HP Network Node Manager i Software

ソフトウェアバージョン: 10.10
Windows®およびLinux®オペレーティングシステム

強化ガイド

ドキュメントのリリース日 : 2015年11月
ソフトウェアのリリース日 : 2015年11月

ご注意

保証

HP製品とサービスに関する単独の保証は、かかる製品とサービスに付属する保証ステートメントに明示的に定められています。ここに記載された情報は追加の保証をなすものではありません。HPではここに記載されている技術的、または編集上の不正確さや脱漏については責任を負いません。

ここに記載されている情報は予告なく変更されることがあります。

制限付き権利

機密コンピューターソフトウェア所有、使用、またはコピーに必要なHP提供の有効ライセンス。FAR 12.211および12.212に準拠し、商用コンピューターソフトウェア、コンピューターソフトウェアドキュメント、および商用アイテムの技術データは、ベンダーの標準商用ライセンスの下、米国政府にライセンスされています。

Oracleテクノロジの制限された権限に関する通知

DOD FAR Supplementによって届けられたプログラムは、「商業用コンピューターソフトウェア」であり、ドキュメントを含むプログラムの使用、複製、開示についてはOracleの適切なライセンス契約に基づくライセンス制限に拠る必要があります。それ以外の場合は、連邦調達規則に従って供給されたプログラムは、「制限されたコンピューターソフトウェア」であり、関連文書を含むプログラムの使用、複製、および公開は、FAR 52.227-19、『商用コンピューターソフトウェア - 制限された権限』(1987年6月) に記載されている制限に従うものとします。Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Oracleライセンスの全文は、NNMiの製品DVDにあるlicense-agreementsのディレクトリを参照してください。

著作権

商標について

Adobe ® はAdobe Systems Incorporatedの登録商標です。

Appleは、米国およびその他の国で登録されたApple Computer, Incの商標です。

AMDは、Advanced Micro Devices, Inc.の商標です。

Google™ は、Google Inc.の登録商標です。

Intel ® 、Intel ® Itanium ® 、Intel ® Xeon ® 、およびItanium ® は、米国およびその他の国におけるIntel Coporationの商標です。

Linux ® は、Linus Torvalds氏の米国およびその他の国における登録商標です。

Internet Explorer、Lync、Microsoft、Windows、およびWindows Serverは、米国およびその他の国における Microsoft Corporationの登録商標または商標です。

OracleおよびJavaはOracleおよびその関連会社の登録商標です。

Red Hat ® Enterprise Linux Certifiedは、米国およびその他の国におけるRed Hat, Incの登録商標です。

sFlowは、InMon Corp.の登録商標です。

UNIX ® はThe Open Groupの登録商標です。

謝辞

この製品には、Apache Software Foundationで開発されたソフトウェアが含まれています。(http://www.apache.org/)

この製品には、Visigoth Software Society (http://www.visigoths.org/) によって開発されたソフトウェアが含まれています。

マニュアル更新

このドキュメントのタイトルページには、次の識別情報が含まれています。

- ソフトウェアーバージョン番号。ソフトウェアーのバージョンを示します。
- ドキュメントリリース日。ドキュメントが更新されるたびに変更されます。
- ソフトウェアリリース日。ソフトウェアのこのバージョンのリリース日を示します。

最近の更新を確認するか、ドキュメントの最新版を使用していることを確認するには、次のサイトを参照してください。**https://softwaresupport.hp.com**

このサイトでは、HPパスポートに登録してサインインする必要があります。HPパスポートIDに登録するには、次のURLにアクセスしてください。**https://hpp12.passport.hp.com/hppcf/createuser.do**

