Hewlett Packard Enterprise

HPE Network Node Manager i Software

ソフトウェアバージョン: 10.20
Windows®およびLinux®のオペレーティングシステム用

強化ガイド

ドキュメントのリリース日 : 2016年 8月
ソフトウェアのリリース日 : 2016年 7月

ご注意

保証

Hewlett Packard Enterprise製品とサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。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。HPE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これらを所有、使用、または複製するには、HPEが提供する有効なライセンスが必要です。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

© Copyright 2008-2016 Hewlett Packard Enterprise Development LP

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

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

Internet Explorer、Lync、Microsoft、Windows、Windows Serverは、米国および/または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/またはその子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、https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword= を参照してください。

このサイトでは、HPパスポートのアカウントが必要です。HPパスポートのアカウントがない場合は、HPパスポートのサインインページで [**アカウントを作成してください**] ボタンをクリックしてください。

サポート

HPEソフトウェアサポートWebサイトには、次のアドレスからアクセスしてください。**https://softwaresupport.hpe.com**

このWebサイトでは、製品、サービス、およびHPEソフトウェア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。

HPEソフトウェアサポートでは、お客様にセルフソルブ機能を提供しています。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
- HPEサポートの問合せ先の検索
- 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パスポートのIDを登録するには、**https://softwaresupport.hpe.com** にアクセスし、[**HPパスポートに登録**] をクリックしてください。

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.hpe.com/web/softwaresupport/access-levels

目次

このガイドの使用 6

HTTPS通信の設定 8
- HTTPS通信の暗号プロトコルの設定 8
  - アプリケーションフェイルオーバー 9

デバイス通信の強化 10
- SNMPv3を使用するためのNNMiの設定 10
  - SNMPv1トラップまたはSNMPv2cトラップのブロック 10
  - セキュアなSNMPv3通信の設定 10
  - SNMPv3通信のFIPS認証アルゴリズムの選択 11

暗号化の強化 13

ユーザー認証 14

パスワード 15
- LDAPまたはPKIユーザー認証を使用するためのNNMiの設定 15
- デフォルトのNPSパスワードの変更 15
  - NPSデータベースのパスワードの変更 15
  - NPS BIサーバーのパスワードの変更 15
  - NPS SDKのパスワードの変更 15
- NNMi組み込みデータベースのパスワードの変更 16

クリックジャッキングからの保護 17

FIPS 140-2検証済み暗号モジュールを使用するためのNNMiの設定 18
- 前提条件 18
- NNMiの設定 19

NPSデータベースへのリモートアクセスの制限 20
- NPSコンソールの設定 21

監査 22

セキュリティの強化 23
- HTTPS専用通信の有効化 23
- NNMi Webサーバーで使用される暗号の設定 23
- 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 24
- NNMi Webサーバーへのユーザーアクセスの制限 25
- NPSのセキュリティの強化 25
  - HTTPS通信の有効化 25

すべてのNNMiサービスの開始、停止、または再開 26

すべてのNNM iSPI Performance for Trafficサービスの開始、停止、または再開 28
ドキュメントのフィードバックを送信 31

このガイドの使用

このドキュメントには、次の製品のセキュリティ向上に関する情報が記載されています。

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

このドキュメントの情報は、NNMi 10.20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」(26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」(26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HPE 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
    ```

HTTPS通信の設定

このトピックでは、NNMiにおけるHTTPS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およびHPE Network Node Manager i Software Smart Plug-ins (iSPIs)は、インストール時に生成された自己署名証明書でHTTPSをサポートします。

  注: CA署名証明書をインストールして、デフォルトの証明書と置き換えることを強くお勧めします。詳細については、『HPE Network Node Manager i Softwareデプロイメントリファレンス』の「「証明書の管理」の章」を参照してください。

- NNMi Webサーバーとの HTTPS通信におけるデフォルトの暗号プロトコルはTLSv1.2です。

HTTPS通信の暗号プロトコルの設定

NNMiはデフォルトでは、HTTPS通信に対してTLSv1.2プロトコルをサポートしています。

従来のクライアントをサポートするために以前の安全性の低いプロトコルが必要な場合を除き、NNMiではTLSv1.2のみを使用することをお勧めします。

TLSv1.2以外のプロトコルを使用するようにNNMiを設定するには、以下の手順に従います。

1. NNMi管理サーバーにログオンします。
2. テキストエディターで以下のファイルを開きます。
   - Windowsの場合:

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

   - Linuxの場合:

