Hewlett Packard Enterprise

HPE Network Node Manager i Software

ソフトウェアバージョン: NNMi 10.20

HPE Network Node Manager i Software—HPE Network Automation統合ガイド

ドキュメントのリリース日 : 2016年7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。

国防省連邦調達規則補足 (DOD FAR Supplement) に従って提供されるプログラムは、「商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同プログラムの使用、複製および開示は、該当するOracleのライセンス契約に規定された制約を受けるものとします。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の商標です。

Appleは、米国および他の国々で登録された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。

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

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

HPE NNMi–HPE NA統合

HPE Network Node Manager i Software (NNMi) は、SNMPやICMPなどの一般的なネットワークプロトコルを使用して高度なネットワークの障害および可用性をモニタリングする機能を提供し、組織全体でネットワークの稼働状態を維持するのに役立ちます。NNMiは、自動的かつ継続的にネットワークのノード (スイッチやルーターなど) を検出し、ネットワークトポロジ (レイヤー2および3) を最新の状態で表示できます。

NNMiは、トポロジベースの根本原因分析 (RCA) 機能を使用することにより、ネットワークの状態を正確に把握してネットワークの問題を特定します。RCA、高度な相関機能、および例外別の管理インシデント管理モデルと連携することにより、刻々と変化するネットワーク環境のための動的障害管理ソリューションとして機能します。

またNNMiは、使用率とインタフェースエラーなどのインタフェースのパフォーマンスメトリックスとともに、CPUやメモリの使用率などのデバイスのヘルスインジケータを監視します。リアルタイムのパフォーマンスインジケータは、ライブパフォーマンスグラフにより、1秒間隔の細分度で監視することができます。

Network Automationソフトウェア (NA) は、エンタープライズクラスのネットワークデバイス変更および設定管理ツールです。ポリシーベースの変更管理モデルによって標準へのコンプライアンス状態を維持しつつ、デバイスの設定変更時における人的誤りを解消します。NAは、NA telnetプロキシを介して行われたコマンドライン変更のキーストロークログを含め、すべてのデバイス変更の完全な監査証跡を保持します。

NAは、主要なベンダーが提供するネットワークデバイスモデルとオペレーティングシステムの数千におよぶ組み合わせをサポートしています。NAは、設定アーカイブと配備を使用してMTTRを最小限に短縮し、次の情報を追跡します。

- ネットワークデバイスに加えられた変更。
- 各変更の実行者。
- 現在のデバイスの設定。
- 組織的な標準に対するデバイスの設定のコンプライアンス

> **注:** ポリシーコンプライアンス関連の機能には、NA Ultimateライセンスが必要です。

NNMiやNAのご購入については、HPE営業担当者にお問い合わせください。

この章では、HPE NNMi–HPE NA統合およびサポートされる統合配備アーキテクチャーについて説明します。内容は以下のとおりです。

- 「統合の概要」(7ページ)
- 「統合アーキテクチャー」(10ページ)

統合の概要

HPE NNMi–HPE NA統合は、NA設定変更の検出機能とNNMiネットワーク監視機能を合わせ、障害が発生した場合にユーザーにより多くの情報を提供します。

統合によって、以下の機能が提供されます。

- 所有コストを下げて、プロビジョニング済みデバイスの管理範囲を適切にするため、NNMiとNAトポロジを同期する。
- 特定のNNMiインシデントが発生したとき、NAデバイス診断を自動的に実行する。

- アクティブな設定ポリシーを含む、同期ノードのNAノード設定情報およびコンプライアンス情報を、NNMi分析ペインに表示する。

  注: コンプライアンス情報には、NA Ultimateライセンスが必要です。

- 同期ノードのインタフェース用のNNMi分析ペインのNAインタフェース設定情報を表示する。
- NAがデバイス設定更新を適用しているときにデバイスがサービス停止中になっている間、NNMiで不要なアラームを防止する。
- 管理対象デバイスにアクセスするための情報でNNMi設定を更新する。

また、既存のNNMiコンソールを使用せずに、NAコンソールを起動して、NA管理デバイスの情報や設定変更イベントの情報を表示することができます。NAコンソールでは、ユーザーが必要な資格情報を持っている場合にNA機能を実行できます。

HPE NNMi–HPE NA統合では、NNMiビューのコンテキストでNAコンソールへの接続を開いたり、NAで管理されるデバイスの設定情報を表示したりするためのメニュー項目がNNMiコンソールに追加されます。これらのツールを使用して以下を実行できます。

- ベンダー、モデル、モジュール、オペレーティングシステムのバージョン、最近の診断結果など、デバイスの詳細情報を表示する
- デバイスの設定変更と設定履歴を表示する
- 設定 (通常、最も最近、または最後の以前の設定) を比較し、変更内容、変更理由、および変更適用者を表示する
- デバイスのコンプライアンス情報を表示する

  注: コンプライアンス情報には、NA Ultimateライセンスが必要です。

- NNMiノードからNA診断とコマンドスクリプトを実行する
- 不整合な速度設定または二重設定の接続を検出する

注: これらの機能は、NAで設定されていないネットワークデバイスまたは変更の検出が無効にされているNAデバイスでは利用できません。

注: HPE NNMi–HPE NA統合では、管理アドレスとしてIPv6アドレスを使用するデバイス、またはSNMP管理アドレス設定がIPv6に設定されているデュアルスタックデバイスはサポートされていません。

注: HPE NNMi–HPE NA統合は、重複するIPアドレスを区別できません。そのため、統合は重複アドレスドメイン (OAD) 環境ではサポートされていません。

値

HPE NNMi–HPE NA統合では、すでにNNMiとNAを実行している環境で、以下の機能や利点が提供されます。

- アラーム統合 - HPE NNMi–HPE NA統合は、NNMiコンソールにNA設定変更情報を示し、設定変更がネットワークの障害によるものであるかどうかを迅速に識別できるようにします。NNMiコンソールからNA機能に

すばやくアクセスし、特定の設定変更やデバイス情報の表示、変更適用者の識別、ネットワーク操作を復元するための以前の設定へのロールバックを行えます。多くのネットワーク使用停止は、デバイスの設定エラーに由来するものであるため、この機能によって問題の特定とネットワークダウンタイムの解決における対応時間が改善されます。

- コンテンツ統合 — HPE NNMi–HPE NA統合は、同期ノード用のNNMiコンソールの分析ペインにタブを追加します。これらのタブには、現在のデバイス設定やインタフェース設定、デバイス設定の履歴、およびNA設定ポリシーに対するコンプライアンスの現在のステータスが表示されます。NNMiコンソール内から、現在のビューのコンテキストでNAコンソールにすばやくアクセスし、特定の問題の調査を続行できます。

  注: コンプライアンス情報には、NA Ultimateライセンスが必要です。

- 操作の効率性 - ネットワークオペレーターは、1つの画面で2つのデータソースの情報を監視し、調査することができます。

統合製品

このドキュメントの情報は、以下の製品に当てはまります。

- NNMi
- NA

各製品は、同じまたは異なるレベルでライセンスを取得できます。ライセンスレベルにより、各製品で利用可能な機能が異なります。詳細については、HPE営業担当者にお問い合わせください。

ヒント: サポートされるバージョンのリストについては、NNMiシステムとデバイス対応マトリックスまたはNA対応マトリックスを参照してください。

統合設定の詳細

サポートされる統合アーキテクチャーの詳細については、「統合アーキテクチャー」(10ページ)を参照してください。

NNMiおよびNAは、同一のコンピューターまたは異なるコンピューターにインストールできます。

ヒント: NAおよびNNMiは、各専用サーバーで実行することをお勧めします。

注意: NNMiおよびNAを同一のコンピューター上で正しく実行するには、NAをインストールする前にNNMiをインストールする必要があります。NNMiをインストールする前にNAをインストールしている場合、NNMiのインストール時にNAとのポートの競合が報告され、インストールは完了しません。

HPE NNMi–HPE NA統合は、オペレーティングシステムに依存しません。

サポートされているハードウェアプラットフォームおよびオペレーティングシステムの最新情報については、両方の製品の対応マトリックスを参照してください。

ドキュメント

このドキュメントでは、HPE NNMi–HPE NA統合の設定方法と使用方法について説明します。

統合アーキテクチャー

HPE NNMi–HPE NA統合は、以下のいずれかの統合アーキテクチャーに配備できます。

- **1つのNNMi管理サーバーから1つのNAコア**

  スタンドアロンのNAコアまたは水平スケーラビリティを持つ環境に参加するNAコアに接続されている、1つのスタンドアロンNNMi管理サーバー。「図1 配備アーキテクチャーの例:1つのNNMi管理サーバーから1つのNAコア」を参照してください。

- **NNMiグローバルネットワーク管理から複数スタンドアロンNAコア**

  別のスタンドアロンNAコアに統合されているグローバルネットワーク管理環境内の各NNMiリージョナル管理サーバー。「図2 配備アーキテクチャーの例:NNMiグローバルネットワーク管理から複数スタンドアロンNAコア」を参照してください。

- **NNMiグローバルネットワーク管理からスタンドアロンNAコアまたはNA水平スケーラビリティ**

  水平スケーラビリティを持つ環境で実行されているスタンドアロンNAコアまたは1つ以上のNAコアと統合されたグローバルネットワーク管理環境のNNMi。一部またはすべてのNNMiリージョナルサーバー(必要に応じてNNMiグローバルサーバー)は、いずれかのNAコアに接続できます。例:

  - すべてのNNMi管理サーバーを1つのNAコアに接続できます。この場合、すべてのNAコンソールページが、そのNAコアで実行されているNNMiから起動されます。このNAコアは、ユーザー要求への応答専用としてユーザー相互作用のために予約することを検討してください。詳細については、『NA Horizontal Scalability Guide』を参照してください。

  - 各NNMi管理サーバーを別のNAコアに接続できます。

  「図3 配備アーキテクチャーの例:NNMiグローバルネットワーク管理からNA水平スケーラビリティ」を参照してください。

  このアーキテクチャーについては、以下の内容に注意してください。

  - NAは、各統合NNMi管理サーバーからインベントリを受信します。完全なインベントリ同期を行うには、各NNMiリージョナルマネージャーをNAコアと統合します。NNMiグローバルマネージャーがノードをローカルで管理する場合、NNMiグローバルマネージャーもNAコアと統合します。

  - NNMiグローバルマネージャーがローカルで管理していないノードの場合は、NNMiグローバルマネージャーをNAコアと統合すると、分析ペインのNAデータおよびNNMiコンソールからNAコンソールページを起動する機能が提供されます。

  - インベントリ同期はNNMiからNAにのみ実行されます。NAが、NNMi管理サーバーのインベントリに表示されないデバイスを管理している場合、これらのデバイスをNNMiインベントリに手動で追加することを検討してください。

  - 各NNMi管理サーバーは1つのNAコアのみに接続されているため([**HPE NNMi–HPE NAの統合設定**]フォームの指定に従って)、各NNMi管理サーバーは1つの統合NAコアのみに対して通信を開始します。NNMiからNAへの通信の例を以下に示します。
    - NNMiインシデントに応じたNA診断の開始
    - NAコンソールページの表示

  - すべてのNAコアが単一のNAデータベースに接続されているため、各NAコアは任意の統合NNMi管理サーバーと通信を開始できます。NNMi管理サーバーはNAコアの開始に応答できます。NAからNNMiへの通信の例を以下に示します。

- SNMPトラップの送信
- デバイスのSNMPコミュニティ文字列の更新

NNMiマルチテナント環境

アーキテクチャーに関係なく、NNMiがマルチテナント環境で実行されているときは以下の点に注意してください。

- NNMiマルチテナント環境では、インベントリ同期はNNMiからNAにのみ実行されます。
- HPE NNMi–HPE NA統合は、重複するIPアドレスを区別できません。この理由から、NNMi管理サーバーから接続されたNNMiコアへ同期されるすべてのノードが、一意のIPアドレスを持つ必要があります。

「表1　統合の機能」(11ページ)は、HPE NNMi–HPE NA統合の使用可能な機能をリストし、サポートされる統合アーキテクチャーに該当する特別な考慮事項を説明します。

表1　統合の機能

統合の機能	開始サーバー	メモ	関連項目
NNMiインベントリをNAインベントリに同期する	NNMi	• NNMiグローバルマネージャーでは、ローカルで管理されるノードのみを同期します。	「NNMiとNA間のインベントリ同期」(27ページ)
NAインベントリをNNMiインベントリに同期する	NA	• NNMiグローバルネットワーク管理からNA水平スケーラビリティアーキテクチャーでは使用できません。 • NNMiマルチテナント環境では使用できません。	
NNMiのノードを削除してNAでデバイスを管理対象外にする	NNMi	• NNMi管理サーバーがそのノードを管理していないとき。	
NAでデバイスを削除してNNMiのノードを削除する	NA	• ノードを管理するすべてのNNMi管理サーバーで。	
NNMiコンソールからNAコンソールページを起動する	NNMi	• すべての統合NNMi管理サーバーで使用可能です。 • 統合NAコアでNAコンソールページを開きます。	「NNMiコンソールからのNAコンソールのページの起動」(30ページ)
NA診断をNNMiからトリガーする	NNMi	• 統合NAコアで診断を実行します。	「NNMiからのNA診断のトリガー」(31ページ)
不整合な状態のレイヤー2接続を特定する	NNMi	• NAインベントリに、レイヤー2接続を形成する両方のインタフェース用のMACアドレスが含まれる必要があります。	「不整合な状態のレイヤー2接続の特定」
NNMi分析ペインにNAデータを表示する(権限あり)	NNMi	• すべての統合NNMi管理サーバーで使用可能です。	「NNMi分析ペインに表示されるNA情報」(33ページ)
NAコンソールからNNMiコンソールページを起動する	NA	• 水平スケーラビリティを持つ環境内のすべてのNAコアで	「NAコンソールからのNNMiコンソールの

表1　統合の機能 (続き)

