Hewlett Packard Enterprise

# HPE Network Node Manager i Software

软件版本：10.20
适用于 Windows® 和 Linux® 操作系统

## 强化指南

文档发布日期：2016 年 8 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。HPE 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 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。

**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



## 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.hpe.com/group/softwaresupport/search-result?keyword= 。

此站点要求使用 HP Passport 帐户。如果还不具有该帐户，请单击 HP Passport“Sign in”页面上的 **Create an account** 按钮。

# 支持

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

此网站提供了联系信息，以及有关 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 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 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

# 使用本指南

本文档提供有关增强以下产品安全性的信息：

- NNMi
- NNM iSPI
- Network Performance Server (NPS)

本文档中的信息适用于 NNMi 10.20。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 25 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 25 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 HPE Network Node Manager i Software Smart Plug-in (iSPI)，`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

# HTTPS 通信配置

本主题描述 NNMi 中的 HTTPS 通信的默认安全配置。

- 默认情况下，NNMi 和 HPE Network Node Manager i Software Smart Plug-in (iSPI) 支持 HTTPS 使用安装时生成的自签名证书，

  **备注:** 但我们强烈建议用户安装 CA 签名证书来替换该默认证书。有关详细信息，请参阅《HPE Network Node Manager i Software 部署参考》中的“管理证书”章节。

- 与 NNMi Web 服务器进行 HTTPS 通信所用的默认加密协议是 TLSv1.2。

# 为 HTTPS 通信配置加密协议

默认情况下，NNMi 支持为 HTTPS 通信使用 TLSv1.2 协议。

建议 NNMi 仅使用 TLSv1.2，除非为了支持旧版客户端而不得不使用较不安全的更低版本协议。

要将 NNMi 配置为使用 TLSv1.2 之外的协议，请执行以下步骤：

1. 登录 NNMi 管理服务器。
2. 用文本编辑器打开以下文件：
   - Windows：

     `%NnmDataDir%\nmsas\nms\server.properties`

   - Linux：

     `/var/opt/OV/nmsas/nms/server.properties`

3. 使用含有所需协议的逗号分隔列表添加或更新 `com.hp.ov.nms.ssl.PROTOCOLS` 属性。

   例如，如果要使用 TLSv1、TLSv1.1 和 TLSv1.2 协议，请确保 `server.properties` 文件中存在以下行：

   ```
   com.hp.ov.nms.ssl.PROTOCOLS=TLSv1.0,TLSv1.1,TLSv1.2
   ```

4. 通过运行以下命令重新启动 NNMi 进程：
   - 在 Windows 上：
     i. **%nnminstalldir%\bin\ovstop -c**
     ii. **%nnminstalldir%\bin\ovstart -c**
   - 在 Linux 上：
     i. **/opt/OV/bin/ovstop -c**
     ii. **/opt/OV/bin/ovstart -c**

# 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。

# 强化设备通信

NNMi 使用 SNMP(v1、v2c 和 v3)与许多设备通信。本部分将指导您将 NNMi 配置为针对所有 SNMP 通信仅使用 SNMPv3 安全通信。

# 配置 NNMi 以使用 SNMPv3

使用 SNMPv3 进行发现和通信更为安全，因为 SNMPv3 需要使用基于用户的安全模型 (USM) 用户名，而不是 SNMPv1/SNMPv2c 团体字符串来验证 NNMi 和 SNMP 代理之间发送的消息。请按照《NNMi 管理员帮助》中的"配置通信协议"部分所述，将 NNMi 配置为仅使用 SNMPv3 协议来发现设备以及与设备通信。

# 阻止 SNMPv1 或 SNMPv2c 陷阱

将设备发现配置为仅使用 SNMPv3 后，某些被管节点仍可能尝试向 NNMi 管理服务器发送 SNMPv1 或 SNMPv2c 陷阱。为防止 SNMPv1 或 SNMPv2c 陷阱发送到 NNMi 管理服务器，建议将 NNMi 配置为仅接受 SNMPv3 陷阱并阻止所有 SNMPv1 和 SNMPv2c 陷阱。

**备注:** 完成此配置步骤前，请确保已将 NNMi 配置为使用 SNMPv3 协议发现网络。

1. 登录 NNMi 管理服务器。
2. 运行以下命令：
   在 Windows 上：**"%nnminstalldir%\bin\nnmtrapconfig.ovpl -setProp disallowV1V2 -persist"**
   在 Linux 上：**/opt/OV/bin/nnmtrapconfig.ovpl -setProp disallowV1V2 -persist**
3. 执行以下某项操作：
   - 在 Windows 上：从"服务"窗口重新启动 `NNM TrapReceiver` 服务。
   - 在 Linux 上：运行以下命令：
     **/etc/init.d/nettrap stop**
     **/etc/init.d/nettrap start**

