢复主收集器数据库，请执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到主收集器系统。
2. 通过运行以下命令，停止主收集器：
   在 Windows 上

`%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl` 或
`%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`

在 Linux 上

`/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl`

3. 运行以下命令：

   在 Windows 上

   <安装目录>\traffic-master\bin\nmstrafficmasterresetdb.ovpl

   在 Linux 上

   /opt/OV/traffic-master/bin/nmstrafficmasterresetdb.ovpl

4. 运行以下命令恢复主收集器配置文件和数据库：
   `nmstrafficmasterrestore.ovpl -source <要恢复的存档文件的完整路径> -scope [all|db]`

   在此实例中，<要恢复的存档文件的完整路径>是要恢复的备份文件的完整路径。

   选项 `all` 将恢复数据库和配置文件的备份。仅当之前在备份主收集器 (第 66 页)的步骤 3 中使用选项 `all` 备份过数据库和配置文件后，才可使用选项 `all` 恢复备份。

   选项 `db` 仅恢复数据库的备份。仅当之前在备份主收集器 (第 66 页)的步骤 3 中使用选项 `db` 备份过数据库后，才可使用选项 `db` 恢复备份。

5. 如果新系统的 FQDN 与原始主收集器系统(在其中进行备份)的 FQDN 不同，请执行更改主收集器主机名 (第 61 页)中的步骤。

6. 通过运行以下命令，启动主收集器：
   在 Windows 上

   `%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl` 或
   `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl`

   在 Linux 上

   `/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl`

备份叶收集器

要备份叶收集器，请执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到叶收集器系统。
2. 通过运行以下命令，停止叶收集器：
   在 Windows 上

   `%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl` 或
   `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl`

   在 Linux 上

   `/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl`

3. 运行以下命令启动叶收集器数据库和配置文件的备份：
   `nmstrafficleafbackup.ovpl -target <目标存档文件的完整路径> -scope [all|db]`

   在此实例中，<目标存档文件的完整路径>是用于存储备份文件的目录。

   选项 `all` 可以备份数据库和配置文件。

   选项 `db` 仅可备份数据库。

   备份脚本可创建备份数据的 tar 文件。

4. 通过运行以下命令，启动叶收集器：
   在 Windows 上

   %NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl 或
   %TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl

   在 Linux 上

   /opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl

重置叶收集器数据库

要重置叶收集器数据库，请执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到叶收集器系统。
2. 通过运行以下命令，停止叶收集器：
   在 Windows 上

   %NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl 或
   %TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl

   在 Linux 上

   /opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
3. 运行以下命令重置叶收集器数据库：
   nmstrafficleafresetdb.ovpl -start
4. 通过运行以下命令，启动叶收集器：
   在 Windows 上

   %NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl 或
   %TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl

   在 Linux 上

   /opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl

恢复叶收集器

备注： 恢复叶收集器数据库之前，必须先重置叶收集器数据库，如重置叶收集器数据库 (第 69 页)中所述。

要恢复叶收集器数据库，请执行以下步骤：

1. 在 Windows 上以管理员身份，在 Linux 上以根用户身份登录到叶收集器系统。
2. 通过运行以下命令，停止叶收集器：
   在 Windows 上

   %NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl 或
   %TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl

   在 Linux 上

   /opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
3. 运行以下命令恢复叶收集器配置文件和数据库：
   nmstrafficleafrestore.ovpl -source <要恢复的存档文件的完整路径> -scope [all|db]
   在此实例中，<要恢复的存档文件的完整路径>是要恢复的备份文件的完整路径。

选项 all 将恢复配置文件和数据库的备份。仅当之前在备份叶收集器 (第 68 页)的步骤 3 中使用选项 all 备份过配置文件和数据库后，才可使用选项 all 恢复备份。

选项 db 仅恢复数据库的备份。仅当之前在备份叶收集器 (第 68 页)的步骤 3 中使用选项 db 备份过数据库后，才可使用选项 db 恢复备份。

4. 如果新系统的 FQDN 与原始叶收集器系统(在其中进行备份)的 FQDN 不同，请执行更改叶收集器主机名 (第 63 页)中的步骤。
5. 通过运行以下命令，启动叶收集器：
在 Windows 上

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl 或
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

在 Linux 上

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

第 11 章: NNM iSPI Performance for Traffic 日志记录

要监视主收集器或叶收集器的性能，或观察 NNM iSPI Performance for Traffic 进程和服务的行为，可以查看显示 NNM iSPI Performance for Traffic 的进程和服务活动历史的日志文件。这些文件位于以下目录中：

- 主收集器
  Windows

  `%NnmDataDir%\log\traffic-master` 或 `%TrafficDataDir%\log\traffic-master`

  Linux

  `/var/opt/OV/log/traffic-master`
- 叶收集器
  Windows

  `%NnmDataDir%\log\traffic-leaf` 或 `%TrafficDataDir%\log\traffic-leaf`

  Linux

  `/var/opt/OV/log/traffic-leaf`

NNM iSPI Performance for Traffic 在以下日志文件中存储日志消息：

- 对于叶收集器：`traffic_spi_leaf.log`
- 对于主收集器：`traffic_spi_master.log`

NNM iSPI Performance for Traffic 用以下日志记录级别记录消息：

- SEVERE：与异常主收集器或叶收集器行为相关的事件。
- WARNING：表示存在潜在问题的事件。
- INFO：写入到 NNMi 控制台(或其同等设备)的消息，以及 WARNING 日志记录级别中包含的所有消息。