統合の機能	開始サーバー	メモ	関連項目
		使用可能です。 • リンクに関連付けられたNNMi管理サーバーのNNMiコンソールページを開きます。	ページの起動」(37ページ)
NAデバイスイベントの通知をNNMiに送信する	NA	• NAは、ノードをローカルで管理する各NNMi管理サーバーと通信します。 • NNMiリージョナル管理サーバーが管理するノードの場合、この機能はNNMiグローバル管理サーバーでは使用できません。	「NNMiへのSNMPトラップの送信」(37ページ)
特定のNAタスクの後にNNMiノード設定のポーリングをトリガーする	NA		「NAからのNNMiノード設定ポーリングのトリガー」(38ページ)
デバイス設定中のネットワーク管理を無効にする	NA		「デバイス設定中のネットワーク管理の無効化」(39ページ)
デバイスコミュニティ文字列の変更を伝達する	NA		「NAへのデバイスコミュニティ文字列の変更の伝達」(40ページ)
NNMiからNAにSSL接続を使用する	NNMi	• すべての統合NNMi管理サーバーとすべてのNAコアの間で証明書を交換します。 • 水平スケーラビリティを持つ環境内のNAでは、統合の設定内容に関係なく、すべてのNAコアでNNMi証明書をインストールします。	「NNMiとNA間のSSL通信の設定」(19ページ)
NAからNNMiにSSL接続を使用する	NA		
NNMiからNAにシングルサインオンする	NNMi	• すべてのNNMi管理サーバーとすべてのNAコアで同じ初期化ストリングを使用します。 • 水平スケーラビリティを持つ環境内のNAでは、統合の設定内容に関係なく、すべてのNAコアでシングルサインオンを設定します。	「NNMiとNA間のシングルサインオンの設定」(23ページ)
NAからNNMiにシングルサインオンする	NA		

図1　配備アーキテクチャーの例:1つのNNMi管理サーバーから1つのNAコア

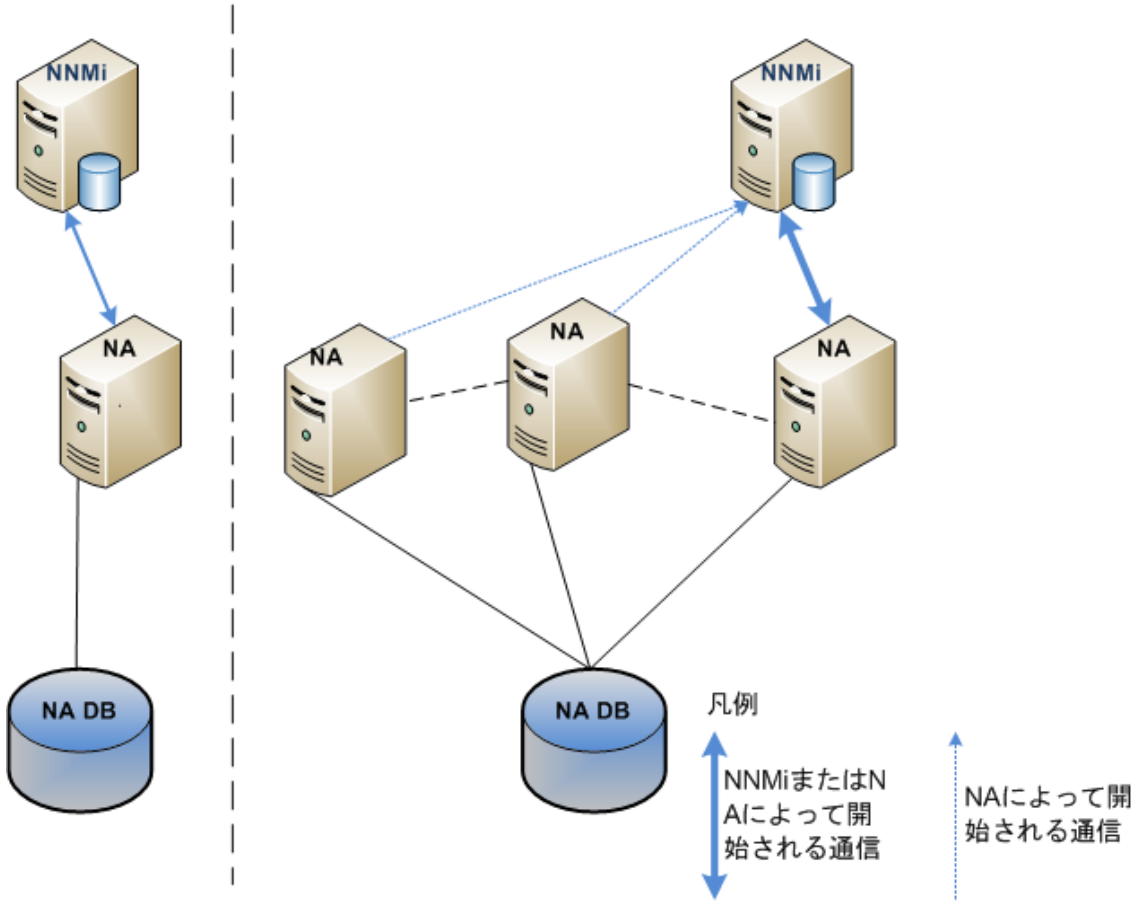


図2　配備アーキテクチャーの例:NNMiグローバルネットワーク管理から複数スタンドアロンNAコア

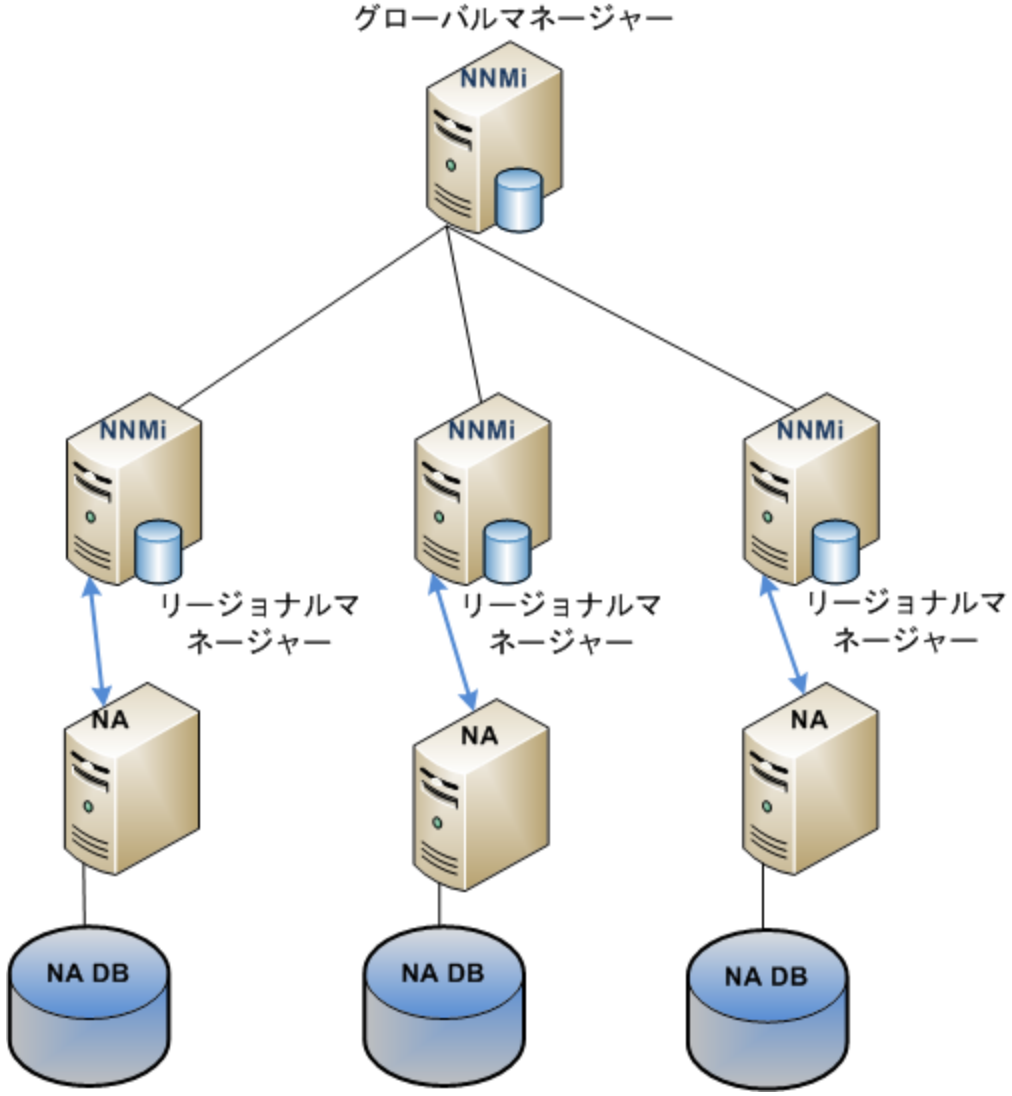
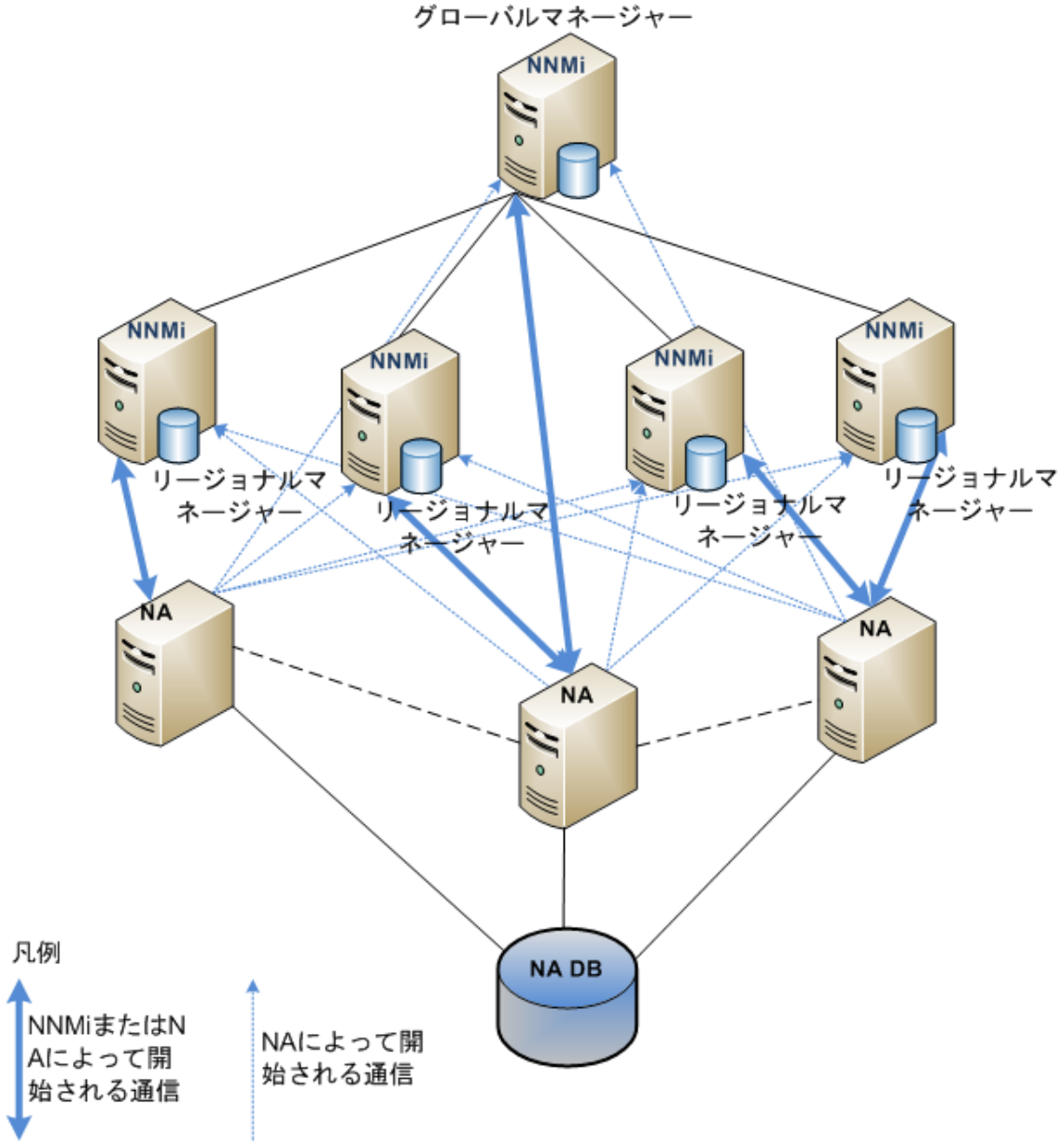


図3　配備アーキテクチャーの例:NNMiグローバルネットワーク管理からNA水平スケーラビリティ



HPE NNMi–HPE NA統合の有効化

HPE NNMi–HPE NA統合を有効にすると、NNMiとNA間のインベントリ同期が開始されます。統合により、NNMiインベントリがNAに常に同期されます。NAと統合されるNNMi管理サーバーが1つのみの場合、統合によりNAインベントリをNNMiに同期することもできます。

このセクションでは、以下の手順について説明します。

準備

各NNMi管理サーバーに対して、NAに同期するノードを決定します。あるNNMi管理サーバーのNNMiインベントリを完全には同期しない場合、NAインベントリと同期するノードを含むノードグループを1つ作成します。

統合により、NNMiセキュリティグループをNAパーティションに同期できます。この機能を有効にする前に、以下の手順をすべて実行します。

- NNMi管理者およびNA管理者と連携して、ユーザーセキュリティ計画を準備し、NNMiセキュリティグループからNAパーティションへのマッピングの有効化によるユーザーセキュリティへの影響を評価します。
- 各NNMiノードが正しいセキュリティグループ内にあることを確認してください。
- NAで、NNMiセキュリティグループにマッピングされるNAパーティションと、そのパーティションを表示するNAユーザーを設定します。
- NNMiマルチテナント環境では、各NNMiノードが正しいテナントに割り当てられていることを確認してください。