または、[HPソフトウェアサポート] ページ上部にある [**登録**] リンクをクリックしてください。

適切な製品サポートサービスの契約をしている場合は、更新版または新版を受信することもできます。詳細については、HPの営業担当者に問い合わせてください。

サポート

HPソフトウェアーサポートオンラインWebサイトへのアクセス:**https://softwaresupport.hp.com**

このWebサイトでは、製品、サービス、およびHPソフトウェアーが提供するサポートに関する詳細と連絡先の情報を提供します。

HPソフトウェアーオンラインサポートでは、お客様ご自身で問題を解決できるケーパビリティを提供しています。すばやく効率的な方法で、お客様のビジネス管理に必要な対話型テクニカルサポートツールにアクセスできます。サポートの大切なお客様として、サポートWebサイトで次の操作が可能です。

- 興味のあるナレッジドキュメントの検索
- サポート事例と改善要求の送信と追跡
- ソフトウェアーパッチのダウンロード
- サポート契約の管理
- HPサポート契約の検索
- 利用可能なサービスに関する情報のレビュー
- 他のソフトウェアーユーザーとの情報交換
- ソフトウェアートレーニングの調査と登録

ほとんどのサポートエリアでは、HPパスポートのユーザーとして登録してサインインする必要があります。また、多くのエリアではサポート契約も必要です。HPパスポートIDに登録するには、次のURLにアクセスしてください。

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

アクセスレベルの詳細については、次のURLにアクセスしてください。

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

HP Software Solutions Now (英語) はHPSWのソリューションと統合に関するポータルWebサイトです。このサイトでは、お客様のビジネスニーズを満たすHP製品ソリューションを検索したり、HP製品間の統合に関する

http://h20230.www2.hp.com/sc/solutions/index.jsp です。

目次

このガイドの使用

このドキュメントには、NNMiインストールのセキュリティの向上に関する情報が記載されています。このドキュメントの情報は、NNMi 10.10に当てはまります。別バージョンの製品のセキュリティ設定については、そのバージョンの該当するドキュメントを参照してください。

手順内で別途指定がない限り、このドキュメントでは次のように操作手順を進めます。

1. すべてのNNMiサービスを停止します (「すべてのNNMiサービスの開始、停止、または再開」(17ページ)を参照してください)。
2. このドキュメントの説明に従い、設定を適宜行います。

   注: 何か変更を加える場合は、変更前にNNMiディレクトリ構造以外の場所に各設定ファイルをバックアップすることを忘れないでください。

3. すべてのNNMiサービスを起動します (「すべてのNNMiサービスの開始、停止、または再開」(17ページ)を参照してください)。

注: NNMiのグローバルネットワーク管理 (GNM) 環境、アプリケーションフェイルオーバー環境、または高可用性環境では、一度に1つのNNMi管理サーバーで作業を行います。つまり、1つのNNMi管理サーバーでNNMiサービスを停止し、変更を適用した後、そのNNMi管理サーバーでNNMiサービスを開始します。この方法が当てはまらない場合は、別途説明されています。

このドキュメントの表記規則は次のとおりです。

- 一部のファイルパスには<PRODUCT>ディレクトリが含まれます。<PRODUCT>は、設定する個々の製品の値に読み替えてください。使用できる値は次のとおりです。
  - nnm
  - qa
  - traffic-master
  - traffic-leaf
  - ipt
  - mcast
  - mpls

- NNMiとHP Network Node Manager i Software Smart Plug-ins (iSPIs)の場合、`server.properties` ファイルに指定されている設定がデフォルトの設定よりも優先されます。このファイルは以下の場所にあります。
  - Windowsの場合:

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

  - Linuxの場合:

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

- Network Performance Server (NPS) の場合、`NNMPerformanceSPI.cfg`ファイルに指定されている設定がデフォルトの設定よりも優先されます。このファイルは以下の場所にあります。
  - Windowsの場合:

    `%NnmDataDir%\NNMPerformanceSPI\rconfig\NNMPerformanceSPI.cfg`

  - Linuxの場合:

    `/var/opt/OV/NNMPerformanceSPI/rconfig/NNMPerformanceSPI.cfg`

通信の設定

このトピックでは、NNMiにおける通信のデフォルトのセキュリティ設定について説明します。

- デフォルトでは、NNMiとHP Network Node Manager i Software Smart Plug-ins (iSPIs)はWebブラウザーとの通信にHTTPを使用します。