# 配置 SNMPv3 安全通信

如果打算使用 SNMPv3 协议发现设备，则必须额外执行以下步骤，以确保实现通过 FIPS 认证的 SNMPv3 安全通信。

1. 登录 NNMi 管理服务器。
2. 备份以下文件：
   - Windows：`%nnmdatadir%\shared\nnm\conf\crypto\nms-snmpv3-crypto-config.xml`
   - Linux：`/var/opt/OV/shared/nnm/conf/crypto/nms-snmpv3-crypto-config.xml`
3. 转到以下目录：

- Windows：%nnminstalldir%\newconfig\HPOvNmsSnmpCo
- Linux：/opt/OV/newconfig/HPOvNmsSnmpCo

4. 执行以下步骤，在系统上将 nms-snmpv3-crypto-config-fips.xml 文件另存为 nms-snmpv3-crypto-config.xml：
   - Windows：
     i. 用文本编辑器打开 nms-snmpv3-crypto-config-fips.xml 文件。
     ii. 复制该文件的内容。
     iii. 创建一个新的 nms-snmpv3-crypto-config.xml 文件。
     iv. 将之前复制的内容粘贴到 nms-snmpv3-crypto-config.xml 文件中。
     v. 将 nms-snmpv3-crypto-config.xml 文件保存到 %nnmdatadir%\shared\nnm\conf\crypto 目录中。
   - Linux：
     运行以下命令：
     **cp /opt/OV/newconfig/HPOvNmsSnmpCo/nms-snmpv3-crypto-config-fips.xml /var/opt/OV/shared/nnm/conf/crypto/nms-snmpv3-crypto-config.xml**
   - /var/opt/OV/shared/nnm/conf/crypto

   **备注：**此时会覆盖旧版本 nms-snmpv3-crypto-config.xml 文件。
5. 重新启动 NNMi：

# 为 SNMPv3 通信选择通过 FIPS 认证的算法

如果已将 NNMi 配置为使用 SNMPv3 协议发现设备，请确保将 NNMi 配置为使用以下通过 FIPS 认证的算法之一来发现 SNMPv3 信息：

- 验证协议：
  - SHA-1
- 隐私协议：
  - Triple-DES
  - AES-128
  - AES-192
  - AES-256

如果在按照配置 SNMPv3 安全通信 (第 9 页)中的说明操作后使用较弱的算法，则 NNMi 与设备的通信将会失败。

如果在配置发现和通信期间并未选择上面列出的任何算法，请执行以下操作：

1. 以管理员身份登录 NNMi 控制台。
2. 从“配置”工作区中，启动“通信配置”表单。

   **备注:** 请参阅《NNMi 管理员帮助》中的“配置通信协议”一节。

3. 从“通信配置”表单启动“SNMPv3 设置”表单。
4. 将“验证协议”设置为 SHA-1。
5. 将“隐私协议”设置为 Triple-DES、AES-128、AES-192 或 AES-256。
6. 保存配置。

或者，您也可以使用 `nnmcommunication.ovpl` 命令选择这些协议。`-authProtocol` 和 `-privProtocol` 参数可用来选择验证协议和隐私协议。有关详细信息，请参阅参考页(在 NNMi 帮助菜单中，单击**帮助 > NNMi 文档库 > 参考页**)或 Linux 中的 `nnmcommunication.ovpl` 手册页。

# 强化加密

本主题描述 NNMi 中的加密和哈希算法的默认安全配置。

- 新安装的 NNMi 10.20 将使用通过美国联邦信息处理标准 (FIPS) 140-2 验证的加密模块 (RSA BSAFE) 进行加密和密钥管理。
- 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:** HPE 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《HPE Network Node Manager i Software 部署参考》中的“NNMi 数据加密”。

# 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 13 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。

# 密码

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

# 将 NNMi 配置为使用 LDAP 或 PKI 用户验证

建议通过轻量级目录访问协议 (LDAP) 将 NNMi 与目录服务集成，或将其配置为使用公钥基础设施 (PKI) 用户验证。

请按照《NNMi 部署参考》中的以下几节所述执行操作：

- 通过 LDAP 将 NNMi 与目录服务集成
- 将 NNMi 配置为支持公钥基础设施用户验证

# 更改默认 NPS 密码

NNM iSPI Performance for Metrics 安装程序在安装 NPS 时会一并安装使用预设密码的以下三个应用程序：

- NPS 数据库
- NPS BI 服务器
- NPS 软件开发套件 (SDK)