新規統合設定

HPE NNMi–HPE NA統合を有効にするには、以下の手順を実行します。

1. 「準備」(16ページ)で説明されているプロセスを実行します。
2. オプション。NNMi WebサービスまたはNA WebサービスとのSSL通信を使用するには、「NNMiとNA間のSSL通信の設定」(19ページ)の説明に従って、NNMiサーバーとNAサーバーの間で証明書を交換します。
3. NNMiインベントリでノードのNAデバイスのパスワードルールを作成します。NAコンソールで以下の手順を実行します。
   a. [**デバイスのパスワードルール**] ページを開きます (**[デバイス] > [デバイスツール] > [デバイスのパスワードルール]**)。
   b. デバイスのパスワードルールを1つ以上作成し、NNMiインベントリのノードと通信する方法を指定します。
4. NAインベントリのデバイス数をメモします。
5. NNMiコンソールで、NNMiからNAへの接続を以下のように設定します。

a. [**HPE NNMi–HPE NAの統合設定**] フォームを開きます (**[統合モジュールの設定] > [HPE NA]**)。
b. [**統合の有効化**] チェックボックスをオンにし、フォームの残りのフィールドに入力できるようにします。
c. オプション。[**NNMi SSL**] か [**NA SSL**] またはその両方を選択します。これらのチェックボックスのいずれかをオンにする前に、「オプション。NNMi WebサービスまたはNA WebサービスとのSSL通信を使用するには、「NNMiとNA間のSSL通信の設定」(19ページ)の説明に従って、NNMiサーバーとNAサーバーの間で証明書を交換します。」(16ページ)で証明書を交換したことを確認します。
d. このNNMi管理サーバーへの接続情報を入力します。これらのフィールドの詳細については、「NNMi管理サーバー接続」(65ページ)を参照してください。
e. NAコアへの接続情報を入力します。これらのフィールドの詳細については、「NAコアサーバー接続」(65ページ)を参照してください。
f. 残りのフィールドに値を入力します。
   - NNMiマルチテナント環境では、[**トポロジフィルターノードグループ**] フィールドをクリアし、[**NNMiセキュリティグループをNAパーティションにマップします**] チェックボックスをオンにします。
   - ほかの環境では、ニーズに合わせてこれらのフィールドを設定します。

   これらのフィールドの詳細については、「統合動作」(66ページ)を参照してください。
g. フォームの下部にある [**送信**] をクリックします。

   新しいウィンドウにステータスメッセージが表示されます。NAコアサーバーへの接続に問題があることを示すメッセージが表示されたら、[**戻る**] をクリックして、エラーメッセージのテキストを参考にNAコアサーバーに接続するための値を調整してください。

6. NNMiコンソールの [**アクション**] メニューでNAメニュー項目を使用できない場合、NNMiコンソールからサインアウトして、もう一度サインインしてください。
7. オプション。初期のインベントリの同期処理が完了するまで待ちます。

   NNMiインベントリのノード数をNAインベントリのデバイス数と比較します。NAインベントリのデバイス数は、統合前のNAインベントリに存在しなかったNNMiインベントリの (またはNNMiトポロジフィルターノードグループの) ノード数に相関して増加します。

   初期のインベントリからNAコアへの同期処理が完了するまで待つことで、同期がNAのパフォーマンスに影響を与えないようにできます。
8. NAと統合するNNMi管理サーバーが増えるたびに、「NAインベントリのデバイス数をメモします。」(16ページ)から「オプション。初期のインベントリの同期処理が完了するまで待ちます。」(17ページ)までを繰り返します。
9. NNMiコアアーキテクチャーに対する1つのNNMi管理サーバーと、複数のスタンドアロンNNMiコアアーキテクチャーに対するNNMiグローバルネットワーク管理に対しては省略可能。管理環境にNNMiマルチテナントが含まれていない場合、以下のようにNNMiデバイスインベントリからNNMiインベントリへの同期を有効にします。
   a. NNMiコンソールで、[**自動検出ルール**] タブに [**検出の設定**] フォームを開きます (**[設定] > [検出] > [検出の設定]**)。
   b. 自動検出ルールを1つ以上作成し、NNMiインベントリのデバイスと通信する方法を指定します。

      注意: この時点でNNMiインベントリのデバイスがNNMi自動検出ルールに含まれていない場合、統合ではそのデバイスはNNMiインベントリに同期されません。

   c. NAコンソールで、[**ルールステータス**] を「**アクティブ**」に設定することで、[デバイス追加のNA/NNMiトポロジ同期] イベントルールを有効にします。詳細については、「NAイベントルールの有効化」(42ページ)を参照してください。

d. 統合を再度有効化します。
   - NNMiコンソールで、[**HPE NNMi–HPE NAの統合設定**] フォームを開きます ([**統合モジュールの設定**] > [**HPE NA**])。
   - [**統合の有効化**] チェックボックスをオフにして、フォームの下部にある [**送信**] をクリックします。
   - [**統合の有効化**] チェックボックスをオンにして、フォームの下部にある [**送信**] をクリックします。

10. オプション。NAコンソールにおいて、統合によって提供されるNA機能のデフォルト設定を以下のように変更します。
    a. [**管理設定 - NA/NNMi統合**] ページを開きます ([**管理者**] > [**管理設定**] > [**NA/NNMi統合**])。
    b. 以下いずれかのフィールドで、選択項目を変更します。
       - **デバイスをサービス停止中にするタスク**
       - **デバイスタスクが失敗した場合**
       - **デバイス準拠確認が失敗した場合の処理** (利用可能な場合)
       - **非稼働完了遅延**
       - **NNMi設定ポーリングを要求するタスク**

       これらのフィールドの詳細については、「NAコンソールでの設定パラメーター」(69ページ)を参照してください。
    c. ページの下にある [**保存**] をクリックします。

11. オプション。統合により、デバイスの不整合な速度設定や全二重設定の接続を検出するには、NAがデバイスのドライバを検出するようにしてください。以下の方法の1つを使用します。
    - ドライバを検出するように統合を設定した場合は、統合によってこの手順はすでに完了しています。
    - NAコンソールにおいて、[**新規タスク - ドライバの検出**] ページで ([**デバイス**] > [**デバイスのタスク**] > [**ドライバの検出**])、NNMiインベントリからインポートされたデバイスのドライバを検出します。

12. オプション。「NNMiとNA間のシングルサインオンの設定」(23ページ)の説明に従って、すべての統合されたNNMi管理サーバーとすべてのNAコアの間でシングルサインオンを設定します。

> **ヒント:** すべてのNNMi管理サーバーとすべてのNAコアで同じ初期化ストリングを使用します。水平スケーラビリティを持つ環境内のNAでは、統合の設定内容に関係なく、すべてのNAコアでシングルサインオンを設定します。

NNMi 10.10からNNMi 10.20にアップグレードされた統合設定

NNMi 10.0xまたはNA 10.1xのいずれかをバージョン10.2xにアップグレードする場合、統合が正常に動作するように、両方のアプリケーションを必要なバージョンにアップグレードする必要があります。NNMi 10.20およびNA 10.20を使用するためにHPE NNMi–HPE NA統合をアップグレードして有効にするには、以下の手順に従ってください。

1. 各統合NNMi管理サーバーのNNMiコンソールで、HPE NNMi–HPE NA統合を無効にします。「HPE NNMi–HPE NA統合の無効化」(60ページ)を参照してください。
2. 配備されたすべてのNNMi管理サーバーおよびNAコアをバージョン10.2xにアップグレードします。アップグレードの順序は重要でないため、これらのアプリケーションは任意の順序でアップグレードできます。

注: NNMiとNAを同じサーバーにインストールしている場合、NAをアップグレードするときにNAインストーラーからポートの競合警告が表示される可能性があります。警告で示されたポートをNNMiが使用している可能性があるため、これらの警告は無視します。詳細については、NNMiのnnm.portsのリファレンスページ、またはLinuxのマンページを参照してください。

注: NNMiとNAの両方を必要なバージョンにアップグレードするまで、HPE NNMi–HPE NA統合を有効にしないでください。

3. 「新規統合設定」(16ページ)の説明に従って、HPE NNMi–HPE NA統合を設定します。以下の点に注意してください。
   - [**HPE NNMi–HPE NAの統合設定**] フォームには以前の統合設定の値が含まれています。このフォームの新しいフィールドは、デフォルト値に設定されています。
   - NNMi 10.00では [**分析ペインデータを表示する最小オブジェクトアクセス権限**] フィールドが追加されます。このフィールドは [**分析ペインデータを表示する最小NNMiロール**] フィールドと相互動作します。NNMiのアップグレードにより、[**分析ペインデータを表示する最小NNMiロール**] フィールドの値が繰り越され、[**分析ペインデータを表示する最小オブジェクトアクセス権限**] フィールドが [オブジェクトゲスト] に設定されます。この設定はアップグレード前に設定されたアクセスレベルを維持します。[**分析ペインデータを表示する最小オブジェクトアクセス権限**] フィールドの値を変更することで、アクセスレベルの精度を高められます。詳細については、「NNMi分析ペインのNA情報へのNNMiユーザーアクセスの設定」(68ページ)を参照してください。
   - NA 10.00以前は、統合で単一のNNMiサーバー統合のためのコマンドスクリプトのサンプルが提供されていました。NA 10.00では、これらのスクリプトは含まれなくなりました。NA 10.00への統合のアップグレードにより、削除されるNNMi管理サーバーからコマンドスクリプトが削除されます。これにより、コマンドスクリプトで使用されるNAシステム変数は無効になります。
   - 以前のバージョンのNAからアップグレードする場合、[**NNMi-NA統合レベル**] フィールドは以下のようにマッピングされます。
     - 値「**完全**」によって、NA 10.00以降の [デバイス追加のNA/NNMiトポロジ同期] イベントルールが有効になります。
     - 値「**部分**」および「**NNMiからの一方向**」はNA 10.00以降の [デバイス追加のNA/NNMiトポロジ同期] イベントルールを無効にします。

NNMiとNA間のSSL通信の設定

SSL通信との統合を有効にする前に、NNMiサーバーとNAサーバーの間で証明書を交換するために以下の手順を実行します。

ヒント: 統合に関係するすべてのNNMi管理サーバーとNNMiコアの間で証明書を交換します。水平スケーラビリティを持つ環境内のNNMiでは、統合の設定内容に関係なく、すべてのNNMiコアでNNMi証明書をインストールします。

注: この手順において、「いずれかのNAコアサーバーで、以下のコマンドを実行して、truecontrol.keystoreファイルからNA証明書をエクスポートします。」(20ページ)および「各NNMi管理サーバーで、以下のコマンドを実行して、NNMi nnm.truststoreファイルにNAの証明書をインポートします。」(20ページ)での指示は、truecontrol.keystoreファイルからデフォルトのNA自己署名証明書をエクスポートすることを前提としています。参照されるコマンドの -alias sentinel部分は、truecontrol.keystoreファイルに含まれる証明書のタイプに応じて異なる場合があります。詳細については、『NA Administration Guide』の「Using Certificates with NA」を参照してください。

1. NNMi 10.00以降、NNMiと統合したシステムのSSL証明書には、ドメインネームサーバー (DNS) の短縮名やlocalhostという名前ではなく、統合されたサーバーの完全修飾ドメイン名 (FQDN) を含める必要があります。必要に応じて、NNMiと統合したNAコアサーバーの証明書を再生成します。証明書の生成時には、共通名 (CN) の値としてサーバーのFQDNを指定します。
2. いずれかのNAコアサーバーで、以下のコマンドを実行して、truecontrol.keystoreファイルからNA証明書をエクスポートします。
   - Windowsの場合:
     ```
     <NA_HOME>\jre\bin\keytool.exe -export -alias sentinel
     -file C:\temp\na.cer -keystore <NA_HOME>\server\ext\jboss\
     server\default\conf\truecontrol.keystore
     -storepass sentinel
     ```
   - Linuxの場合:
     ```
     <NA_HOME>/jre/bin/keytool -export -alias sentinel
     -file na.cer -keystore <NA_HOME>/server/ext/jboss/server/
     default/conf/truecontrol.keystore -storepass sentinel
     ```
3. 「Certificate stored in file directory:\na.cer」というメッセージが表示されることを確認します。
4. 「いずれかのNAコアサーバーで、以下のコマンドを実行して、truecontrol.keystoreファイルからNA証明書をエクスポートします。」(20ページ)で作成したNAの証明書ファイル (na.cer) を各NNMi管理サーバーにコピーします。
5. 各NNMi管理サーバーで、以下のコマンドを実行して、NNMi nnm.truststoreファイルにNAの証明書をインポートします。
   - Windowsの場合:
     ```
     %NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -import
     -alias sentinel -file "<certificate file directory>\na.cer"
     -keystore %NnmDataDir%\shared\nnm\certificates\
     nnm.truststore -storepass ovpass
     ```
   - Linuxの場合:
     ```
     $NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -import
     -alias sentinel -file <certificate file directory>/na.cer
     -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore
     -storepass ovpass
     ```

   「Trust this certificate?」という質問に対しては、必ず「**yes**」と答えます。以下のプログラムー覧は、このコマンドを実行した後の表示例です。

   ```
   Owner: CN=localhost, OU=Hewlett Packard Company, O=Hewlett Packard Company, L=Palo
   Alto, ST=CA, C=US
   Issuer: CN=localhost, OU=Hewlett Packard Company, O=Hewlett Packard Company, L=Palo
   ```

```
Alto, ST=CA, C=US
Serial number: 484e9d84
Valid from: Tue Jun 10 09:28:04 MDT 2008 until:Fri Jun 08 09:28:04 MDT 2018
Certificate fingerprints:
         MD5: 65:94:D1:A0:44:84:E2:69:A4:23:DC:B9:5E:EB:91:A8
          SHA1: 05:DE:DC:68:58:45:CA:EA:88:FF:16:05:E7:65:A9:5B:23:29:D7:65
Trust this certificate?[no]: yes
Certificate was added to keystore
```