  注: 製品のドキュメントの説明に従って製品ごとにHTTPS通信を有効にすることをお勧めします。

- NNMi WebサーバーとのHTTPS通信におけるデフォルトのSSLプロトコルはTLSv1.0、TSLv1.1、およびTLSv1.2です。

  注: TLSv1.2をサポートしないアプリケーションとの通信に必要でない限り、TLSv1.0とTLSv1.1は無効にすることをお勧めします。手順については、「TLSプロトコルの設定」(8ページ)を参照してください。

TLSプロトコルの設定

デフォルトでは、NNMiは以下のプロトコルをサポートします。

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

TLSv1.2をサポートしないアプリケーションとの通信に必要でない限り、TLSv1.0とTLSv1.1は無効にすることをお勧めします。

次のファイルで、`com.hp.ov.nms.ssl.PROTOCOLS`パラメーターを使用して、使用するプロトコルを設定します。

- Windowsの場合:

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

- Linuxの場合:

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

アプリケーションフェイルオーバー

アプリケーションフェイルオーバー環境では、NNMiはNNMi管理サーバー間の通信に常にTLSv1.2を使用します。この設定は変更できません。

暗号化

このトピックでは、NNMiにおける暗号化とハッシングのデフォルトのセキュリティ設定について説明します。

- インストール時に、NNMiは2048ビット暗号化キー、SHA 256、およびRSAを使用して自己署名証明書を生成します。

  注: NNMiによって提供される自己署名証明書ではなく、CA署名の証明書を使用することをお勧めします。

- NNMiに対するローカル認証の場合、NNMiユーザーパスワードを保存するのにNNMiはソルト (Salt) 付きのSHA-256パスワードハッシュを使用します。
- NNMiデータベースに保存されているデバイスパスワードの暗号化の場合、NNMiはAES 128アルゴリズムを使用します。

詳細については、『HP Network Node Manager i Softwareデプロイメントリファレンス』の「NNMiデータの暗号化」を参照してください。

パスワード

組み込みデータベースのパスワード変更の詳細については、HP Network Node Manager i Softwareデプロイメントリファレンスの「組み込みデータベースツールのパスワードの入力」を参照してください。

ユーザー認証

ユーザーは、ローカルユーザーアカウントを使用するかまたはいくつかの外部認証コンポーネントの1つを使用してNNMiコンソールに対する認証を行うことができます。各手段には管理設定が必要です。

ローカルユーザーアカウント

ローカルユーザーアカウントは、NNMiインストールにのみ固有のものです。NNMiは、ローカルユーザーアカウントのパスワードポリシー設定をサポートしません。

注: 使用環境のセキュリティ基準で特定のパスワードポリシー (最小のパスワード長やパスワードの有効期限など) が要求される場合は、ユーザー認証に外部メカニズムを使用することをお勧めします。「外部認証」(11ページ)を参照してください。

NNMiのローカルユーザーアカウントを作成する方法については、NNMiヘルプの「ユーザーアカウントの設定」を参照してください。

外部認証

外部認証コンポーネントの管理者は、そのコンポーネントを使用するすべてのユーザーおよびアプリケーションのセキュリティ上の動作を決定します。

NNMiコンソールのセッションタイムアウト

デフォルトでは、NNMiコンソールのセッションタイムアウトは18時間です。NNMi管理者は、[ユーザーインタフェースの設定] フォーム (**[設定] > [ユーザーインタフェース] > [ユーザーインタフェースの設定]**) の **[コンソールタイムアウト]** フィールドですべてのNNMiコンソールユーザーについてこの値を変更できます。

注: セッションタイムアウトは、使用環境のポリシーに基づいて設定することをお勧めします。

クリックジャッキングからの保護

NNMiは、リンクがNNMi管理サーバーと同じオリジン (SAMEORIGIN) からの場合にリンクされたページが新しいフレームに開かれるように設定されています。この設定は変更できません。