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

3. 使用するプロトコルのカンマ区切りリストを使用して、`com.hp.ov.nms.ssl.PROTOCOLS`プロパティを追加するか更新します。

   たとえば、TLSv1、TLSv1.1、およびTLSv1.2プロトコルを使用する場合は、以下の行が`server.properties`ファイルに存在することを確認します。

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

4. 以下のコマンドを実行してNNMiプロセスを再起動します。
   - Windowsの場合:
     i. **%nnminstalldir%\bin\ovstop -c**
     ii. **%nnminstalldir%\bin\ovstart -c**

   - Linuxの場合:
     i. **/opt/OV/bin/ovstop -c**
     ii. **/opt/OV/bin/ovstart -c**

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。

デバイス通信の強化

NNMiでは、SNMP (v1、v2c、v3) を使用して多くのデバイスと通信します。このセクションでは、すべてのSNMP通信でセキュアなSNMPv3のみを使用するようにNNMiを設定する方法を説明します。

SNMPv3を使用するためのNNMiの設定

SNMPv3では、NNMiエージェントとSNMPエージェントの間で送信されるメッセージを認証する際に、SNMPv1/SNMPv2cコミュニティ文字列ではなくユーザーベースのセキュリティモデル (USM) のユーザー名を使用する必要があるため、SNMPv3を使用した検出と通信は、より高い安全性が確保されます。管理者用のNNMiヘルプの「通信プロトコルを設定する」セクションに従って、デバイスの検出およびデバイスとの通信にSNMPv3プロトコルのみを使用するようにNNMiを設定します。

SNMPv1トラップまたはSNMPv2cトラップのブロック

SNMPv3のみを使用するようにデバイス検出を設定したにもかかわらず、一部の管理対象ノードが、引き続きNNMi管理サーバーにSNMPv1トラップまたはSNMPv2cトラップの送信を試みる場合があります。SNMPv1トラップまたはSNMPv2cトラップがNNMi管理サーバーに到達しないように、SNMPv3トラップのみを受け入れ、SNMPv1トラップおよびSNMPv2cトラップをすべてブロックするようにNNMiを設定することをお勧めします。

注: この設定手順を完了する前に、SNMPv3プロトコルを使用するネットワークを検出するようにNNMiが設定されていることを確認します。

1. NNMi管理サーバーにログオンします。
2. 以下のコマンドを実行します。

   Windowsの場合: **"%nnminstalldir%\bin\nnmtrapconfig.ovpl -setProp disallowV1V2 -persist"**

   Linuxの場合: **/opt/OV/bin/nnmtrapconfig.ovpl -setProp disallowV1V2 -persist**
3. 以下のいずれかを実行します。
   - Windowsの場合: [サービス] ウィンドウから`NNM TrapReceiver`サービスを再起動します。
   - Linuxの場合: 以下のコマンドを実行します。

     /etc/init.d/nettrap stop

     /etc/init.d/nettrap start

セキュアなSNMPv3通信の設定

SNMPv3プロトコルを使用したデバイスの検証を計画している場合は、この追加手順を実行して、セキュアなSNMPv3通信のFIPS認証モードを実装する必要があります。

1. NNMi管理サーバーにログオンします。
2. 以下のファイルをバックアップします。

- Windowsの場合：%nnmdatadir%\shared\nnm\conf\crypto\nms-snmpv3-crypto-config.xml
- Linuxの場合：/var/opt/OV/shared/nnm/conf/crypto/nms-snmpv3-crypto-config.xml

3. 以下のディレクトリに移動します。
   - Windowsの場合：%nnminstalldir%\newconfig\HPOvNmsSnmpCo
   - Linuxの場合：/opt/OV/newconfig/HPOvNmsSnmpCo
4. 以下の手順を実行して、nms-snmpv3-crypto-config-fips.xmlファイルをnms-snmpv3-crypto-config.xmlとしてシステムに保存します。
   - Windowsの場合：
     i. nms-snmpv3-crypto-config-fips.xmlファイルをテキストエディターで開きます。
     ii. ファイルの内容をコピーします。
     iii. nms-snmpv3-crypto-config.xmlファイルを新しく作成します。
     iv. コピーした内容をnms-snmpv3-crypto-config.xmlファイルに貼り付けます。
     v. nms-snmpv3-crypto-config.xmlファイルを%nnmdatadir%\shared\nnm\conf\cryptoディレクトリに保存します。
   - Linuxの場合：