第 12 章: 在全局网络管理环境中部署 NNM iSPI Performance for Traffic

NNM iSPI Performance for Traffic 为在全局网络管理环境中部署提供了充分支持。每个实例具有以下组件：

- NNMi
- NNM iSPI Performance for Metrics 和 Network Performance Server
- NNM iSPI Performance for Traffic 主收集器
- NNM iSPI Performance for Traffic 叶收集器

全局管理器中的 NNMi 从区域管理器那里接收数据。全局管理器中的主收集器可以配置为通过以下方式从区域主收集器接收数据：

- 全局管理器中的主收集器可从区域管理器中的主收集器接收数据。这种情况下，您必须在全局主收集器中将区域主收集器添加为远程主源。这可以确保将区域主收集器接收的完整数据集转发到全局主收集器。在上述场景中，全局主收集器接收叶收集器 1 和叶收集器 2 处理过的数据。
- 全局管理器中的主收集器可直接从区域叶收集器系统接收数据，绕过区域主收集器。这种情况下，可将区域叶收集器(上述场景中的叶收集器 3)作为叶远程源添加到全局主收集器。这将确保远程叶收集器系统上所有叶收集器接收的数据都会发送到区域主收集器和全局主收集器。

仅可将区域主收集器或区域叶收集器配置为将数据发送到全局主收集器。全局主收集器无法管理这些组件。

将所有区域主收集器作为远程主源添加到全局主收集器。

词汇表

会

会话
会话是在两个设备之间传输数据包的过程。NNM iSPI Performance for Traffic 可以根据 IP 流记录中可用的数据计算在两个设备之间交换的数据包数量(即会话数量) ，并突出显示“排名靠前的会话”报告中会话数量较多的节点对。

节

节点对
“节点对”是交换数据包的一对设备或系统。NNM iSPI Performance for Traffic 可以从叶收集器采集的 IP 流记录标识节点对。

聚

聚合数据
叶收集器可以通过应用内置聚合规则每隔 5 分钟聚合一次原始数据样本。原始数据样本采集自由不同流导出路由器转发到叶收集器的流记录。此数据用于从 Interface_Traffic_Aggregated ExtensionPack 生成报告。

流

流
流或“流量流”是从一个设备或系统发送到另一个设备或系统的一系列数据包。

目

目标
源是网络上的设备或系统，能够接收来自其他设备或系统的数据包。

应

应用程序
NNM iSPI Performance for Traffic 使您能够将流量流与在网络环境中运行的应用程序关联。借助“NNM iSPI Performance for Traffic 配置”表单，您可以将每个流映射到应用程序。在“排名靠前的应用程序”报告中，NNM iSPI Performance for Traffic 提供了具有较多数量的流量流的应用程序列表。

原

原始数据

原始数据是由网络上的流量流导出路由器导出且由 NNM iSPI Performance for Traffic 叶收集器采集的 IP 流记录集。NNM iSPI Performance for Traffic 将原始数据直接记录到 NPS 数据库。在大型环境中，建议禁用将原始数据记录到 NPS 数据库。

源

源

源是网络上的设备或系统，能够将数据包发送到其他设备或系统。从 IP 流记录，NNM iSPI Performance for Traffic 可以标识发出每个流量流的设备或系统。

站

站点

联网设备的逻辑组织。在企业网络中，站点可以是通常位于相似地理位置的联网设备的逻辑分组。位置可以包含楼层、建筑物或整个分公司，或者通过 WAN/MAN 与其他分公司连接的数个分公司。每个站点都可由其名称唯一识别。对于服务提供商网络，可将提供商边缘 (PE) 路由器或客户边缘 (CE) 路由器上的虚拟路由和转发 (VRF) 定义为站点。将网络设备逻辑分组到站点，使您能够获得网络性能的概述。

站点优先级

一个接口只能与一个站点相关联。创建站点时，需要为站点指定位序，以解决一个接口与多个站点匹配的冲突。NNM iSPI Performance for Traffic 将接口与具有最小位序的站点相关联。如果没有为站点提供位序，则 NNM iSPI Performance for Traffic 会分配默认位序。站点的默认位序的优先级最低。如果一个接口与多个站点匹配，则具有最小位序的站点优先与此接口相关联。

发送文档反馈

如果对本文档有任何意见，可以通过电子邮件与文档团队联系。如果在此系统上配置了电子邮件客户端，请单击以上链接，此时将打开一个电子邮件窗口，主题行中为以下信息：

关于部署参考 (Network Node Manager iSPI Performance for Traffic Software 10.20) 的反馈

只需在电子邮件中添加反馈并单击“发送”即可。

如果没有可用的电子邮件客户端，请将以上信息复制到 Web 邮件客户端的新邮件中，然后将您的反馈发送至 network-management-doc-feedback@hpe.com 。

我们感谢您提出宝贵的意见！