6. いずれかのNNMi管理サーバーで、以下のコマンドを使用して、NNMiの証明書のエイリアス名を決定します。
   - Windowsの場合:
     %NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -v -list
     -keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore
     -storepass nnmkeypass
   - Linuxの場合:
     <NnmInstallDir>/nonOV/jdk/hpsw/bin/keytool -v -list -keystore
     <NnmDataDir>/OV/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass
7. 以下のコマンドを使用して、NNMiの証明書をファイルにエクスポートします。<alias>には、「いずれかのNNMi管理サーバーで、以下のコマンドを使用して、NNMiの証明書のエイリアス名を決定します。」(21ページ)でコマンドから出力された値を使用します。
   - Windowsの場合:
     %NnmInstallDir%\nonOV\hpsw\bin\keytool.exe -export
     -alias <alias> -file <directory>\nnm.cer
     -keystore %NNMDataDir%\shared\nnm\certificates\nnm.keystore
     -storepass nnmkeypass
   - Linuxの場合:
     <NnmInstallDir>/nonOV/jdk/hpsw/bin/keytool -export
     -alias <alias> -file <directory>/nnm.cer
     -keystore <NnmDataDir>/shared/nnm/certificates/nnm.keystore
     -storepass nnmkeypass
8. NNMiの証明書ファイル(nnm.cer)を各NAコアサーバーにコピーします。
9. 各NAコアサーバーで、以下のコマンドを実行して、NNMiの証明書をNAのtruecontrol.truststoreファイルにインポートします。<alias>には、「いずれかのNNMi管理サーバーで、以下のコマンドを使用して、NNMiの証明書のエイリアス名を決定します。」(21ページ)でコマンドから出力された値を使用します。
   - Windowsの場合:
     <NA_HOME>\jre\bin\keytool.exe -import -alias <alias>
     -file <Directory>\nnm.cer -keystore <NA_HOME>\server\ext
     jboss\server\default\conf\truecontrol.truststore
     -storepass sentinel
   - Linuxの場合:
     <NA_HOME>/jre/bin/keytool -import -alias <alias>
     -file <Directory>/nnm.cer -keystore <NA_HOME>/server/
     ext/jboss/server/default/conf/truecontrol.truststore
     -storepass sentinel

「Trust this certificate?」という質問に対しては、必ず「**yes**」と答えます。以下のプログラムー覧は、このコマンドを実行した後の表示例です。

```
Owner: CN=naqa-e01-vm59.fc.usa.hp.com
Issuer: CN=naqa-e01-vm59.fc.usa.hp.com
Serial number: 4e81ef8f
Valid from: Tue Sep 27 09:45:19 MDT 2011 until:Thu Sep 03 09:45:19 MDT 2111
Certificate fingerprints:
          MD5: E4:26:B2:0C:C5:A5:FE:46:F2:0E:2A:C3:5E:83:18:AE
          SHA1: EB:E9:A3:F0:6B:C7:45:E9:4B:16:00:52:1C:B4:9F:75:B6:DF:3F:DC
Signature algorithm name: SHA1withRSA
          Version: 1
Trust this certificate?[no]: yes
Certificate was added to keystore
```

10. 各NAコアサーバーで、NAサービスを再起動します。
    - Windowsの場合: [**サービス**] コントロールパネルを開きます。サービスのリストから、以下の各サービスを右クリックし、[**再起動**] をクリックします。

      TrueControl ManagementEngine

      TrueControl FTP Server

      TrueControl SWIM Server

      TrueControl Syslog Server

      TrueControl TFTP Server

    - Linuxの場合: 以下のコマンドを実行します。

      /etc/init.d/truecontrol restart

11. 各NNMi管理サーバーで、コマンドを以下の順序で実行します。
    - **ovstop**
    - **ovstart**

12. オプション。各NNMi管理サーバーおよび各NAコアサーバーで、以下のコマンドを実行します。出力を比較して、両方のサーバーのトラストストアファイルにキーストアが存在することを確認します。
    - NNMi管理サーバー (Windowsの場合):
      %NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -v -list -keystore %NnmDataDir%\shared\nnm\certificates\nnm.truststore -storepass ovpass
    - NNMi管理サーバー (Linuxの場合):
      <NnmInstallDir>/nonOV/jdk/hpsw/bin/keytool -v -list -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass
    - NAコアサーバー (Windowsの場合):
      <NA_HOME>\jre\bin\keytool.exe -v -list -keystore <NA_HOME>\server\ext\jboss\server\default\conf\truecontrol.truststore -storepass sentinel
    - NAコアサーバー (Linuxの場合):
      <NA_HOME>/jre/bin/keytool -v -list -keystore

```
/opt/NA/server/ext/jboss/server/default/conf/truecontrol.truststore -storepass
sentinel
```

NNMiとNA間のシングルサインオンの設定

注: Security Assertion Markup Language (SAML) を有効にした場合、NAはNNMiとNA間のHPE SSO (LWSSO (Light-weight Single Sign-on) とも呼ばれる) 機能をサポートしません。

シングルサインオンは、同一の初期化ストリング値を使用し、共通のネットワークドメイン名を共有するすべてのHPEアプリケーションで使用できます。

あるユーザーが、NNMiとNAでまったく同じユーザー名を使用している場合、そのユーザーはNNMiコンソールにログオンし、NAコンソールにログオンすることなくNAページを表示できます。同様に、そのユーザーは、NAコンソールにログオンし、NNMiコンソールにログオンすることなくNNMiページを表示できます。

このシングルサインオン機能では、2つの製品間のユーザー名をマッピングしますが、パスワードはマッピングしません。NNMiとNAのログオンパスワードが異なる場合があるためです。また、ユーザーロールもマッピングしないため、ユーザーは各アプリケーションで異なる権限を有することができます。たとえば、あるユーザーが、NNMiではオペレーターレベル1の権限、NAでは管理者権限を有する場合があります。

NNMiとNA間のシングルサインオンアクセスを行うには、両方のアプリケーションで同じ初期化ストリングが使用されていることを確認します。アプリケーションから別のアプリケーションにストリングをコピーして使用できます。使用する初期化ストリングを選択するときは、やり取りするすべてのアプリケーションを考慮します。必要に応じて、他のアプリケーションの初期化ストリング設定も更新します。

ヒント: すべてのNNMi管理サーバーとすべてのNAコアで同じ初期化ストリングを使用します。水平スケーラビリティを持つ環境内のNAでは、統合の設定内容に関係なく、すべてのNAコアでシングルサインオンを設定します。

NNMiとNA間にシングルサインオンを設定するには、以下の両方のタスクを実行します。

- 「タスク1: シングルサインオン用のNNMiの設定」(23ページ)
- 「タスク2: シングルサインオン用のNAの設定」(24ページ)

タスク1: シングルサインオン用のNNMiの設定

各NNMi管理サーバーで、以下の手順を実行します。

1. 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: `%NNM_PROPS%\nms-ui.properties`
   - Linuxの場合: `$NNM_PROPS/nms-ui.properties`
2. ファイルから、以下のようなセクションを特定します。

   ```
   com.hp.nms.ui.sso.isEnabled = false
   ```

   これを以下のように変更します。

   ```
   com.hp.nms.ui.sso.isEnabled = true
   ```
3. ストリング`initString`を検索します。

初期化ストリングは、initStringパラメーターの値です。引用符は含みません。

たとえば、nms-ui.propertiesファイルに以下のテキストが含まれているとします。

```
initString=E091F3BA8AE47032B3B35F1D40F704B4
```

この場合、以下が初期化ストリングです。

```
E091F3BA8AE47032B3B35F1D40F704B4
```

4. initStringパラメーターの値が、すべてのNNMi管理サーバーと同じであることを確認します。initStringパラメーターの値を変更した場合は、以下のコマンドを実行して変更をコミットします。

   nnmsso.ovpl -reload

   詳細については、nnmsso.ovplのリファレンスページ、またはLinuxのマンページを参照してください。

タスク2: シングルサインオン用のNAの設定

各NAコアサーバーで、以下の手順を実行します。

1. 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:
     <NA_HOME>\server\ext\jboss\server\default\conf\lwssofmconf.xml
   - Linuxの場合:
     <NA_HOME>/server/ext/jboss/server/default/conf/lwssofmconf.xml

   <NA_HOME> のデフォルト値は以下のとおりです。
   - Windowsの場合: C:\na
   - Linuxの場合: /opt/NA
2. enableLWSSOタグで、enableLWSSOFramework属性をtrueに設定します。

   ```
   enableLWSSOFramework="true"
   ```
3. lwssoValidationブロックで、以下の手順を実行します。
   - domainタグの値をNAコアサーバーの完全ドメイン名に設定します。たとえば、NAコアサーバーのホスト名がna.location.example.comの場合、<domain>location.example.com</domain> を設定します。

     注: この手順では、NNMi管理サーバーがNAコアサーバーと同じドメインにあることを前提としています。同じドメインにない場合、NNMi管理サーバーのドメインのDNSDomainエレメントをtrustedHostsブロックに追加する必要があります。
4. cryptoタグで、initString属性がNNMi nms-ui.propertiesファイルのinitStringプロパティの値であることを確認または設定します。

   注: cryptoブロック内の設定は、SSOを使用するすべてのアプリケーションで同一である必要があります。
5. trustedHostsブロックで、DNSDomainタグをlwssoValidationブロックのdomainタグの値に設定します。たとえば、以下のようになります。

   ```
   <DNSDomain>location.example.com</DNSDomain>
   ```

6. 「trustedHostsブロックで、DNSDomainタグをlwssoValidationブロックのdomainタグの値に設定します。たとえば、以下のようになります。」(24ページ)のアクションでは、NNMi管理サーバーがNAコアサーバーと同じドメインにあることを前提としています。NAコアサーバーが、NNMi管理サーバーとは異なるドメインにある場合、以下の例で示されている `<!--` と `-->` の文字を削除し、両方のドメインにDNSDomainエントリを追加します。

```
<multiDomain>
    <trustedHosts>
        <!--
        <DNSDomain>gmx.com</DNSDomain>
        <DNSDomain>companydomain2.com</DNSDomain>
        <NetBiosName>myserver</NetBiosName>
        <IP>192.168.12.13</IP>
        <FQDN>myserver.companydomain.com</FQDN>
        -->
    </trustedHosts>
</multiDomain>
```

7. SSOを使用するすべてのアプリケーションが、最大15分の差異の範囲でGMT (グリニッジ標準時) 時間に設定されていることを確認してください。これらのアプリケーションのタイムゾーンは異なる場合がありますが、GMTに変換するとシステム時間は同じになります。
8. NA jbossサーバーを再起動します。
   - Windowsの場合: NAコンソールの **[管理者] > [サービスの開始/停止]** ページで、管理エンジンを再起動します。
   - Linuxの場合: 以下のコマンドを実行します。

     `/etc/init.d/truecontrol restart`

9. NNMiとNAの両方で、一定期間後にユーザーインタフェースから自動的にユーザーがログアウトされます。HPE NNMi–HPE NA統合でSSOを設定するときに、NNMiとNAのタイムアウト値を同じ値に設定します。

   注: NNMiまたはNAで自動的にユーザーインタフェースからログアウトされる場合や、NNMiまたはNAから手動でログアウトする場合、NNMiコンソールおよびNAコンソールの両方からログアウトされます。

   NNMiとNAに同一のタイムアウト値を設定するには、以下の手順を実行します。

   a. NNMiとNAコンソールのタイムアウト値として、タイムアウト値 (分) を1つ選択します。HPEでは、30分の値を使用することをお勧めします。HPE NNMi–HPE NA統合で高レベルのセキュリティが不要な場合は、60分以上の値を使用します。
   b. 各NAコアサーバーで、以下のファイルをテキストエディターで開きます。
      - Windowsの場合: `<NA_HOME>\server\ext\jboss\server\default\conf\lwssofmconf.xml`
      - Linuxの場合: `<NA_HOME>/server/ext/jboss/server/default/conf/lwssofmconf.xml`

      `<NA_HOME>` のデフォルト値は以下のとおりです。
      - Windowsの場合: `C:\na`
      - Linuxの場合: `/opt/NA`
   c. `<expirationPeriod>1440</expirationPeriod>` タグを探します。

d. 既存の値を「NNMiとNAコンソールのタイムアウト値として、タイムアウト値 (分) を1つ選択します。HPEでは、30分の値を使用することをお勧めします。HPE NNMi–HPE NA統合で高レベルのセキュリティが不要な場合は、60分以上の値を使用します。」(25ページ)で選択した値に置き換えます。

e. 変更を保存します。この変更は、次回NAサービスを再起動したときに適用されます。

f. 各NNMi管理サーバーで、以下のファイルをテキストエディターで開きます。

   - Windowsの場合: `%NNM_PROPS%\nms-ui.properties`
   - Linuxの場合: `$NNM_PROPS/nms-ui.properties`

g. `#!com.hp.nms.ui.sso.expirationPeriod=1440`文字列を探します。

h. 文字列の先頭にある「**#!**」文字を削除し、既存の値を「NNMiとNAコンソールのタイムアウト値として、タイムアウト値 (分) を1つ選択します。HPEでは、30分の値を使用することをお勧めします。HPE NNMi–HPE NA統合で高レベルのセキュリティが不要な場合は、60分以上の値を使用します。」(25ページ)で選択した値に置き換えます。

i. 変更を保存します。

j. 以下のコマンドを実行し、変更をコミットします。

   `nnmsso.ovpl -reload`

   詳細については、nnmsso.ovplのリファレンスページ、またはLinuxのマンページを参照してください。

HPE NNMi–HPE NA統合の使用法

HPE NNMi–HPE NA統合は、NNMiとNAの両方に機能を追加します。このセクションでは以下の内容について説明します。

NNMiとNA間のインベントリ同期

HPE NNMi–HPE NA統合では、NNMiインベントリがNAインベントリのデバイスと動的に同期します。統合により、IPアドレスが比較され、NNMiノードとNAデバイスが照合されます。統合により、同期されたそれぞれのNNMiノードにNAデバイスIDが追加され、同期されたそれぞれのNAデバイスにNNMiノードUUIDが追加されます。