为提高所监控环境的安全性，请更改全部三个预设密码。

## 更改 NPS 数据库密码

要更改 NPS 数据库密码，请运行以下命令：

**changeDBpwd.ovpl** <密码>

在此实例中，<密码> 是您选择的密码。

## 更改 NPS BI 服务器密码

要更改 NPS BI 数据库密码，请运行以下命令：

**changeBIpwd.ovpl** <密码>

在此实例中，<密码> 是您选择的密码。

## 更改 NPS SDK 密码

要更改 NPS SDK 密码，请运行以下命令：

**changesdkUserPwd.ovpl -u**<用户名>**-p**<密码>

在此实例中，<用户名>是用户名，<密码>是您选择的密码。

**备注：** changesdkUserPwd.ovpl 命令始终要求为用户名提供一个值。如果只希望更改 NPS SDK 密码，请为命令指定旧用户名。

# 更改 NNMi 嵌入式数据库密码

NNMi 提供了默认密码，该密码可使用 nnmchangeembdbpw.ovpl 脚本更改。

有关详细信息，请参阅《NNMi 部署参考》中的“为嵌入式数据库工具提供密码”部分。

# 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。

# 将 NNMi 配置为使用通过 FIPS 140-2 验证的加密模块

本部分介绍如何将 NNMi 配置为使用通过美国联邦信息处理标准 (FIPS) 140-2 验证的加密模块。FIPS 准则针对美国国家标准与技术研究院 (NIST) 定义的加密模块规定了一套安全要求标准。本部分介绍如何将 NNMi 配置为使用符合 FIPS 要求的加密模块。

**备注:** 您可以只将 NNMi Premium(即 NNMi、NNM iSPI Performance for Metrics 和 NNM iSPI Performance for QA)配置为符合 FIPS 要求。

为了能符合 FIPS 140-2 标准的要求，必须将 NPS 和 NNMi 安装在同一台服务器上。

新安装的 NNMi 10.20 将使用通过 FIPS 140-2 验证的加密模块 (RSA BSAFE) 进行加密和密钥管理。

在升级后的 NNMi 环境中，大多数密码加密和网络通信过程都将自动使用通过 FIPS 认证的密码和算法。但是，在升级后的环境中，确实存在一些不符合 FIPS 准则要求的旧密码和旧算法。

要实现通过 FIPS 140-2 验证的最高级别加密，请执行以下操作：

- 使用全新安装的 NNMi 10.20
- 默认情况下，NNMi 会安装一个自签名证书。HPE 建议使用 CA 签名证书，而非该自签名证书。有关使用 CA 签名证书的详细信息，请参阅《NNMi 部署参考》中的“高级配置”部分。
- 根据配置步骤禁用一些未通过 FIPS 认证的较弱的 SNMPv3 密码。
- 仅使用 NNMi Premium。
- 在同一系统上安装 NNMi 和 NPS。

**备注:** 即便满足了上述列出的要求，NNMi 和 NPS 的以下组件仍然不会使用通过 FIPS 140-2 验证的加密：

- NPS 控制台
- 性能疑难解答窗口
- NNMi 控制台中“分析”窗格的“性能”选项卡

本部分介绍将 NNMi 配置为使用通过 FIPS 140-2 验证的最高级别加密的步骤

# 先决条件

确保禁用 HTTP 通信模式。有关详细信息，请参阅启用仅 HTTPS 通信 (第 22 页)。

# 配置 NNMi

执行以下配置任务：

1. 任务 1：升级后步骤：加密密码

   只有从旧版 NNMi 升级到 NNMi 10.20 后，才需要执行此步骤。

   如果在将 NNMi 升级到 10.20 之前未使用 `nnmsetcmduserpw.ovpl` 命令，则跳过此步骤。

   **提示：**有关详细信息，请参阅 `nnmsetcmduserpw.ovpl` 命令的参考页。

   如果使用了 `nnmsetcmduserpw.ovpl` 命令来配置有效的 NNMi 用户名属性值和 NNMi 密码属性值以无缝运行命令行工具，则必须执行以下步骤：

   a. 以根用户或管理员身份登录到 NNMi 管理服务器。
   b. 再次运行 `nnmsetcmduserpw.ovpl` 命令，以配置在将 NNMi 升级到版本 10.20 之前设置的所有 NNMi 凭据。

      **提示：**要找出在将 NNMi 升级到 10.20 之前已使用 `nnmsetcmduserpw.ovpl` 命令加密密码的所有用户，请找到 `nms-users.properties` 文件，然后检查文件内容。服务器上可能存在 `nms-users.properties` 文件的多个副本。

2. 配置 SNMPv3 安全通信 (第 9 页)
3. 为 SNMPv3 通信选择通过 FIPS 认证的算法 (第 10 页)

# 限制对 NPS 数据库的远程访问

**备注:** 如果 NNMi 和 NPS 未安装在同一系统上，请勿按本部分的说明操作。

NPS 使用嵌入式数据库存储 NNMi 和 iSPI 收集的性能数据，以便构建报告。NPS 会使用名为内容存储的另一个数据库存储并维护有关扩展包和报告的全部详细信息。执行此步骤可防止远程系统访问这两个数据库。