     以下のコマンドを実行します。

     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

   注： 以前のバージョンのnms-snmpv3-crypto-config.xmlファイルは、この手順で上書きされます。
5. NNMiを再起動します。

SNMPv3通信のFIPS認証アルゴリズムの選択

SNMPv3プロトコルを使用してデバイスを検出するようにNNMiを設定した場合は、次のFIPS認証アルゴリズムのいずれかを使用してSNMPv3情報を検出するようにNNMiが設定されていることを確認します。

- 認証プロトコル:
  - SHA-1
- プライバシプロトコル:
  - Triple-DES
  - AES-128
  - AES-192
  - AES-256

「セキュアなSNMPv3通信の設定」(10ページ)の指示に従って弱いアルゴリズムを使用すると、NNMiによるデバイスとの通信は失敗します。

検出と通信の設定時に上記のアルゴリズムのいずれかを選択しなかった場合は、次の手順を実行します。

1. 管理者としてNNMiコンソールにログオンします。
2. [設定] ワークスペースから [通信の設定] フォームを起動します。

   注: 管理者用のNNMiヘルプの「通信プロトコルを設定する」を参照してください。

3. [通信の設定] フォームから [SNMPv3設定] フォームを起動します。
4. 認証プロトコルをSHA-1に設定します。
5. プライバシプロトコルをTriple-DES、AES-128、AES-192、またはAES-256に設定します。
6. 設定を保存します。

または、`nnmcommunication.ovpl`コマンドを使用して、これらのプロトコルを選択することもできます。`-authProtocol`および`-privProtocol`パラメーターを使用すると、認証プロトコルおよびプライバシプロトコルを選択できます。詳細については、`nnmcommunication.ovpl`のリファレンスページ (NNMiのヘルプメニューから[**ヘルプ**] > [**NNMiドキュメントライブラリ**] > [**リファレンスページ**] をクリック) またはLinuxのマニュアルページを参照してください。

暗号化の強化

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。

- NNMi 10.20の新規インストールでは、暗号化とキー管理に連邦情報処理標準 (FIPS) 140-2検証済み暗号モジュール (RSA BSAFE) を使用します。
- 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、『HPE 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。

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」(14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。

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、HPE 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。

LDAPまたはPKIユーザー認証を使用するためのNNMiの設定

NNMiを、Lightweight Directory Access Protocol (LDAP) を使用してディレクトリサービスに統合するか、公開キーインフラストラクチャー (PKI) ユーザー認証を使用するように設定することをお勧めします。

『NNMiデプロイメントリファレンス』の次のセクションのいずれかの手順に従います。

- NNMiとLDAPによるディレクトリサービスの統合
- 公開キーインフラストラクチャーユーザー認証をサポートするためのNNMiの設定

デフォルトのNPSパスワードの変更

NNM iSPI Performance for Metricsインストーラーは、パスワードがあらかじめ設定されている以下の3つのアプリケーションとともにNPSをインストールします。

- NPSデータベース
- NPS BIサーバー
- NPSソフトウェア開発キット (SDK)

モニタリング環境のセキュリティを強化するには、このあらかじめ設定された3つのパスワードをすべて変更します。

NPSデータベースのパスワードの変更

NPSデータベースのパスワードを変更するには、以下のコマンドを実行します。

changeDBpwd.ovpl <password>

この場合の<password>は、任意のパスワードです。

NPS BIサーバーのパスワードの変更

NPS BIサーバーのパスワードを変更するには、以下のコマンドを実行します。

changeBIpwd.ovpl <password>

この場合の<password>は、任意のパスワードです。

NPS SDKのパスワードの変更

NPS SDKのパスワードを変更するには、以下のコマンドを実行します。

changesdkUserPwd.ovpl -u<username>**-p**<password>

この場合、<username>はユーザー名で、<password>は任意のパスワードです。

> **注:** `changesdkUserPwd.ovpl`コマンドでは、必ずユーザー名を指定する必要があります。NPS SDKのパスワードのみを変更する場合は、コマンドで古いユーザー名を指定します。

NNMi組み込みデータベースのパスワードの変更

NNMiによってデフォルトで設定されているパスワードは、`nnmchangeembdbpw.ovpl`スクリプトを使用して変更できます。

詳細については、『NNMi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」セクションを参照してください。

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。

FIPS 140-2検証済み暗号モジュールを使用するためのNNMiの設定

このセクションでは、連邦情報処理標準 (FIPS) 140-2検証済み暗号モジュールを使用するようにNNMiを設定する方法について説明します。FIPSガイドラインでは、アメリカ国立標準技術研究所 (NIST) が定義した暗号モジュールのセキュリティ要件の基準を提供します。このセクションでは、FIPS要件に準拠する暗号モジュールを使用するようにNNMiを設定する方法について説明します。