NNMiインベントリの同期のタイミング

HPE NNMi–HPE NA統合では、NNMiインベントリからNAインベントリへの同期が可能です。統合が有効になっている間、NNMiインベントリからNAインベントリへ継続的に同期が発生します。

対象となるNNMiノード

HPE NNMi–HPE NA統合では、NNMiインベントリのノードの一部またはすべてが同期されます。これは、[HPE NNMi–HPE NA**の統合設定**] フォームの [**トポロジフィルターノードグループ**] パラメーターによって決まります。

- ノードグループが指定されている場合、そのグループのノードのみがNAインベントリと同期されます。
- NNMiインベントリ全体をNAインベントリと同期するには、[**トポロジフィルターノードグループ**] フィールドをオフにします。

NNMiノードの移動先 (NAインベントリ)

インベントリ同期のNAパーティションは、[**HPE NNMi–HPE NAの統合設定**] フォームの [**NNMiセキュリティグループをNAパーティションにマップします**] チェックボックスがオンになっているかどうかによって異なります。

- [**NNMiセキュリティグループをNAパーティションにマップします**] チェックボックスがオンの場合、NNMiからNAに同期されたデバイスは、そのノードを含むNNMiセキュリティグループと同じ名前で常にNAパーティションに追加されるか更新されます。NNMi管理者が後でこのノードを別のセキュリティグループに移動すると、同期によって対応するNAパーティションにNAデバイスが移動します。パーティションが存在しない場合、NNMiによってNNMiセキュリティグループと同じ名前でパーティションが作成され、NNMiセキュリティグループの説明とともにNA Siteビューに関連付けられます。デバイスが別のNAパーティションに存在する場合、同期によって、NNMiセキュリティグループに一致するNAパーティションにデバイスが移動します。NNMiのDefault Security Groupは、NAのDefault Siteパーティションにマッピングされます。どちらの名前を変更しても、このマッピングは変更されません。

  > **ヒント:** 複数のNNMiリージョナルマネージャーで同じノードを管理している場合、すべてのNNMiリージョナルマネージャーのNNMiセキュリティグループにそのノードが含まれていることを確認します。

- [**NNMiセキュリティグループをNAパーティションにマップします**] チェックボックスがオフになっている場合、デバイス

のNAパーティションは、NAインベントリにデバイスがすでに存在しているかどうかによって異なります。

- NAインベントリにデバイスがまだ存在していない場合、同期によってNA Default Siteパーティションにデバイスが作成されます。NA管理者が後でこのデバイスを別のパーティションに移動すると、統合によってその別のパーティションにデバイスが残ります。
- NAインベントリにデバイスがすでに存在している場合、デバイスは割り当てられたパーティションに残ります。

注: NA10.00より前のバージョンでは、各同期周期ですべての同期デバイスがNA Default Siteパーティションに移動していました。

NNMiへのノードの追加

NNMiインベントリのノードグループ ([**トポロジフィルターノードグループ**] パラメーターで指定したノードグループ) にノードが追加されると、ここで説明するように統合によってそのノードがNAインベントリと同期します。

NNMiからのノードの削除

同期ノードがNNMiから削除されると、統合によってそのNNMi管理サーバーとの関連付けがNAデバイスから削除されます。デバイスに関連付けられたNNMiノードUUIDがなくなると、統合によってNAの対応するデバイスが管理対象外になります。NAで管理対象外になったデバイスのデバイス履歴は、まだ使用可能です。

NAインベントリの同期のタイミング

1つのNNMi管理サーバーのみがNAと統合される場合、[デバイス追加のNA/NNMiトポロジ同期] イベントルールにより、統合でNAインベントリからNNMiインベントリへの同期が発生するかどうかが決まります。

- [デバイス追加のNA/NNMiトポロジ同期] イベントルールがアクティブである場合、ここで説明するようにNAインベントリ全体で同期が発生します。
- [デバイス追加のNA/NNMiトポロジ同期] イベントルールがアクティブでない場合、統合の同期はNNMiからNAへの一方向で発生します。

注: 複数のNNMi管理サーバーが1つのNA配備と統合される場合、統合で [デバイス追加のNA/NNMiトポロジ同期] イベントルールが無視され、NAインベントリからNNMiインベントリへの同期は発生しません。1つのNA配備は以下のいずれかになります。

- スタンドアロンNAコア
- 水平スケーラビリティを持つ環境のNA

ヒント: NNMiマルチテナント環境では、NNMi自動検出では常に新しいノードがデフォルトテナントに割り当てられるため、NNMi管理者はNNMiインベントリへの新しいノードの追加を直接制御する必要があるという点に注意してください。このため、NNMiマルチテナント環境では、[デバイス追加のNA/NNMiトポロジ同期] イベントルールを常に無効にしておく必要があります。

NAインベントリからNNMiインベントリへの同期は、統合が有効になるたびに発生します。

対象となるNAデバイス

NAインベントリ全体で同期が発生します。

注: 仮想デバイスコンテキスト (VDC) をサポートするCiscoデバイスの場合、NAはこれらのデバイスのコンテキスト検出時にすべてのVDCを検出します。統合の同期中、NAは解決可能な管理コンテキストIPアドレスのみをNNMiに送信します。同期されたインベントリに残りのVDCを含めるには、NNMiでそれらのVDCノードを別々にシードします。

NAデバイスの移動先 (NNMiインベントリ)

NAインベントリのデバイスがNNMiインベントリにない場合は、統合によって検出ヒントがNNMiに送信されます。

- NNMi自動検出ルールにヒントを受けたデバイスが含まれている場合、NNMiでノードが検出されます。NNMiのノードグループ設定によって、NAからヒントを受けたデバイスがどのノードグループに含まれるかが決まります。NNMiで、新しいノードがデフォルトセキュリティグループとデフォルトテナントに追加されます。
- NNMi自動検出ルールにヒントを受けたデバイスが含まれていない場合、NNMiでノードは検出されません。

ヒント: 統合で検出ヒントが送信されるのは、最初の同期中だけです。検出ヒントを再送信するように統合をトリガーするには、統合を無効にしてから有効にします。

NAへのデバイスの追加

NAインベントリに新しいデバイスが追加されると、統合によって検出ヒントがNNMiに送信されます。

ヒント: 新しいデバイスが以前にNAインベントリに存在し、同期後に削除された場合、NNMiはその検出のヒントに応答しません。この場合、NNMiでデバイスの検出シードを作成します。

NAからのデバイスの削除

同期デバイスがNAから削除されると、統合によって、対応するノードを管理しているすべてのNNMi管理サーバーのNNMiインベントリからそのノードが削除されます。

同期後のノードの移動

同期ノードが [**トポロジフィルターノードグループ**] パラメーターで指定されたノードグループから別のノードグループに移動しても、NAインベントリはすぐには影響されません。ただし、このノードが後でNNMiから削除されると、統合によってNAの対応するデバイスが管理対象外になります。同じように、このノードが後でNAから削除されると、統合によって対応するノードがNNMiインベントリから削除されます。

定期的同期の考慮事項

HPE NNMi–HPE NA統合は、NNMiからNAへの完全なインベントリ同期を定期的に実行します。
HPE NNMi–HPE NA統合は、NAからNNMiへの完全なインベントリ同期は実行しません。HPE NNMi–HPE NA統合が有効なままの場合、この定期的同期は統合を最初に有効にしたときに行われた同期と同じプロセスに従います。

[**HPE NNMi–HPE NAの統合設定**] フォームの [**トポロジ同期間隔 (時間)**] パラメーターでは、定期インベントリ同期の頻度を指定します。

インベントリ同期はフェイルセーフメカニズムです。NNMi管理サーバーとNAコアサーバーの間で接続の信頼性が高い場合、トポロジ同期の間隔は広くすることができます。

定期インベントリ同期はNNMiスパイラル検出で負荷分散され、NNMi管理サーバーに負荷がかかり過ぎないようにペース配分されます。検出アクティビティが多い期間は、インベントリ同期は行われません。

HPE Blade System Virtual Connectデバイスのサポート

HPE Blade System Virtual Connectデバイスを統合して、1つのプライマリデバイスと、1つ以上のスタンバイデバイスおよびスレーブデバイスで構成されるVirtual Connectドメインを形成することができます。この統合は、ドメインプライマリサービス、またはスタンドアロンサービスとして機能するVirtual Connectデバイスのみに関するNAインベントリ情報に渡されます。

NAインベントリと同期するVirtual Connectデバイスを制限するには、以下の手順を実行します。

1. 以下のいずれかの機能を使用する追加フィルターに基づいて、1つ以上のNNMiノードグループを作成します。
   - com.hp.nnm.capability.node.hpvcStandalone
   - com.hp.nnm.capability.node.hpvcPrimary
   - com.hp.nnm.capability.node.hpvcStandby
   - com.hp.nnm.capability.node.hpvcSlave
2. 「以下のいずれかの機能を使用する追加フィルターに基づいて、1つ以上のNNMiノードグループを作成します。」(30ページ)で作成したすべてのノードグループに対して、親ノードグループを1つ作成します。

   この親ノードグループに、NAインベントリと同期する必要のあるほかのデバイスも入れます。
3. その親ノードグループの名前を使用して、[**HPE NNMi–HPE NAの統合設定**] フォームの [**トポロジフィルターノードグループ**] パラメーターを更新します。詳細については、「統合動作」(66ページ)を参照してください。

統合が提供するNNMi機能

HPE NNMi–HPE NA統合では、以下の機能のために、NNMiからNAへの通信が提供されます。

- 「NNMiコンソールからのNAコンソールのページの起動」(30ページ)
- 「NNMiからのNA診断のトリガー」(31ページ)
- 「不整合な状態のレイヤー2接続の特定」(32ページ)
- 「NNMi分析ペインに表示されるNA情報」(33ページ)

NNMiコンソールからのNAコンソールのページの起動

HPE NNMi–HPE NA統合は、NNMiビューのコンテキストでNNMiコンソールからNAコンソールのページを開くためのリンクを提供します。

HPE NNMi–HPE NA統合を有効にすると、NNMiコンソールの [**アクション**] メニューに以下の項目が追加されます。

- [**HPE NA診断の結果の表示**] — NNMiインシデントのデバイスにスケジュールされたタスクのリストを表示します。タスクを選択してタスクの結果を表示します。詳細については、「NAにアクセスするインシデントアクションの結果の表示」(32ページ)を参照してください。
- [**HPE NA診断の再実行**] — NNMiインシデントのデバイスに設定されたNAアクションを実行します。詳細については、「NAにアクセスするインシデントアクションの結果の表示」(32ページ)を参照してください。

- [**不整合の接続を表示**]—速度または全二重設定に差があるすべてのレイヤー2接続のテーブルを表示します。詳細については、「不整合な状態のレイヤー2接続の特定」(32ページ)を参照してください。
- [**HPE NAデバイス情報の表示**]—NNMiで選択されたデバイスについて、現在のNAの[**デバイスの詳細**]ページを開きます。
- [**HPE NAデバイス設定の表示**]—NNMiで選択されたデバイスについて、NAの[**現在の設定**]ページを開きます。

  注: デバイスのリアルタイム変更の検出が無効になっている場合、最後のデバイスポーリング周期でNAが取得した設定が表示されます。その取得に続いて設定変更が行われた場合、[**現在の設定**]ページの情報は、実際の現在の設定でない場合があります。

- [**HPE NAデバイス設定の差異の表示**]—NNMiで選択されたデバイスについて、NAの[**デバイス設定を比較**]ページを開きます。
- [**HPE NAデバイス設定の履歴の表示**]—NNMiで選択されたデバイスについて、NAの[**NAデバイス設定の履歴**]ページを開きます。
- [**HPE NAポリシーコンプライアンスレポートの表示**]—NNMiで選択されたデバイスについて、NAの[**ポリシー、ルール、およびコンプライアンスの検索結果**]ページを開きます。

  注: コンプライアンス情報には、NA Ultimateライセンスが必要です。

- [**HPE NAデバイスへのTelnet**]—NNMiで選択されたデバイスに接続する[**Telnet**]ウィンドウを開きます。
- [**HPE NAデバイスへのSSH**]—NNMiで選択されたデバイスに接続する[**SSH**]ウィンドウを開きます。
- [**HPE NAの起動**]—NAコンソールを開きます。
- [**HPE NAコマンドスクリプトの起動**]—NAの[**新規タスク — コマンドスクリプトを実行**]ページを開きます。このページは、NNMiコンソールで選択されたノードまたはインシデントについて事前入力されます。
- [**HPE NA診断の起動**]—NAの[**新規タスク — 診断実行**]ページを開きます。このページは、NNMiコンソールで選択されたノードまたはインシデントについて事前入力されます。

NA機能の使用方法については、『HPE Network Automationユーザガイド』を参照してください。

NNMiからのNA診断のトリガー

HPE NNMi–HPE NA統合を有効にすると、関連するインシデントタイプが発生するたびに、NA Diagnosticsにアクセスするインシデントアクションを含めるように、すぐに使用できるNNMiインシデントのいくつかが変更されます。「表2　NA診断で設定されたNNMiインシデント」(31ページ)には、変更されたインシデントがリストされています。

表2　NA診断で設定されたNNMiインシデント

NNMiインシデント	NA診断
OSPFNbrStateChange	隣接ノードを表示
OSPFVirtIfStateChange	隣接ノードを表示
OSPFIfStateChange	隣接ノードを表示 インタフェースを表示

表2　NA診断で設定されたNNMiインシデント (続き)