NPS 数据库使用以下端口：

- 9301
- 9303
- 9306

此步骤有助于配置在 NNMi 管理服务器上运行的防火墙，以便利用防火墙阻止通过这些端口的通信。

限制对嵌入式 NPS 数据存储的远程访问：

在 Windows 上：

使用 Windows 防火墙程序阻止通过 9303 和 9306 端口的远程通信。有关详细信息，请参阅 Microsoft Windows 文档。

在 Linux 上：

1. 以根用户身份登录到 NNMi 管理服务器。
2. 运行以下命令：
   a. **service iptables start**
   b. **iptables -A INPUT -p tcp -i eth+ --dport 9303 -j REJECT**
   c. **iptables -A INPUT -p tcp -i eth+ --dport 9306 -j REJECT**
   d. **service iptables save**

限制对内容存储的远程访问：

1. 以根用户或管理员身份登录到 NNMi 管理服务器。
2. 用文本编辑器打开以下文件：
   - 在 Windows 上：`%nnminstalldir%\nonOV\sybasease\interface`
   - 在 Linux 上：`/opt/OV/nonOV/sybasease/interfaces`
   - 确保以下各行不含任何外部 IP 地址或主机名：

```
ASECONTENTSERVER

                    master tcp ether 127.0.0.1 9301


                    query tcp ether 127.0.0.1 9301

ASECONTENTSERVER_BS
```

```
master tcp ether localhost 9308

query tcp ether localhost 9308
```

# 配置 NPS 控制台

**备注:** 如果 NNMi 和 NPS 未安装在同一系统上，请勿按本部分的说明操作。

除了禁用对 NPS 数据库的远程访问外，您还可通过执行以下步骤，将 NPS 控制台配置为限制用户从远程系统启动 BI 服务器门户：

1. 登录 NNMi 管理服务器。
2. 用文本编辑器打开以下文件：
   a. Windows：`%ovdatadir%\NNMPerformanceSPI/rconfig/NNMPerformanceSPI.cfg`
   b. Linux：`/var/opt/OV/NNMPerformanceSPI/rconfig/NNMPerformanceSPI.cfg`
3. 为防止用户从远程系统启动 BI 服务器门户，请将 `CC_DISABLE_REMOTE_COGNOS_ADMINISTRATION` 设置为 `true`。
4. 保存该文件。
5. 通过运行以下命令重新启动 BI 服务器：
   a. **stopBI.ovpl**
   b. **startBI.ovpl**

   目前在 NPS 控制台中无法继续使用 BI 服务器工作区下的菜单项目。

   **备注:** 但您仍可登录 NPS 系统，使用本地浏览器启动 NPS 控制台，然后再使用 BI 服务器工作区。

# 审核

默认情况下，对 NNMi、NPS 和 NNM iSPI Performance for QA 启用用户操作审核。

有关 NNMi 审核日志文件的详细信息，请参阅《NNMi 联机帮助》。

有关 NPS 和 NNM iSPI Performance for Metrics 审核日志文件的详细信息，请参阅《NNM iSPI Performance for Metrics 联机帮助》。

有关 NNM iSPI Performance for QA 审核日志文件的详细信息，请参阅《NNM iSPI Performance for QA 联机帮助》。

# 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：



# 启用仅 HTTPS 通信

### 对 NNMi 启用仅 HTTPS 通信

将 NNMi 安装和配置为使用 HTTPS 通信后，HTTP 通信模式仍可使用。为了能限制通过 HTTP 对 NNMi 进行远程访问，请完全禁用 NNMi 的 HTTP 通信模式，为此请按照《NNMi 部署参考》中的“将 NNMi 配置为要求加密远程访问”一节所述执行相关操作。

**备注:** 在全局网络管理环境中，请对每个区域管理器和全局管理器执行此任务。

### 对 NPS 启用仅 HTTPS 通信

确保将 NPS 配置为仅使用 HTTPS。请参阅启用 HTTPS 通信 (第 24 页)。

# 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，HPE 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 22 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。

# 加强 NPS 安全性

本部分介绍在安装和配置了 NPS 的环境中增强安全的必要步骤。

## 启用 HTTPS 通信

确保 NPS 已安装且已配置为仅使用 HTTPS 协议。
从 HTTPS 通信切换为 HTTP 通信：

1. 以根用户或管理员身份登录到 NPS 系统。
2. 运行以下命令：

   **configureWebAccess.ovpl -ssl**

# 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 QA

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 27 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 25 页)
- 应用程序故障转移 (第 26 页)
- 高可用性 (第 26 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 10.20) 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！