HP Network Node Manager i Software

软件版本：10.10
Windows® 和 Linux® 操作系统

强化指南

文档发布日期：2015 年 11 月
软件发布日期：2015 年 11 月

法律声明

担保

HP 产品和服务的唯一担保已在此类产品和服务随附的明示担保声明中提出。此处的任何内容均不构成额外担保。HP 不会为此处出现的技术或编辑错误或遗漏承担任何责任。

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 HP 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。

Oracle Technology - 受限权利声明

根据 DOD FAR Supplement 提供的程序是“商业计算机软件”，这些程序（包括文档）的使用、复制和披露将受限于适用的 Oracle 许可协议中规定的许可限制。否则，根据 Federal Acquisition Regulations 提供的程序是“受限制的计算机软件”，这些程序（包括文档）的使用、复制和披露应受限于“FAR 52.227-19, 商业计算机软件 - 受限权利（1987 年 6 月）”中的限制。Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065。

有关完整的 Oracle 许可证文本，请访问 NNMi 产品 DVD 上的 license-agreements 目录。

版权声明

© Copyright 2015 Hewlett-Packard Development Company, L.P.

商标声明

Adobe® 是 Adobe Systems Incorporated 的商标。

Apple 是 Apple Computer, Inc. 在美国和其他国家/地区的注册商标。

AMD 是 Advanced Micro Devices, Inc. 的商标。

Google™ 是 Google Inc. 的注册商标。

Intel®、Intel® Itanium®、Intel® Xeon® 和 Itanium® 是 Intel Corporation 在美国和其他国家/地区的商标。

Linux® 是 Linus Torvalds 在美国和其他国家/地区的注册商标。

Internet Explorer、Lync、Microsoft、Windows 和 Windows Server 是 Microsoft Corporation 在美国和/或其他国家/地区的注册商标或商标。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。

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

sFlow 是 InMon Corp 的注册商标。

UNIX® 是 The Open Group 的注册商标。

致谢

本产品包含由 Apache Software Foundation 开发的软件。
(http://www.apache.org)。

本产品包含由 Visigoth Software Society (http://www.visigoths.org/) 开发的软件。

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。

要检查是否有最新的更新，或者验证是否正在使用最新版本的文档，请访问：**https://softwaresupport.hp.com**

需要注册 HP Passport 才能登录此站点。要注册 HP Passport ID，请访问：**https://hpp12.passport.hp.com/hppcf/createuser.do**

或单击 HP 软件支持页面顶部的 **Register** 链接。

此外，如果订阅了相应的产品支持服务，则还会收到更新的版本或新版本。有关详细信息，请与您的 HP 销售代表联系。

支持

请访问 HP 软件联机支持网站：**https://softwaresupport.hp.com**

此网站提供了联系信息，以及有关 HP 软件提供的产品、服务和支持的详细信息。

HP 软件联机支持提供客户自助解决功能。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 HP 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 HP Passport ID，请访问：

https://hpp12.passport.hp.com/hppcf/createuser.do

要查找有关访问级别的详细信息，请访问：

https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now 可访问 HPSW 解决方案和集成门户网站。此网站将帮助您寻找可满足您业务需求的 HP 产品解决方案，包括 HP 产品之间的集成的完整列表以及 ITIL 流程的列表。此网站的 URL 为 **http://h20230.www2.hp.com/sc/solutions/index.jsp**

目录

使用本指南

本文档提供有关增强 NNMi 安装安全性的信息。本文档中的信息适用于 NNMi 10.10。有关其他产品版本的安全配置，请参阅该版本的相应文档。

除非步骤中另有说明，否则此文档中内容的预期使用模式如下：

1. 停止所有的 NNMi 服务（请参阅启动、停止或重新启动所有 NNMi 服务 (第 15 页)）。
2. 按本文档中所述应用所需的配置。

   备注: 在进行任何更改之前，请记得将每个配置文件备份到 NNMi 目录结构以外的位置。

3. 启动所有的 NNMi 服务（请参阅启动、停止或重新启动所有 NNMi 服务 (第 15 页)）。

备注: 在 NNMi 全局网络管理 (GNM)、应用程序故障转移或高可用性环境中，一次只能在一个 NNMi 管理服务器上工作。即，在一个 NNMi 管理服务器上，停止 NNMi 服务、应用更改，然后在该 NNMi 管理服务器上启动 NNMi 服务。此方法如有例外请务必指出。