NNMiインシデント	NA診断
InterfaceDown	インタフェースを表示
CiscoChassisChangeNotification	モジュールを表示

NA診断コマンドスクリプトをインシデントアクションとして設定

別のNNMiインシデントにNAにアクセスするアクションを追加し、デフォルトのインシデントアクションを変更できます。インシデントの [**アクション**] タブで、ScriptOrExecutableの [**コマンドタイプ**] を使用して新しいライフサイクルの以降アクションを追加します。[**コマンド**] テキストボックスに、適切な引数を使用して、naruncmdscript.ovplまたはnarundiagnostic.ovplを入力します。例については、「表2　NA診断で設定されたNNMiインシデント」(31ページ)にリストされたインシデントのアクション設定を参照してください。

NAにアクセスするインシデントアクションの結果の表示

NAアクションで設定された、あるタイプのインシデントが届くと、NNMiは、設定されたアクションを開始し、診断またはコマンドスクリプトのタスクIDをそのインシデントの属性として保存します。タスクIDの存在によって、[**アクション**] メニューの [**HPE NA診断の結果の表示**] と [**HPE NA診断の再実行**] 項目が利用できるようになります。

インシデントが発生したときのアクションの結果を表示するには、NNMiインシデントビューでインシデントを選択し、**[アクション] > [HPE NA診断の結果の表示]** を選択します。

設定されたアクションの現在の結果を表示するには、NNMiインシデントビューでインシデントを選択し、**[アクション] > [NA NA診断の再実行]** を選択します。

タスクを複数回実行する場合、NNMiは、[**インシデント**] フォームの [**カスタム属性**] タブに最近のタスクIDのリストを表示します。[**NA NA診断の結果の表示**] アクションは、異なるユーザーの結果を比較できるように、インシデントに実行されたすべてのタスクを表示します。

不整合な状態のレイヤー2接続の特定

HPE NNMi–HPE NA統合が有効になっている場合、NNMiは、NNMiトポロジの各レイヤー2接続のいずれかのエンドにある2つのインタフェースの速度と全二重設定をNAに定期的にクエリーします。さらに、NNMiは、NNMiトポロジに追加される新しい接続と、NNM iSPI Performance for Metricsが実行している場合は、不整合接続を示すパフォーマンスしきい値の例外を伴う接続の、インタフェースの速度と全二重設定をNAにクエリーします。NNMiは、不整合検出アルゴリズムを使用して、その値によって不整合な接続となるかどうかを判断します。

注: NNMiは、NAインベントリにレイヤー2接続を形成するインタフェース用のMACアドレスが含まれている場合にのみ、不整合分析を実行します。

- NAインタフェースのレコードに有効なMACアドレスが含まれていない場合は、NAの**トポロジデータ収集**診断を実行して、MACアドレスフィールドを更新します。詳細については、「オプション。統合により、デバイスの不整合な速度設定や全二重設定の接続を検出するには、NAがデバイスのドライバを検出するようにしてください。以下の方法の1つを使用します。」(18ページ)を参照してください。
- 複数のポートで同じMACアドレスを使用するデバイスの場合は、NAで重複MACアドレスの保存を有効にしてください。詳細については、『NA Administration Guide』の「Configuring NA to Store Duplicate MAC Addresses」を参照してください。

[アクション] > [一致していない接続の表示]コマンドでは、速度の不整合か全二重の不整合、またはその両方を含むとNNMiが考えるレイヤー2接続のテーブルが表示されます。

疑わしい接続について、テーブルは、接続のいずれかー端にあるインタフェースの速度と全二重の値、およびデータの解釈を示します。考えられる解釈は以下のとおりです。

- POSSIBLE_MISMATCHは、速度の値か全二重の値、またはその両方の値が競合しており、接続不良またはパフォーマンスが低い接続となる可能性があることを示します。
- MISMATCHは、速度の値か全二重の値、またはその両方の値が競合しており、接続不良またはパフォーマンスが低い接続となる可能性が高いことを示します。

[**HPE NNMi–HPE NAの統合設定**] フォームの [**NA接続チェック間隔 (時間)**] パラメーターは、接続クエリーの頻度を指定します。

NNMi分析ペインに表示されるNA情報

NNMi分析ペインには、HPE NNMi–HPE NA統合を介して同期されたノードおよびノードのインタフェースのNA情報が表示されます。「表3 NNMi分析ペインのNA情報」(33ページ)には、統合で提供される分析ペインのタブが表示される可能性のあるNNMiビューがリストされています。

表3 NNMi分析ペインのNA情報

NNMiビュー	使用できるNA分析ペインのタブ
• [ノード] インベントリビュー • [ノード詳細] フォーム	• ノードの設定 • ノード設定の履歴 • ノードポリシーコンプライアンス
• [インシデントの参照] ビュー • [インシデント] フォーム 特定のインシデントタイプについては、「NA分析ペインのタブのノードインシデントタイプ」(35ページ)を参照してください。	• ノードの設定 • ノード設定の履歴
• [インタフェース] インベントリビュー • [インタフェース詳細] フォーム	• インタフェースの設定
• [インシデントの参照] ビュー • [インシデント] フォーム 特定のインシデントタイプについては、「NA分析ペインのタブのインタフェースインシデントタイプ」(36ページ)を参照してください。	• インタフェースの設定

注: NNMi管理者は、これらの分析ペインのタブへのアクセスを特定のNNMiユーザーロールやオブジェクトアクセスレベルに制限できます。詳細については、「NNMi分析ペインのNA情報へのNNMiユーザーアクセスの設定」(68ページ)を参照してください。

[ノードの設定] タブ

[**ノード設定**] タブには、現在のノードの実行設定が表示されます。

[**ノード設定**] タブは、以下のNNMiビューで使用できます。

- [ノード] インベントリビュー
- 同期ノードの [ノード詳細] フォーム
- [インシデントの参照] ビュー
- 同期ノードに関連するインシデントの [インシデント] フォーム

適用可能なインシデントタイプについては、「NA分析ペインのタブのノードインシデントタイプ」(35ページ)を参照してください。

NAコンソールでこの情報にアクセスするには、NNMiコンソールで [**アクション**] > [**HPE Network Automation**] > [**HPE NAデバイス設定の表示**] を選択します。

[ノード設定の履歴] タブ

[**ノード設定の履歴**] タブには、ノード設定が変更された時間のテーブルが表示されます。

NAコンソールで追加ノードの設定情報を表示するには、[**前と比較**] または [**表示設定**] をクリックします。

[**ノード設定の履歴**] タブは、以下のNNMiビューで使用できます。

- [ノード] インベントリビュー
- 同期ノードの [ノード詳細] フォーム
- [インシデントの参照] ビュー
- 同期ノードに関連するインシデントの [インシデント] フォーム

適用可能なインシデントタイプについては、「NA分析ペインのタブのノードインシデントタイプ」(35ページ)を参照してください。

NAコンソールでこの情報にアクセスするには、NNMiコンソールで [**アクション**] > [**HPE Network Automation**] > [**HPE NAデバイス設定の履歴の表示**] を選択します。

ノードポリシーコンプライアンスタブ

[**ノードポリシーコンプライアンス**] タブには、ノードに適用されるアクティブな設定ポリシーのテーブルが表示されます。また、ノードが各ポリシーに準拠しているかどうかも示されます。

> **注:** コンプライアンス情報には、NA Ultimateライセンスが必要です。

[**コンプライアンス状態**] 列で使用される値は以下のとおりです。

- はい — デバイスの設定は、該当のすべてのポリシーに準拠しています。
- いいえ — デバイスの設定は、該当の1つ以上のポリシーに準拠していません。
- 認識不能 — デバイスに対してポリシーが実行されていないか、該当のポリシーにエラーがあります。この値は、NA APIの`show policy compliance`コマンドの出力に表示される`Not checked yet`の値に対応します。

NAコンソールでこのノードのポリシーを表示するには、[**NAのポリシーコンプライアンスの表示**] をクリックします。

[**ノードポリシーコンプライアンス**] タブは、以下のNNMiビューで使用できます。

- [ノード] インベントリビュー
- 同期ノードの[ノード詳細] フォーム

以下のメッセージは、NAでこのノードに対してポリシーコンプライアンスチェックが実行されていないことを示します。

```
There is no active device policy compliance information to report.
```

このメッセージは、次のいずれかの場合に表示されます。

- NAが、このデバイスに対して設定ポリシーを実行していない場合。
- このデバイス用のNA設定ポリシーがアクティブになっていない場合。NAコンソールの[ポリシー] ページ (**[ポリシー] > [ポリシーリスト]**) には、使用可能な設定ポリシーのステータス ([アクティブ] または [非アクティブ]) が表示されます。
- NAで、NA Ultimateライセンスが使用されていない場合。

[インタフェースの設定] タブ

[**インタフェース設定**] タブには、デバイス設定によって決まる現在のインタフェースの実行設定が表示されます。

[**インタフェース設定**] タブは、以下のNNMiビューで使用できます。

- [インタフェース] インベントリビュー
- 同期ノードのインタフェースの[インタフェース詳細] フォーム
- [インシデントの参照] ビュー
- 同期ノードのインタフェースに関連するインシデントの[インシデント] フォーム

適用可能なインシデントタイプについては、「NA分析ペインのタブのインタフェースインシデントタイプ」(36ページ)を参照してください。

統合でNAポートに対してNNMiインタフェースを照合する方法については、「NNMiとNAの間のインタフェースの照合」(36ページ)を参照してください。

NA分析ペインのタブのノードインシデントタイプ

[ノード設定] および [ノード設定の履歴] 分析ペインのタブは、以下のインシデントタイプで使用できます。

- AddressNotResponding
- NodeDown
- NodeOrConnectionDown
- SNMPv1 NA Config trap
- SNMPv2 NA Config trap
- BackplaneOutOfRangeOrMalfunctioning
- BufferOutOfRangeOrMalfunctioning
- CpuOutOfRangeOrMalfunctioning
- DiskOutOfRangeOrMalfunctioning
- MemoryOutOfRangeOrMalfunctioning
- NodeTraffic
- RoundTripTimeHigh
- TestFailed

NA分析ペインのタブのインタフェースインシデントタイプ

[インタフェース設定]分析ペインのタブは、以下のインシデントタイプで使用できます。

- InterfaceDown
- InterfaceFCSLANErrorRateHigh
- InterfaceFCSWLANErrorRateHigh
- InterfaceInputDiscardRateHigh
- InterfaceInputErrorRateHigh
- InterfaceInputUtilizationHigh
- InterfaceOutputDiscardRateHigh
- InterfaceOutputErrorRateHigh
- InterfaceOutputUtilizationHigh
- InterfaceTraffic

NNMiとNAの間のインタフェースの照合

NNMiで管理されるインタフェースがNAのポート名と一致する場合、NNMiにNAのポート情報が表示されます。以下の照合手順の最初の一致がNNMiによって選択されます。

1. NNMiによって、NNMiのインタフェースIPアドレスがNAのポートIPアドレスと照合されます。
2. NNMiによって、NAのポート名がNNMiのインタフェース属性のいずれか(`ifName`、`ifAlias`、`ifDescr`、または`sourceObjectName`)と照合されます。
3. NNMiによって、NAのMAC層アドレスがNNMiの物理アドレスと照合されます。

注: NAの複数のポート設定がNNMiで管理される1つのインタフェースに一致する場合、この一致する設定情報はNNMiには表示されません。

NNMiで管理される複数のインタフェースがNAの1つのポート設定と一致する場合、この一致するNAのポート情報がNNMiの[**インタフェースの設定**]タブに表示されます。

統合が提供するNA機能

HPE NNMi–HPE NA統合では、以下の機能のために、NAからNNMiへの通信が提供されます。

- 「NAコンソールからのNNMiコンソールのページの起動」(37ページ)
- 「NNMiへのSNMPトラップの送信」(37ページ)
- 「NAからのNNMiノード設定ポーリングのトリガー」(38ページ)
- 「デバイス設定中のネットワーク管理の無効化」(39ページ)
- 「NAへのデバイスコミュニティ文字列の変更の伝達」(40ページ)
- 「HPE NNMi–HPE NA統合のNAイベントルール」(41ページ)

注: NAで設定された統合動作は、統合されるすべてのNNMi管理サーバーに適用されます。

NAコンソールからのNNMiコンソールのページの起動

HPE NNMi–HPE NA統合は、NAコンソールからNNMiコンソールのページを開くためのリンクを提供します。

- [**デバイスの詳細**] ページの [NNMiの関連付け] テーブルには、デバイスを管理している各NNMi管理サーバーの以下のリンクが含まれます。
  - NNMiサーバー — NNMiコンソールが開いて、このNNMi管理サーバーの初期ビューが表示されます。
  - NNMiノードUUID — NNMiコンソールが開いて、このデバイスの [**ノード**] フォームが表示されます。
- [**システム管理設定 - NA/NNMi統合**] ページにある [統合サーバーリスト] の [NNMiサーバー] 列の各値は、このNNMi管理サーバーのNNMiコンソールの初期ビューへのリンクです。

NNMi機能の使用法については、NNMiヘルプを参照してください。

NNMiへのSNMPトラップの送信

HPE NNMi–HPE NA統合を有効にすると、同期NAデバイスで指定のNAイベントが発生したときにNAからNNMiにSNMPトラップが送信されるように設定されます。NNMiオペレーターはこのトラップをインシデントビューで確認でき、必要に応じてその変更を調査できます。

NNMiでは、NASnmpTrapv1およびNASnmpTrapv2インシデントタイプにより、NNMiインシデントビューのNAトラップメッセージの形式が制御されます。統合を有効にすると、NNMiで使用できるSNMPトラップ設定にこれらのインシデントタイプが追加されます。

NAでは、[SNMPトラップによるNA/NNMi統合 (NNMiサーバー)] イベントルールにより、NAからNNMiにSNMPトラップを送信するNAイベントが決まります。また、このイベントルールでは、トラップのコミュニティ文字列、トラップのSNMPバージョン、およびNAからトラップが送信されるNNMiポートも決まります。