セキュリティの強化

以下の変更のいずれかまたはすべてを適用し、NNMiのセキュリティを強化できます。

NNMi Webサーバーで使用される暗号の設定

NNMiは、NNMi Webサーバーとのセキュア通信に対して以下の暗号をサポートします。

- 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

NNMiが使用できるプロトコルのリストを変更するには、以下のファイル内の com.hp.ov.nms.ssl.CIPHERSパラメーターのコメントを解除し、このパラメーターを設定します。

- Windowsの場合:

  %NnmDataDir%\shared\<PRODUCT>\conf\props\nms-jboss.properties

- Linuxの場合:

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

このパラメーターには、1つ以上の暗号の順序付きリストが入っています。NNMi Webサーバーとの接続とユーザーのWebブラウザーとの接続を確立する際にNNMiがこのリスト内の最初の暗号を使用できない場合、NNMiは次の暗号の使用を試み、その暗号が使用できない場合にはその次を試みます。(上記のリストはデフォルトの暗号順を示しています。)

com.hp.ov.nms.ssl.CIPHERSパラメーターの値を編集することにより、NNMiが使用してはならない暗号を削除することも、NNMiが使用できる暗号を試みる順序を変更することもできます。

サポートされる暗号のリストを変更する場合は強度の順に暗号を順序付けることをお勧めします。つまり、256ビット暗号を128ビット暗号よりも上に配置することが望まれます。

注:

- com.hp.ov.nms.ssl.CIPHERSパラメーターの値は、連続した1つの行に、スペースを含まないカンマ区切りのリストとして指定する必要があります。
- 暗号リストを変更する前に暗号リストを保存してください。com.hp.ov.nms.ssl.CIPHERSリストから暗号を削除すると、NNMiが起動しなくなることがあります。
- Webブラウザーは設定された暗号の少なくとも1つをサポートしている必要があります。
- GNM環境では、1つのNNMi管理サーバーでこのファイルを修正し、修正されたファイルをGNM環境内の他のNNMi管理サーバーにコピーします。すべてのNNMi管理サーバーにファイルが配置された後、すべてのNNMi管理サーバーを起動します。

  高可用性環境では、アクティブなNNMi管理サーバーでのみこのファイルを修正します。

アプリケーションフェイルオーバー: NNMi Webサーバーで使用される暗号の設定

アプリケーションフェイルオーバー環境では、アプリケーションフェイルオーバーファイルIOポートの暗号設定で以下のファイルのcom.hp.ov.nms.cluster.ssl.CIPHERSパラメーターを使用します。

- Windowsの場合:

  %NnmInstallDir%\misc\<PRODUCT>\props\shared\nms-cluster.properties

- Linuxの場合:

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

アプリケーションフェイルオーバークラスター内の一方のNNMi管理サーバーでこのファイルを修正し、修正されたファイルをもう一方のNNMi管理サーバーにコピーします。

サポートされる暗号と設定の考慮事項は、「NNMi Webサーバーで使用される暗号の設定」(13ページ)の説明と同じです。

NNMi Webサーバーへのユーザーアクセスの制限

NNMi Webサーバーに対するトラフィックはアクセス権限のあるユーザーのみに限定することをお勧めします。このトラフィックを制限するには以下の方法を使用できます。

- NNMi管理サーバーの前面でファイアウォールを設定する。

  NNMiが使用するポートについての詳細は、『NNMiデプロイメントガイド』の「NNMiおよびNNM iSPIのデフォルトポート」を参照してください。
- 特定のネットワークインタフェース上のみNNMi管理サーバーに対するユーザーアクセスを分離する。

JMXコンソールの無効化

JMXコンソールは、トラブルシューティングのために必要になるまでは無効にすることをお勧めします。

注: NNM iSPI Performance for Trafficでは、マスターコレクターシステムと各リーフコレクターシステムでこのタスクを実行する必要があります。