请注意本文档中使用的以下约定：

- 某些文件路径包含 <产品> 目录。将 <产品> 替换为您要配置的特定产品。可能值如下：
  - nnm
  - qa
  - traffic-master
  - traffic-leaf
  - ipt
  - mcast
  - mpls
- 对于 NNMi 和 HP Network Node Manager i Software Smart Plug-ins (iSPIs)，server.properties 文件中指定的任何配置均将覆盖默认配置。此文件位置如下：
  - Windows:

    %NnmDataDir%\nmsas\<产品>\server.properties
  - Linux:

    /var/opt/OV/nmsas/<产品>/server.properties
- 对于 Network Performance Server (NPS)，NNMPerformanceSPI.cfg 文件中指定的任何配置均将覆盖默认配置。此文件位置如下：
  - Windows:

    %NnmDataDir%\NNMPerformanceSPI\rconfig\NNMPerformanceSPI.cfg

- Linux:
  /var/opt/OV/NNMPerformanceSPI/rconfig/NNMPerformanceSPI.cfg

通信配置

本主题描述与 NNMi 通信的默认安全配置。

- 默认情况下，NNMi 和 HP Network Node Manager i Software Smart Plug-ins (iSPIs) 使用 HTTP 与 Web 浏览器进行通信。

  备注: 建议如产品文档中所述，为每个产品启用 HTTPS 通信。

- 与 NNMi Web 服务器进行 HTTPS 通信所用的默认 SSL 协议是 TLSv1.0、TSLv1.1 和 TLSv1.2。

  备注: 如果不需要与不支持 TLSv1.2 的应用程序通信，建议禁用 TLSv1.0 和 TLSv1.1。有关说明，请参阅配置 TLS 协议 (第 7 页)。

配置 TLS 协议

默认情况下，NNMi 支持以下协议:

- SSLv2Hello
- TLSv1.0
- TLSv1.1
- TLSv1.2

如果不需要与不支持 TLSv1.2 的应用程序通信，建议禁用 TLSv1.0 和 TLSv1.1。

使用以下文件中的 `com.hp.ov.nms.ssl.PROTOCOLS` 参数来配置要使用的协议:

- Windows:

  `%NnmDataDir%\nmsas\<产品>\server.properties`

- Linux:

  `/var/opt/OV/nmsas/<产品>/server.properties`

应用程序故障转移

在应用程序故障转移环境中，NNMi 始终使用 TLSv1.2 在 NNMi 管理服务器之间进行通信。无法配置此设置。

加密

本主题描述 NNMi 中的加密和哈希算法的默认安全配置。

- 安装期间，NNMi 使用 2048 位加密密钥、SHA 256 和 RSA 生成自签名证书。

  备注: HP 建议使用 CA 签名证书，而非 NNMi 提供的自签名证书。

- 对于通过本地身份验证登录的 NNMi 的，NNMi 使用强化的 SHA-256 密码哈希算法来存储 NNMi 用户密码。
- 对于存储在 NNMi 数据库中的设备密码加密，NNMi 使用 AES 128 算法。