統合を有効にすると、各NNMi管理サーバーのいずれかのイベントルールが追加されます。[SNMPトラップによるNA/NNMi統合 (NNMiサーバー)] イベントルールのデフォルト設定は、以下のとおりです。

- デバイス設定の変更時にのみNAからSNMPトラップが送信される。
- トラップには、デバイスにアクセスするためにNAで使用されるコミュニティ文字列が含まれている。
- トラップではSNMPv1形式が使用される。
- トラップはNNMi管理サーバーのポート162に送信される。

イベントルールは、NNMi管理サーバーごとに異なるカスタマイズを行うことができます。

SNMPトラップの送信のカスタマイズ

1つのNNMi管理サーバーと統合する場合の [SNMPトラップによるNA/NNMi統合] イベントルールの設定を変更するには、以下の手順を実行します。

1. NAコンソールで、[イベントの通知とリスポンスルール] ページ (**[管理者] > [イベントの通知とリスポンスルール]**) を開きます。
2. NNMi管理サーバーの [SNMPトラップによるNA/NNMi統合] イベントルールの行で、[**編集**] を選択します。
3. [イベントの通知とリスポンスルールを編集] ページで、以下のいずれかの手順を実行します。
   - [**以下のイベントが発生するとき**] フィールドで、NAからNNMiにSNMPトラップを送信するNAイベントを選択します。

ヒント: デバイスに関連付けられたNAイベントの場合にのみNAからSNMPトラップが送信されます。このフィールドには、デバイスに固有でないイベント(ユーザーの追加など)が含まれます。NAでは、これらの非デバイスイベントは無視されます。

- [**SNMPトラップレシーバーポート**] フィールドをNNMi管理サーバーの値に設定します。
- [**SNMPコミュニティ文字列**] フィールドをこのNNMi管理サーバーへのトラップに含まれる値に設定します。
- [**SNMPバージョン**] フィールドを [SNMPv1] または [SNMPv2] のいずれかに設定します。

注: イベントルール設定のほかの設定は変更しないでください。

4. [**保存**] をクリックします。

SNMPトラップの送信の無効化

NAからNNMi管理サーバーにSNMPトラップが送信されないようにするには、そのNNMi管理サーバーの [SNMPトラップによるNA/NNMi統合] イベントルールのルールステータスを非アクティブに設定します。詳細については、「NAイベントルールの無効化」(43ページ)を参照してください。

NAからのNNMiノード設定ポーリングのトリガー

特定のデバイス設定タスクの場合、タスクが完了すると、そのデバイスを管理しているNNMi管理サーバーのノード再検出がNAからトリガーされます。このノード再検出では、デバイスに関する正確な情報がNNMiで保持されていることが確認されます。

NNMiノード設定ポーリングのトリガーのカスタマイズ

NAコンソールの [**システム管理設定 - NA/NNMi統合**] ページの [**NNMiに構成ポーリングを要求するタスク**] フィールドで、デバイスを再検出するようにNNMiをトリガーするデバイス設定タスクを指定します。デフォルトの選択は以下のとおりです。

- デバイスソフトウェアの更新
- パスワードの配布
- デバイスの再起動
- ドライバの検出

以下のタスクのいずれかまたはすべてをさらに選択できます。

- コマンドスクリプトの実行
- 診断の実行
- ACLの削除
- Syslogの設定
- ICMPテストの実行
- スナップショットの作成

- スタートアップと実行の同期
- OS分析

NNMiノード設定ポーリングのトリガーの無効化

NAからNNMiのノード設定ポーリングがトリガーされないようにするには、[NA/NNMi統合再検出ホスト] イベントルールのルールステータスを非アクティブに設定します。詳細については、「NAイベントルールの無効化」(43ページ)を参照してください。

デバイス設定中のネットワーク管理の無効化

NNMiは、[管理対象] 管理モードでノードのステータスを定期的にチェックし、応答しないノードのインシデントを生成します。NAによって開始されるデバイスメンテナンス手順の間に、HPE NNMi–HPE NA統合によってNNMiの管理モードが [サービス停止中] に変更される可能性があります。このようにすることで、非応答の理由がわからないノードに関する不要なインシデントがNNMiで生成されなくなります。

特定のデバイス設定タスクの場合、NAは、そのデバイスを管理しているNNMi管理サーバーにサービス停止中イベントを送信します。デバイス設定が成功したら、NAは、サービス状態イベントを同じNNMi管理サーバーに送信します。NNMiは、サービス状態イベントに応答し、デバイスから [サービス停止中] 管理モードを解除して、通常の状態ポーリングを再開します。

サービス停止中の動作のカスタマイズ

NAコンソールの [**システム管理設定 - NA/NNMi統合**] ページの [**デバイスをサービス停止中にするタスク**] フィールドで、タスクの実施中にデバイスを [サービス停止中] 管理モードに設定するようにNNMiをトリガーするデバイス設定タスクを指定します。デフォルトの選択は以下のとおりです。

- デバイスソフトウェアの更新
- パスワードの配布
- デバイスの再起動

以下のタスクのいずれかまたはすべてをさらに選択できます。

- コマンドスクリプトの実行
- 診断の実行
- ACLの削除
- Syslogの設定
- ドライバの検出
- ICMPテストの実行
- スナップショットの作成
- スタートアップと実行の同期
- OS分析

NAコンソールの [**システム管理設定 - NA/NNMi統合**] ページの [**サービス停止中の完了の遅延**] フィールドの値で、[**デバイスをサービス停止中にするタスク**] フィールドで選択したいずれかのタスクが完了してから、デバイスの管理モードをリセットするようにNNMiをトリガーするまでのNAの待機時間を指定します。この時間によって、デバイスが設定タスクから復帰している間にNNMiで停止中インシデントが作成されなくなります。たとえば、デバイスの起動には数分かかります。

デバイス設定が正しく行われない場合、動作は統合設定に依存します。

- [**デバイスタスクが失敗した場合**]設定では、デバイス設定に失敗した場合に統合でNNMi管理モードをどのように処理するのかを指定します。選択肢は以下のとおりです。
  - 管理モードをNAサービス停止中イベントの前の値に復元する。(これはデフォルト設定です)。
  - [サービス停止中]管理モードを維持する。
- [**デバイス準拠確認が失敗した場合の処理**]設定では、NAタスクの完了時にデバイス設定が準拠していない場合に統合でNNMi管理モードをどのように処理するのかを指定します。選択肢は以下のとおりです。
  - 管理モードをNAサービス停止中イベントの前の値に復元する。(これはデフォルト設定です)。
  - [サービス停止中]管理モードを維持する。

> **注:** デバイス準拠確認は、NA Ultimateライセンスでのみ使用できます。

これらの設定は、[**デバイスをサービス停止中にするタスク**]フィールドで選択されたすべてのデバイスタスクに適用されます。タスク別に復旧の動作を設定することはできません。

サービス停止中の動作の無効化

NAからNNMiのノード設定ポーリングがトリガーされないようにするには、[NA/NNMi統合サービス停止中]イベントルールのルールステータスを非アクティブに設定します。詳細については、「NAイベントルールの無効化」(43ページ)を参照してください。

NAへのデバイスコミュニティ文字列の変更の伝達

SNMPコミュニティ文字列の伝播が有効である場合、統合は以下のように動作します。

- 同期したデバイスにアクセスするためにNAが使用するSNMPv1またはSNMPv2cコミュニティ文字列を変更した場合、NAは、そのデバイスの変更を管理しているNNMi管理サーバーに通知します。NNMiは、そのデバイスとの通信設定を更新します。

  NNMiは、デバイスの新しいコミュニティ文字列をすぐに使用します。

  > **ヒント:** NAは、デバイスを管理するために使用されるコミュニティ文字列が変更された場合にのみ、NNMiに更新内容を送信します。NAがデバイスに新しいコミュニティ文字列を設定するとき、NNMiは更新を受信しません。

  > **注:** NAは、[**トポロジフィルターノードグループ**]パラメーターによって指定されたノードグループに含まれているすべてのノードの更新をNNMiに送信します。

- 新しいデバイスがNAインベントリに追加された場合、NAは、デバイスの管理に使用するSNMPv1およびSNMPv2cのコミュニティ文字列をNNMiに通知します。

> **注:** 統合により、SNMPv3ユーザーがNAからNNMiに伝達されることはありません。

デフォルトでは、SNMPコミュニティ文字列の伝達は無効になっています。SNMPコミュニティ文字列の伝達を有効にするには、[NA/NNMi統合SNMPコミュニティ文字列伝達]イベントルールのルールステータスをアクティブに設定します。詳細については、「NAイベントルールの有効化」(42ページ)を参照してください。

HPE NNMi–HPE NA統合のNAイベントルール

NAイベントルールでは、NAがNNMi管理サーバーと通信する方法を定義します。NAコンソールの [**イベントの通知とリスポンスルール**] ページ ([**管理者**] > [**イベントの通知とリスポンスルール**]) でこれらのイベントルールにアクセスします。

注意: これらのイベントルールをNAから削除しないでください。これらのイベントルールは、このドキュメントの別の場所で指示されている場合にのみ変更してください。

統合により、NAでは以下のイベントルールが定義されます。

- NA/NNMi統合サービス停止中

  特定のNAタスクが開始すると、統合によってNNMiの同期デバイスが [サービス停止中] 管理モードに設定されます。NAタスクが完了すると、統合によってNNMiのデバイスが以前の管理モードに設定されます。

  このイベントルールでは、NAは、そのデバイスを管理しているNNMi管理サーバーとのみ通信します。

  NAの [**システム管理設定 - NA/NNMi統合**] ページの [**デバイスをサービス停止中にするタスク**] フィールドで、このイベントルールを設定します。このイベントルールを有効または無効にして、この機能を有効または無効にします。

  このイベントルールのデフォルトの必須設定では、[**以下のイベントが発生するとき**] フィールドで、以下のイベントが選択されています。

  - タスク完了
  - タスク開始

  詳細については、「デバイス設定中のネットワーク管理の無効化」(39ページ)を参照してください。

- NA/NNMi統合再検出ホスト

  同期NAデバイスの設定が変更されると、NAはNNMiによるデバイス再検出を要求します。

  このイベントルールでは、NAは、そのデバイスを管理しているNNMi管理サーバーとのみ通信します。

  [**システム管理設定 - NA/NNMi統合**] ページの [**NNMiに構成ポーリングを要求するタスク**] フィールドで、このイベントルールを設定します。このイベントルールを有効または無効にして、この機能を有効または無効にします。

  このイベントルールのデフォルトの必須設定では、[**以下のイベントが発生するとき**] フィールドで、以下のイベントが選択されています。

  - デバイス設定の変更

  詳細については、「NAからのNNMiノード設定ポーリングのトリガー」(38ページ)を参照してください。

- NA/NNMi統合SNMPコミュニティ文字列伝播

  NAで、デバイスにアクセスするためのコミュニティ文字列が変更された場合、NAからNNMiにそのコミュニティ文字列が送信されます。

  このイベントルールでは、NAは、そのデバイスを管理しているNNMi管理サーバーとのみ通信します。

  このイベントルールを有効または無効にして、この機能を設定します。

  このイベントルールのデフォルトの必須設定では、[**以下のイベントが発生するとき**] フィールドで、以下のイベントが選択されています。

- デバイスパスワードの変更
- 最後に使用したデバイスパスワードの変更

詳細については、「NAへのデバイスコミュニティ文字列の変更の伝達」(40ページ)を参照してください。

- SNMPトラップによるNA/NNMi統合 (NNMiサーバー)

  同期NAデバイスで特定のNAイベントが発生した場合、NAからNNMiにSNMPトラップが送信されます。HPE NNMi–HPE NA統合により、統合に含まれるNNMi管理サーバーごとに、このイベントルールのコピーが1つ作成されます。

  複数のNNMi管理サーバーでデバイスを管理している場合、NAにより、そのNNMi管理サーバーのイベントルールの設定に従って、それらのNNMi管理サーバーごとに個別にSNMPトラップが形成されます。

  各NNMi管理サーバーのイベントルールを変更して、この機能を設定します。各NNMi管理サーバーのこのイベントルールを有効または無効にして、この機能を有効または無効にします。

  デフォルトでは、[**以下のイベントが発生するとき**] フィールドで、以下のイベントが選択されています。

  - デバイス追加
  - デバイス設定の変更

  詳細については、「NNMiへのSNMPトラップの送信」(37ページ)を参照してください。

- デバイス追加のNA/NNMiトポロジ同期

  NAインベントリに新しいデバイスが追加されると、NAからNNMiにデバイスの検出ヒントが送信されます。

  このイベントルールは、1つのNNMi管理サーバーのみがNAと統合される場合にのみ適用されます。

  このイベントルールはデフォルトで無効になっています。このイベントルールを有効または無効にして、この機能を設定します。

  このイベントルールのデフォルトの必須設定では、[**以下のイベントが発生するとき**] フィールドで、以下のイベントが選択されています。

  - デバイス追加

  NNMiマルチテナント環境では、このイベントルールを有効にしないでください。詳細については、「NAインベントリの同期のタイミング」(28ページ)を参照してください。

- デバイス削除のNA/NNMiトポロジ同期

  NAインベントリから同期デバイスが削除されると、NAにより、NNMiインベントリからこのデバイスを削除する要求が送信されます。

  このイベントルールでは、NAは、そのデバイスを管理しているNNMi管理サーバーとのみ通信します。

  このイベントルールを有効または無効にして、この機能を設定します。

  このイベントルールのデフォルトの必須設定では、[**以下のイベントが発生するとき**] フィールドで、以下のイベントが選択されています。

  - デバイス削除

NAイベントルールの有効化

NAイベントルールを有効にするには、以下の手順を実行します。

1. NAコンソールで、[イベントの通知とリスポンスルール] ページ (**[管理者] > [イベントの通知とリスポンスルール]**) を開きます。
2. NAイベントルールの行で、[**編集**] をクリックします。

3. [イベントの通知とリスポンスルールを編集] ページで、[**ルールステータス**] を [アクティブ] に設定します。

   注: イベントルール設定のほかの設定は変更しないでください。

4. [**保存**] をクリックします。

NAイベントルールの無効化

NAイベントルールを無効にするには、以下の手順を実行します。

1. NAコンソールで、[イベントの通知とリスポンスルール] ページ (**[管理者] > [イベントの通知とリスポンスルール]**) を開きます。
2. NAイベントルールの行で、[**編集**] をクリックします。
3. [イベントの通知とリスポンスルールを編集] ページで、[**ルールステータス**] を [アクティブでない] に設定します。