注: NNMi Premiumのみ (つまりNNMi、NNM iSPI Performance for Metrics、NNM iSPI Performance for QA) をFIPSに準拠するように設定できます。

FIPS 140-2標準の要件を満たすには、NPSとNNMiが同じサーバーにインストールされている必要があります。

NNMi 10.20の新規インストールでは、暗号化とキー管理にFIPS 140-2検証済み暗号モジュール (RSA BSAFE) を使用します。

アップグレードされたNNMi環境では、ほとんどのパスワード暗号化およびネットワーク通信の手順に、FIPS認証の暗号およびアルゴリズムが自動的に使用されます。ただし、アップグレードされた環境に、FIPSガイドラインを満たしていない従来の暗号およびアルゴリズムが存在する場合があります。

最高レベルのFIPS 140-2検証済み暗号を実現するには、次のことを行います。

- NNMi 10.20の新規インストールを使用します。
- デフォルトでは、NNMiは自己署名証明書をインストールします。HPEでは、自己署名証明書ではなく、CA署名証明書を使用することをお勧めします。CA署名証明書を使用する場合の詳細については、『NNMiデプロイメントリファレンス』の「詳細設定」セクションを参照してください。
- FIPSで認証されていない一部の弱いSNMPv3暗号を無効にするための設定手順を実行します。
- NNMi Premiumのみを使用します。
- NNMiとNPSを同じシステムにインストールします。

注: 上記の要件を満たしている場合でも、NNMiとNPSの次のコンポーネントではFIPS 140-2検証済み暗号が使用されません。

- NPSコンソール
- [パフォーマンスのトラブルシューティング] ウィンドウ
- NNMiコンソールの [分析] ペインの [パフォーマンス] タブ

このセクションでは、最高レベルのFIPS 140-2検証済み暗号を使用するようにNNMiを設定する手順について説明します。

前提条件

通信のHTTPモードが無効になっていることを確認します。詳細については、「HTTPS専用通信の有効化」(23ページ)を参照してください。

NNMiの設定

次の設定タスクを実行します。

1. タスク1: アップグレード後の手順: パスワードの暗号化

   この手順は、旧バージョンのNNMiからNNMi10.20にアップグレードした場合にのみ該当します。

   NNMiを10.20にアップグレードする前にnnmsetcmduserpw.ovplコマンドを使用しなかった場合は、この手順を省略してください。

   > **ヒント:** 詳細については、nnmsetcmduserpw.ovplコマンドのリファレンスページを参照してください。

   コマンドラインツールをシームレスに実行するために、nnmsetcmduserpw.ovplコマンドを使用して有効なNNMiユーザー名属性値とNNMiパスワード属性値を設定した場合は、次の手順を実行する必要があります。

   a. ルートまたは管理者としてNNMi管理サーバーにログオンします。
   b. nnmsetcmduserpw.ovplコマンドを再度実行して、NNMiをバージョン10.20にアップグレードする前に設定したすべてのNNMi資格証明を設定します。

      > **ヒント:** NNMiを10.20にアップグレードする前にnnmsetcmduserpw.ovplコマンドを使用してパスワードが暗号化されたすべてのユーザーを調べるには、nms-users.propertiesファイルを見つけて、そのファイルの内容を確認します。サーバーにはnms-users.propertiesファイルの複数のコピーが存在する場合があります。

2. 「セキュアなSNMPv3通信の設定」(10ページ)
3. 「SNMPv3通信のFIPS認証アルゴリズムの選択」(11ページ)

NPSデータベースへのリモートアクセスの制限

注: NNMiとNPSが同じシステムにインストールされていない場合は、このセクションの指示に従わないでください。

NPSでは組み込みデータベースを使用して、レポート作成のためにNNMiおよびiSPIsによって収集されたパフォーマンスデータを格納します。NPSでは、コンテンツストアと呼ばれる別のデータベースを使用して、拡張パックおよびレポートのすべての詳細情報を格納、保持します。これにより、リモートシステムがこの2つのデータベースにアクセスするのを防ぐことができます。

NPSデータベースでは、次のポートが使用されます。

- 9301
- 9303
- 9306

この手順により、これらのポート経由の通信をブロックするように、NNMi管理サーバーで実行されているファイアウォールを設定できます。

組み込みNPSデータストアへのリモートアクセスを制限するには、以下の手順を実行します。

Windowsの場合:

Windowsファイアウォールプログラムを使用して、9303および9306ポート経由のリモート通信をブロックします。詳細については、Microsoft Windowsのドキュメントを参照してください。