有关详细信息，请参阅《HP Network Node Manager i Software 部署参考》中的“NNMi 数据加密”。

密码

有关更改嵌入式数据库密码的信息，请参阅《HP Network Node Manager i Software 部署参考》中的“为嵌入式数据库工具提供密码”。

用户身份验证

用户可以通过使用本地用户帐户或使用若干外部身份验证组件之一登录到 NNMi 控制台。每种方法都需要进行管理设置。

本地用户帐户

本地用户帐户仅特定于 NNMi 安装。NNMi 不支持为本地用户帐户配置密码策略。

备注: 如果环境的安全标准需要特定的密码策略（例如，最小密码长度或密码有效期），则建议使用外部机制进行用户身份验证。请参阅外部身份验证 (第 10 页)。

有关创建本地 NNMi 用户帐户的信息，请参阅 NNMi 帮助中的“配置用户帐户”。

外部身份验证

外部身份验证组件的管理员确定所有用户以及使用该组件的所有应用程序的安全行为。

NNMi 控制台会话超时

默认情况下，NNMi 控制台会话超时是 18 个小时。NNMi 管理员可在“用户界面配置”表单（**配置 > 用户界面 > 用户界面配置**）的**控制台超时**字段中为所有 NNMi 控制台用户更改此值。

备注: 建议根据环境策略来配置会话超时。

点击劫持保护

当链接与 NNMi 管理服务器都来自 SAMEORIGIN 时，NNMi 将配置为在新帧中打开链接的页面。此配置不可更改。

增强安全性

您可以通过应用以下任何或全部更改来增强 NNMi 的安全性：

配置 NNMi Web 服务器所使用的密码

NNMi 支持使用以下密码与 NNMi Web 服务器进行安全通信。

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_HA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

要更改 NNMi 可使用的协议列表，请在以下文件中取消注释并配置 `com.hp.ov.nms.ssl.CIPHERS` 参数：

- Windows:

  `%NnmDataDir%\shared\<产品>\conf\props\nms-jboss.properties`
- Linux:

  `var/opt/OV/shared/<产品>/conf/props/nms-jboss.properties`

此参数包含一个或多个密码的排序列表。如果 NNMi 无法使用该列表中的第一个密码以在 NNMi Web 服务器和用户的 Web 浏览器之间建立连接，NNMi 将尝试使用下一个密码，以此类推。（之前的列表将显示默认密码排序。）

可以通过编辑 com.hp.ov.nms.ssl.CIPHERS 参数的值来删除 NNMi 不应使用的密码，以及更改 NNMi 尝试使用可用密码的顺序。

如果更改受支持的密码列表，HP 建议按照密码强度对密码列表进行排序。即，将 256 位加密密码放在 128 位加密密码前面。

备注:

- com.hp.ov.nms.ssl.CIPHERS 参数的值必须是逗号分隔列表，其中不包含空格且是连续的一行。
- 更改之前请先保存密码列表。从 com.hp.ov.nms.ssl.CIPHERS 列表删除密码可防止 NNMi 启动。
- Web 浏览器必须支持至少一个已配置的密码。
- 在 GNM 环境中，修改一个 NNMi 管理服务器上的文件，然后将修改后的文件复制到 GNM 环境中的其他 NNMi 管理服务器上。将此文件放置到所有 NNMi 管理服务器上后，重新启动所有 NNMi 管理服务器。

  在高可用性环境中，只能修改活动 NNMi 管理服务器上的文件。

应用程序故障转移：配置 NNMi Web 服务器所使用的密码

在应用程序故障转移环境中，应用程序故障转移 fileIO 端口的密码配置使用以下文件中的 com.hp.ov.nms.cluster.ssl.CIPHERS 参数：

- Windows:

  %NnmInstallDir%\misc\<产品>\props\shared\nms-cluster.properties
- Linux:

  /opt/OV/misc/<产品>/props/shared/nms-cluster.properties

修改一个 NNMi 管理服务器上的文件，然后将修改后的文件复制到应用程序故障转移群集中的其他 NNMi 管理服务器上。

支持的密码和配置注意事项与配置 NNMi Web 服务器所使用的密码 (第 12 页)中所述相同。

限制用户对 NNMi Web 服务器的访问

建议限制只有应该具有访问权限的用户才可以访问 NNMi Web 服务器。限制此访问的可能方式包括：

- 在 NNMi 管理服务器前面配置防火墙。

  有关 NNMi 使用的端口的信息，请参阅《NNMi 部署指南》中的“NNMi 和 NNM iSPI 默认端口”。
- 仅在特定网络接口上隔离用户对 NNMi 管理服务器的访问。