NNM iSPI Performance for MetricsにはJMXコンソールがないため、このタスクを実行する必要はありません。

JMXコンソールへのアクセスを無効にするには、次のコンテンツを

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

次のファイルの`realms`ブロックに追加します。

- Windowsの場合:

  `%NnmDataDir%\nmsas\<PRODUCT>\conf\nms-auth-config.xml`
- Linuxの場合:

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

例:

```
<!-- 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>
```

続いて、適切なコマンドを実行して`nms-auth-config.xml`ファイルを再度読み取ります。

- NNMi: **`nnmsecurity.ovpl -reloadAuthConfig`**
- NNM iSPI Performance for QA:**`nmsqaauthconfigreload.ovpl -reloadAuthConfig`**
- NNM iSPI Performance for Trafficマスターコレクター: **`nmsmasterauthconfigreload.ovpl -reloadAuthConfig`**
- NNM iSPI Performance for Trafficリーフコレクター: **`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`**

トラブルシューティングのためにJMXコンソールを有効に戻すには、上記の設定をコメントアウトし、再ロードコマンドをもう一度実行します。

すべてのNNMiサービスの開始、停止、または再開

NNMi設定を変更する前にNNMiサービスを停止すると、矛盾するデータがNNMiデータベースに格納されることが防止されます。手順の中には、更新された設定を読み取るためにNNMiサービスの再開を必要とするものがあります。

ヒント: `ovstart`コマンドと`ovstop`コマンドは、以下の製品すべてに適用されます (これらの製品が環境内にインストールされている場合)。

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

NNM iSPI Performance for Trafficの詳細については、「すべてのNNM iSPI Performance for Traffic サービスの開始、停止、または再開」(20ページ)を参照してください。

使用環境に応じて次の手順を実行してください。

- 「1つのNNMi管理サーバーまたはGNM」(17ページ)
- 「アプリケーションフェイルオーバー」(18ページ)
- 「高可用性」(19ページ)

1つのNNMi管理サーバーまたはGNM

すべてのNNMiサービスを開始する

- Windowsの場合:次のいずれかを実行します。
  - Windowsの [スタート] メニューから、**[すべてのプログラム] > [HP] > [Network Node Manager] > [ovstart]** を実行します。
  - 以下のコマンドを実行します。

    ```
    %NnmInstallDir%\bin\ovstart
    ```
- Linuxの場合: 以下のコマンドを実行します。

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

すべてのNNMiサービスを停止する

- Windowsの場合:次のいずれかを実行します。
  - Windowsの [スタート] メニューから、**[すべてのプログラム] > [HP] > [Network Node Manager] > [ovstop]** を実行します。

- 以下のコマンドを実行します。

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

- Linuxの場合: 以下のコマンドを実行します。

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

すべてのNNMiサービスを再開する

- Windowsの場合:次のいずれかを実行します。
  - Windowsの [スタート] メニューから、**[すべてのプログラム] > [HP] > [Network Node Manager] > [ovstop]** を実行し、続いて **[すべてのプログラム] > [HP] > [Network Node Manager] > [ovstart]** を実行します。
  - 以下のコマンドを実行します。

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

- Linuxの場合: 以下のコマンドを実行します。

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

アプリケーションフェイルオーバー

すべてのNNMiサービスを開始する

- Windowsの場合: 以下のコマンドを実行します。

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

- Linuxの場合: 以下のコマンドを実行します。

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

すべてのNNMiサービスを停止する

- Windowsの場合: 以下のコマンドを実行します。

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

- Linuxの場合: 以下のコマンドを実行します。

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

すべてのNNMiサービスを再開する

- Windowsの場合: 以下のコマンドを実行します。

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

- Linuxの場合: 以下のコマンドを実行します。

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

高可用性

『NNMiデプロイメントリファレンス』の「高可用性設定のメンテナンス」を参照してください。

すべてのNNM iSPI Performance for Trafficサービスの開始、停止、または再開

NNM iSPI Performance for Traffic設定を変更する前にNNM iSPI Performance for Trafficサービスを停止すると、矛盾するデータがNNM iSPI Performance for Trafficデータベースに格納されることが防止されます。手順の中には、更新された設定を読み取るためにNNM iSPI Performance for Trafficサービスの再開を必要とするものがあります。使用環境に応じて次の手順を実行してください。