Linuxの場合:

1. NNMi管理サーバーにrootとしてログオンします。
2. 以下のコマンドを実行します。
   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**

コンテンツストアへのリモートアクセスを制限するには、以下の手順を実行します。

1. ルートまたは管理者としてNNMi管理サーバーにログオンします。
2. テキストエディターで以下のファイルを開きます。
   - Windowsの場合: `%nnminstalldir%\nonOV\sybasease\interface`
   - Linuxの場合: `/opt/OV/nonOV/sybasease/interfaces`
   - 以下の行に、外部のIPアドレスまたはホスト名が含まれていないことを確認します。

```
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
```

NPSコンソールの設定

注： NNMiとNPSが同じシステムにインストールされていない場合は、このセクションの指示に従わないでください。

NPSデータベースへのリモートアクセスを無効化することに加え、以下の手順を実行することで、ユーザーがリモートシステムからBIサーバーのポータルを起動できないようにNPSコンソールを設定できます。

1. NNMi管理サーバーにログオンします。
2. テキストエディターで以下のファイルを開きます。
   a. Windowsの場合：`%ovdatadir%\NNMPerformanceSPI/rconfig/NNMPerformanceSPI.cfg`
   b. Linuxの場合：`/var/opt/OV/NNMPerformanceSPI/rconfig/NNMPerformanceSPI.cfg`
3. ユーザーがリモートシステムからBIサーバーのポータルを起動できないようにするには、`CC_DISABLE_REMOTE_COGNOS_ADMINISTRATION`を`true`に設定します。
4. ファイルを保存します。
5. 以下のコマンドを実行して、BIサーバーを再起動します。
   a. **stopBI.ovpl**
   b. **startBI.ovpl**

   これで、NPSコンソールの [BIサーバー] ワークスペースのメニュー項目を使用できなくなりました。

   注： NPSシステムにログオンし、ローカルブラウザーでNPSコンソールを起動すれば、引き続き [BIサーバー] ワークスペースを使用できます。

監査

デフォルトでは、NNMi、NPS、およびNNM iSPI Performance for QAに対するユーザーアクションの監査は有効になっています。

NNMiの監査ログファイルの詳細については、NNMiオンラインヘルプを参照してください。

NPSおよびNNM iSPI Performance for Metricsの監査ログファイルの詳細については、NNM iSPI Performance for Metricsオンラインヘルプを参照してください。

NNM iSPI Performance for QAの監査ログファイルの詳細については、NNM iSPI Performance for QAオンラインヘルプを参照してください。

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。

- 「HTTPS専用通信の有効化」(23ページ)
- 「NNMi Webサーバーで使用される暗号の設定」(23ページ)
- 「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」(24ページ)
- 「NNMi Webサーバーへのユーザーアクセスの制限」(25ページ)
- 「NPSのセキュリティの強化」(25ページ)

HTTPS専用通信の有効化

NNMiのHTTPS専用通信の有効化

NNMiをインストールしてHTTPS通信を使用するように設定した後でも、通信のHTTPモードを引き続き使用できます。HTTPを経由したNNMiへのリモートアクセスを制限できるようにするには、『NNMiデプロイメントリファレンス』の「リモートアクセスに暗号化を必須とするためのNNMiの設定」セクションの指示に従って、NNMiの通信のHTTPモードを完全に無効化します。

> **注:** グローバルネットワーク管理環境では、各リージョナルマネージャーおよびグローバルマネージャーでこのタスクを実行してください。

NPSのHTTPS専用通信の有効化

HTTPSのみを使用するようにNPSが構成されていることを確認します。「HTTPS通信の有効化」(25ページ)を参照してください。

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、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」(23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。

NPSのセキュリティの強化

このセクションでは、NPSがインストールされ設定されている環境のセキュリティを強化するために必要な手順について説明します。

HTTPS通信の有効化

NPSがインストールされ、HTTPSプロトコルのみを使用するように設定されていることを確認します。
HTTP通信からHTTPS通信に切り替えるには、以下の手順を実行します。

1. NPSシステムにrootまたは管理者としてログオンします。
2. 以下のコマンドを実行します。

   configureWebAccess.ovpl -ssl

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 QA

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」(28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」(26ページ)
- 「アプリケーションフェイルオーバー」(27ページ)
- 「高可用性」(27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」(28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」(28ページ)
- 「高可用性クラスター内のマスターコレクター」(29ページ)
- 「別のサーバーのリーフコレクター」(29ページ)
- 「NNMi管理サーバー上のリーフコレクター」(30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 10.20)

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