禁用 JMX 控制台

如果不需要用于进行疑难解答，建议禁用 JMX 控制台。

备注: **对于 NNM iSPI Performance for Traffic，必须在主收集器系统和每个叶收集器系统上执行此任务。**

因为 NNM iSPI Performance for Metrics 不提供 JMX 控制台，因此不需要针对 NNM iSPI Performance for Metrics 执行此任务。

要禁止访问 JMX 控制台，请将以下内容:

```
<!-- disable the jmx-console -->
<realm name="jmx-console">
    <mode>NO_ACCESS</mode>
</realm>
```

添加到以下文件的 `realms` **块内:**

- Windows:

  `%NnmDataDir%\nmsas\<产品>\conf\nms-auth-config.xml`

- Linux:

  `var/opt/OV/nmsas/<产品>/conf/nms-auth-config.xml`

例如:

```
<!-- realms describes the configuration of specific services or applications -->
<realms>
    <!-- valid modes are X509 or FORM -->
    <realm name="console">
        <mode>FORM</mode>
    </realm>
    <!-- disable the jmx-console -->
    <realm name="jmx-console">
        <mode>NO_ACCESS</mode>
    </realm>
</realms>
```

然后，运行相应命令重新读取 `nms-auth-config.xml` **文件:**

- NNMi: **`nnmsecurity.ovpl -reloadAuthConfig`**
- NNM iSPI Performance for QA: **`nmsqaauthconfigreload.ovpl -reloadAuthConfig`**
- NNM iSPI Performance for Traffic 主收集器: **`nmsmasterauthconfigreload.ovpl -reloadAuthConfig`**
- NNM iSPI Performance for Traffic 叶收集器: **`nmsleafauthconfigreload.ovpl -reloadAuthConfig`**
- NNM iSPI for IP Telephony: **`nmsiptauthconfigreload.ovpl -reloadAuthConfig`**
- NNM iSPI for MPLS: **`nmsmplsauthconfigreload.ovpl -reloadAuthConfig`**
- NNM iSPI for IP Multicast: **`nmsmcastauthconfigreload.ovpl -reloadAuthConfig`**

要重新启用 JMX 控制台以进行疑难解答，请先注释掉之前的配置，然后重新运行重新加载命令。

启动、停止或重新启动所有 NNMi 服务

更改 NNMi 配置之前停止 NNMi 服务可防止将冲突数据存储在 NNMi 数据库中。有些程序要求重新启动 NNMi 服务才能读取更新后的配置。

提示: `ovstart` 和 `ovstop` 命令适用于以下所有产品（如果已安装在环境中）：

- NNMi
- NNM iSPI for IP Telephony
- NNM iSPI for MPLS
- NNM iSPI for IP Multicast
- NNM iSPI Performance for Quality Assurance

有关 NNM iSPI Performance for Traffic 的信息，请参阅启动、停止或重新启动所有 NNM iSPI Performance for Traffic 服务 (第 17 页)。

按照特定于环境的说明执行操作：

- 一个 NNMi 管理服务器或 GNM (第 15 页)
- 应用程序故障转移 (第 16 页)
- 高可用性 (第 16 页)

一个 NNMi 管理服务器或 GNM

启动所有 NNMi 服务

- Windows：执行以下某项操作：
  - 从 Windows“开始”菜单，运行**所有程序 > HP > Network Node Manager > ovstart**。
  - 运行以下命令：

    ```
    %NnmInstallDir%\bin\ovstart
    ```
- Linux：运行以下命令：

  ```
  /opt/OV/bin/ovstart
  ```

停止所有 NNMi 服务

- Windows：执行以下某项操作：
  - 从 Windows“开始”菜单，运行**所有程序 > HP > Network Node Manager > ovstop**。
  - 运行以下命令：

    ```
    %NnmInstallDir%\bin\ovstop
    ```
- Linux：运行以下命令：

  ```
  /opt/OV/bin/ovstop
  ```