- 「スタンドアロンサーバー (ただし高可用性クラスター内ではない) 上のマスターコレクター」(20ページ)
- 「NNMi管理サーバー (ただし高可用性クラスター内ではない) 上のマスターコレクター」(21ページ)
- 「高可用性クラスター内のマスターコレクター」(21ページ)
- 「別のサーバーのリーフコレクター」(21ページ)
- 「NNMi管理サーバー上のリーフコレクター」(22ページ)

スタンドアロンサーバー (ただし高可用性クラスター内ではない) 上のマスターコレクター

NNM iSPI Performance for Trafficマスターコレクターを起動する

- Windowsの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

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

- Linuxの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

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

NNM iSPI Performance for Trafficマスターコレクターを停止する

- Windowsの場合: 以下のコマンドを実行します。

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

- Linuxの場合: 以下のコマンドを実行します。

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

NNM iSPI Performance for Trafficマスターコレクターを再起動する

- Windowsの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

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

- Linuxの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

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

NNMi管理サーバー (ただし高可用性クラスター内ではない) 上のマスターコレクター

NNM iSPI Performance for Trafficマスターコレクターを起動する

- Windowsの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

  ```
  %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
  ```
- Linuxの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

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

NNM iSPI Performance for Trafficマスターコレクターを停止する

- Windowsの場合: 以下のコマンドを実行します。

  ```
  %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
  ```
- Linuxの場合: 以下のコマンドを実行します。

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

NNM iSPI Performance for Trafficマスターコレクターを再起動する

- Windowsの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

  ```
  %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
  %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
  ```
- Linuxの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

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

高可用性クラスター内のマスターコレクター

トラフィックマスターサービスを停止する前に、必要なメンテナンスファイルを作成して、高可用性リソースグループのモニタリングを無効化します。『NNM iSPI Performance for Trafficデプロイメントリファレンス』の「高可用性クラスターでのNNM iSPI Performance for Trafficのデプロイメント」を参照してください。

別のサーバーのリーフコレクター

NNM iSPI Performance for Trafficリーフコレクターを起動する

- Windowsの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

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

- Linuxの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

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

NNM iSPI Performance for Trafficリーフコレクターを停止する

- Windowsの場合: 以下のコマンドを実行します。

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

- Linuxの場合: 以下のコマンドを実行します。

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

NNM iSPI Performance for Trafficリーフコレクターを再起動する

- Windowsの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

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

- Linuxの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

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

NNMi管理サーバー上のリーフコレクター

NNM iSPI Performance for Trafficリーフコレクターを起動する

- Windowsの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

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

- Linuxの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

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

NNM iSPI Performance for Trafficリーフコレクターを停止する

- Windowsの場合: 以下のコマンドを実行します。

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

- Linuxの場合: 以下のコマンドを実行します。

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

NNM iSPI Performance for Trafficリーフコレクターを再起動する

- Windowsの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

- Linuxの場合: NNMiサービスが実行されていることを確認し、その後で次のコマンドを実行します。

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

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

ドキュメントのフィードバックを送信

このドキュメントに関するご意見については、電子メールでドキュメントチームまでご連絡ください。このシステムで電子メールクライアントが設定されていれば、このリンクをクリックすることで、以下の情報が件名に記入された電子メールウィンドウが開きます。

強化ガイドに関するフィードバック (Network Node Manager i Software 10.10)

電子メールの本文にご意見、ご感想を記入の上、[送信] をクリックしてください。

電子メールクライアントが利用できない場合は、上記の情報をコピーしてWebメールクライアントの新規メッセージに貼り付け、network-management-doc-feedback@hpe.com にお送りください。

フィードバックをお寄せください