重新启动所有 NNMi 服务

- Windows：执行以下某项操作：
  - 从 Windows“开始”菜单，运行**所有程序 > HP > Network Node Manager > ovstop**，然后运行**所有程序 > HP > Network Node Manager > ovstart**。
  - 运行以下命令：

    ```
    %NnmInstallDir%\bin\ovstop
    %NnmInstallDir%\bin\ovstart
    ```

- Linux：运行以下命令：

  ```
  /opt/OV/bin/ovstop
  /opt/OV/bin/ovstart
  ```

应用程序故障转移

启动所有 NNMi 服务

- Windows：运行以下命令：

  ```
  %NnmInstallDir%\bin\ovstart
  ```

- Linux：运行以下命令：

  ```
  /opt/OV/bin/ovstart
  ```

停止所有 NNMi 服务

- Windows：运行以下命令：

  ```
  %NnmInstallDir%\bin\ovstop
  ```

- Linux：运行以下命令：

  ```
  /opt/OV/bin/ovstop -nofailover
  ```

重新启动所有 NNMi 服务

- Windows：运行以下命令：

  ```
  %NnmInstallDir%\bin\ovstop -nofailover
  %NnmInstallDir%\bin\ovstart
  ```

- Linux：运行以下命令：

  ```
  /opt/OV/bin/ovstop -nofailover
  /opt/OV/bin/ovstart
  ```

高可用性

请参阅《NNMi 部署参考》中的“维护高可用性配置”。

启动、停止或重新启动所有 NNM iSPI Performance for Traffic 服务

更改 NNM iSPI Performance for Traffic 配置之前停止 NNM iSPI Performance for Traffic 服务可防止将冲突数据存储在 NNM iSPI Performance for Traffic 数据库中。有些程序要求重新启动 NNM iSPI Performance for Traffic 服务才能读取更新后的配置。按照特定于环境的说明执行操作：

独立服务器上（但不在高可用性群集中）的主收集器

启动 NNM iSPI Performance for Traffic 主收集器

- Windows：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl`
- Linux：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl`

停止 NNM iSPI Performance for Traffic 主收集器

- Windows：运行以下命令：
  `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`
- Linux：运行以下命令：
  `/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl`

重新启动 NNM iSPI Performance for Traffic 主收集器

- Windows：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`
  `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl`
- Linux：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl`
  `/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl`

NNMi 管理服务器上（但不在高可用性群集中）的主收集器

启动 NNM iSPI Performance for Traffic 主收集器

- Windows：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl`
- Linux：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl`

停止 NNM iSPI Performance for Traffic 主收集器

- Windows：运行以下命令：
  `%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`
- Linux：运行以下命令：
  `/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl`

重新启动 NNM iSPI Performance for Traffic 主收集器

- Windows：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`
  `%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl`
- Linux：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl`
  `/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl`

高可用性群集中的主收集器

停止流量主服务之前，请通过创建所需的维护文件来禁用高可用性资源组监视。请参阅《NNM iSPI Performance for Traffic 部署参考》中的“在高可用性群集中部署 NNM iSPI Performance for Traffic”。

其他服务器上的叶收集器

启动 NNM iSPI Performance for Traffic 叶收集器

- Windows：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl`
- Linux：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl`

停止 NNM iSPI Performance for Traffic 叶收集器

- Windows：运行以下命令：
  `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl`
- Linux：运行以下命令：
  `/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl`

重新启动 NNM iSPI Performance for Traffic 叶收集器

- Windows：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl`
  `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl`
- Linux：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl`
  `/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl`

NNMi 管理服务器上的叶收集器

启动 NNM iSPI Performance for Traffic 叶收集器

- Windows：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl`
- Linux：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl`

停止 NNM iSPI Performance for Traffic 叶收集器

- Windows：运行以下命令：
  `%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl`
- Linux：运行以下命令：
  `/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl`

重新启动 NNM iSPI Performance for Traffic 叶收集器

- Windows：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl`
  `%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl`
- Linux：验证 NNMi 服务是否正在运行，然后运行以下命令：
  `/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl`
  `/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl`

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：

关于强化指南 (Network Node Manager i Software 10.10) 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！