   注: イベントルール設定のほかの設定は変更しないでください。

4. [**保存**] をクリックします。

HPE NNMi–HPE NA統合を最大限に活用するためのシナリオ例

多くのネットワーク管理シナリオにおいて、エンドツーエンドのネットワーク管理のためにHPE NNMi–HPE NA統合が活用されています。この章では、統合の利点を示すいくつかのシナリオ例について説明します。NNM iSPIsが1つ以上必要になるシナリオもあります。「表4　シナリオ例」(44ページ)に、シナリオ例および各シナリオを有効にするためのNNMiおよびNAの最小ライセンスタイプを示します。

表4　シナリオ例

シナリオ	必要なNNMiライセンス	必要なNAライセンス
「シナリオ1:非コンプライアンスデバイス変更を識別して修正する」(45ページ)	Premium	Ultimate
「シナリオ2:ネットワーク障害問題をトラブルシューティングする」(48ページ)	Premium	Premium
「シナリオ3:デバイス設定の変更後にネットワークを通過するトラフィックフローを検証する」(50ページ)	Ultimate	Premium
「シナリオ4:IPv4アドレスを対応するIPv6アドレスに再割り当てする」(52ページ)	Premium	Premium
「シナリオ5:ネットワークのコンテキストからアプリケーションのパフォーマンス問題をトラブルシューティングする」(54ページ)	Ultimate	Premium
「シナリオ6:ベースラインデータを使用してシステム使用率の異常を識別する」(56ページ)	Ultimate	Premium
「シナリオ7:エラーレートと使用率の問題を識別して修正する」(58ページ)	Premium	Premium

シナリオ1:非コンプライアンスデバイス変更を識別して修正する

不適切なデバイス設定は、ネットワーク問題の一般的な原因です。HPE NNMi–HPE NA統合では、非適合設定のデバイスが存在しないかどうかネットワークを監視し、デバイス設定がこの期待される設定外になっている場合に通知を生成することができます。HPE NNMi–HPE NA統合には、現在のデバイス設定と前のデバイス設定を比較したり、デバイスをリセットして前の設定を使用したりするためのツールが用意されています。

HPE NNMi–HPE NA統合なしのプロセス

この例では、デバイスに対して無権限での設定変更が行われます。デバイス設定変更について知らせる自動通知機能がない場合は、ネットワークオペレーターがデバイスの設定に誤りがあることを識別する必要があります。通常、変更に気付くのは、問題が発生したときか、手動での設定監査が実行されたときのみです。この時点で、ネットワークオペレーターは以下の手順を実行します。

1. デバイスを特定し、設定管理システムにおける変更点を調べます。
2. マニュアルで指定されている設定とそのデバイスの設定を比較して調べ、その設定の変更がコンプライアンス範囲外にあることを確認します。
3. 正しい設定を再作成するか、それをデバイスに復元します。
4. デバイスが正しく設定されたことを検証します。

HPE NNMi–HPE NA統合ありのプロセス

このシナリオでは、以下の製品の機能を使用します。

- NNMi
- NA

統合シナリオの前提条件

- デバイスは、NNMiトポロジとNAインベントリに含まれている必要があります。
- 「syslogメッセージをNAに送信するようにデバイスを設定する」(46ページ)。
- NAデバイス設定ポリシーをデバイスに適用する必要があります。ポリシールールには自動修正スクリプトが含まれています。
- NAでワークフロー承認が有効になっている必要があります。
- NNMiオペレーターには、NAでデバイス設定を表示および変更する権限が必要です。
- 「NA SNMPトラップインシデントのカスタマイズ」(46ページ)。
- 「デバイスの設定変更時にポリシーコンプライアンスチェックタスクを実行するようにNAを設定する」(46ページ)。
- 「ポリシー適合チェックに不合格になった場合にSNMPトラップをNNMiに送信するようNAを設定する」(47ページ)。

syslogメッセージをNAに送信するようにデバイスを設定する

1. NAコンソールで、**[タスク] > [タスクの新規作成] > [Syslogの構成]** をクリックします。
2. [タスク/テンプレートの新規作成 – Syslogの構成] ページで、以下の手順を実行します。
   a. [適用先] をデバイスに設定します。
   b. [スケジューリングオプション] で、[繰り返しオプション] を [定期的] に設定して、適切な間隔を指定します。
   c. [**保存**] をクリックします。

NA SNMPトラップインシデントのカスタマイズ

NNMiコンソールでは、NASnmpTrapv1およびNASnmpTrapv2インシデント設定により、NAが送信したSNMPトラップが、NNMiで表示して処理することができるインシデントに変換されます。

NAによってNNMiに送信されたすべてのトラップがNNMiコンソールの重要なインシデントビューに表示されるようにする場合は、NASnmpTrapv1およびNASnmpTrapv2インシデント設定が根本原因となるように設定します。

注: このアクションにより、内容に関係なくすべてのNAトラップが根本原因となるように設定されます。

NNMiコンソールで、NASnmpTrapv1およびNASnmpTrapv2インシデント設定を根本原因となるように編集します。この変更により、NAによってNNMiに送信されるすべてのトラップは、NNMiコンソールの重要なインシデントビューに表示されるように設定されます。

以下の手順を実行します。

1. NNMiコンソールの [設定] ワークスペースで、**[インシデント] > [SNMPトラップの設定]** をクリックします。
2. [**根本原因**] チェックボックスをオンにするように、NASnmpTrapv1およびNASnmpTrapv2インシデント設定のそれぞれを編集します。

デバイスの設定変更時にポリシーコンプライアンスチェックタスクを実行するようにNAを設定する

NAコンソールの [イベントの通知とリスポンスルール] ページで、デバイスの設定が変更された場合にはいつでもポリシーへのコンプライアンスをチェックする新規ルールを作成します。

1. NAコンソールで、**[管理] > [イベントの通知とリスポンスルール]** をクリックします。
2. [イベントの通知とリスポンスルール] ページの先頭にある、[**イベントの通知とリスポンスルールの新規作成**] リンクをクリックします。
3. [イベントの通知とリスポンスルール] ページで、以下の手順を実行します。
   a. ルール名を入力します。
   b. [このアクションを実行] を [**タスクの実行**] に設定します。
   c. [以下のイベントが発生するとき] を [**デバイス構成の変更**] に設定します。
   d. [次にこのタスクを実行する] を [**ポリシーコンプライアンスチェック**] に設定します。
4. [新規タスク/テンプレート - ポリシーコンプライアンスチェック] ページで、[**完了**] をクリックします。
5. [イベントの通知とリスポンスルールを編集] ページで、[**保存**] をクリックします。

ポリシー適合チェックに不合格になった場合にSNMPトラップをNNMiに送信するようNAを設定する

NAコンソールの[イベントの通知とリスポンスルール]ページで、ポリシー非コンプライアンスイベントが発生した場合にSNMPトラップを送信するように[SNMPトラップによるNA/NNMi統合]ルールを更新します。

1. NAコンソールで、**[管理] > [イベントの通知とリスポンスルール]**をクリックします。
2. [イベントの通知とリスポンスルール]ページで、[SNMPトラップによるNA/NNMi統合]ルールを見つけ、この行の[**編集**]リンクをクリックします。
3. [イベントの通知とリスポンスルールを編集]ページで、以下の手順を実行します。
   a. [以下のイベントが発生するとき]リストで、[**ポリシーに非準拠です**]が選択されていることを確認します。
   b. 必要に応じて、この行を**Ctrl**キーを押しながらクリックして選択リストに追加します。
   c. SNMPバージョンとして設定されている値を確認し、必要に応じて変更してください。
   d. [**保存**]をクリックします。

統合シナリオの概要

シナリオの前提条件を満たした後は、以下のようにしてHPE NNMi–HPE NA統合を使用できます。

1. NAは、syslogイベント(または別の変更トリガー)を受信し、新しい設定を収集し、新しい設定でコンプライアンスチェックを自動的に実行します。
2. NAは、非コンプライアンスについて記述したSNMPトラップをNNMiに送信します。NNMiは、このトラップを[重要な未解決インシデント]ビューに表示します。
3. 分析ペインのNNMiインシデントから[**ノードポリシーコンプライアンス**]タブを開き、デバイスの設定が非コンプライアンスな場合に適用するポリシーを指定します。
4. NNMiインシデントの分析ペインで[**ノード設定の履歴**]タブを開き、次に最新行の[**前と比較**]をクリックして、現在のデバイス設定と前のデバイス設定の比較を表示します。
5. NAコンソールで、デバイスの自動修正タスクを承認します。

   あるいは、デバイスに接続してデバイス設定を編集します。
6. NAで自動修正タスクが実行され、新しい設定が収集されます。次にNAは、自動的に新しい設定のコンプライアンスをチェックします。

利点

このシナリオにおいて、HPE NNMi–HPE NA統合には以下の利点があります。

- 操作の効率が高まる。
- 変更が自動検出される。
- コンプライアンスが自動的にチェックされる。
- 設定とコンプライアンスを1つのインシデントビューで確認することができ、それによりMTTRが短縮される。
- セキュリティとサービス可用性が向上し、それによりROIが向上する。

シナリオ2:ネットワーク障害問題をトラブルシューティングする

デバイス障害が発生した場合は、障害発生時のデバイスに関する情報を収集することが役立ちます。
HPE NNMi–HPE NA統合では、デバイスを自動的に照会することができ、デバイスの障害インシデントに対応するためのツールを使用できます。

HPE NNMi–HPE NA統合なしのプロセス

この例では、ルーターでのACL設定によって、デスティネーションアドレスが224.0.0.5のトラフィックをブロックします。OSPFはこのアドレスに依存してhelloパケットをブロードキャストするため、ルーターは近隣接続ルーターとの近隣接続を確立できません。自動処理なしの場合は、ルーターに直接接続して設定の調査と更新を行うことを含め、ネットワークオペレーターが徹底的な診断手順を実行することによってネットワーク障害インシデントに対応します。そのプロセスは、以下のような手順になります。

1. ネットワーク障害インシデントを分類します。
2. ルーターにログオンして、インシデントの原因を特定する診断機能を実行します。
3. ルーターで、設定を更新します。
4. ルーターで、設定を目視で検査して正しいことを確認します。

HPE NNMi–HPE NA統合ありのプロセス

このシナリオでは、以下の製品の機能を使用します。

- NNMi
- NA

統合シナリオの前提条件

- デバイスは、NNMiトポロジとNAインベントリに含まれている必要があります。
- デバイスは、NNMi管理サーバーにトラップを送信するように設定されている必要があります。
- OSPFトラップがデバイスで有効になっている必要があります。
- NNMiオペレーターには、NAでデバイス設定を表示および変更する権限が必要です。

OSPFNbrStateChangeインシデントの有効化

NNMiコンソールで、OSPFNbrStateChangeインシデント設定を有効にして、NA診断をトリガーするようにこのインシデントタイプを設定します。

1. NNMiコンソールの[設定]ワークスペースで、**[インシデント] > [SNMPトラップの設定]**をクリックします。
2. OSPFNbrStateChangeインシデントの設定を開きます。
3. **[有効にする]**チェックボックスをオンにします。
4. 設定を保存します。

統合シナリオの概要

シナリオの前提条件を満たした後は、以下のようにしてHPE NNMi–HPE NA統合を使用できます。

1. NNMiは、OSPF近隣接続ノードの状態が変化したことを判別し、そのルーターのOSPFNbrStateChangeインシデントを生成します。このインシデントによってNAが起動し、そのルーターに関する情報を収集します。
2. NAは、隣接デバイスの表示診断を実行してルーターのOSPF近隣接続ノードを判別し、その診断のタスクIDをNNMi OSPFNbrStateChangeインシデントの属性として保存します。
3. NNMiインシデントから、NAコンソールを起動してOSPF近隣接続ルーターの診断レポートを表示し、ACL設定のエラーを確認します。
4. NAコンソールで、helloパケットを許可するようにOSPF近隣接続ルーターのACLを変更します。
5. (NA Ultimateのみ) この問題の再発を防止するため、このデバイスまたはその他の関連デバイスで問題のあるACLが許可されないようにするNAデバイス設定ポリシーを作成します。このポリシーに対する違反は、「シナリオ1:非コンプライアンスデバイス変更を識別して修正する」(45ページ)で処理します。

利点

このシナリオにおいて、HPE NNMi–HPE NA統合には以下の利点があります。

- 必要な時点で設定データを利用できる。
- 操作の効率が高まる。
- ネットワークの停止時間が短縮される。
- ネットワークのパフォーマンス問題が減少する。
- セキュリティとサービス可用性が向上し、それによりROIが向上する。

シナリオ3:デバイス設定の変更後にネットワークを通過するトラフィックフローを検証する

承認されたデバイス設定変更を完了する業務の一部として、ネットワークエンジニアは、変更によりアプリケーションのトラフィックが改善されたことの証拠を必要とします。HPE NNMi–HPE NA統合では、2つのネットワークデバイス間のトラフィックのグラフを表示できます。ネットワークエンジニアは、デバイス設定を変更する前後のグラフを表示し、変更の有効性を検証することができます。

HPE NNMi–HPE NA統合なしのプロセス

この例の場合、ネットワークエンジニアは、その領域のネットワークの効率を改善することが期待されるデバイスで利用可能なルーティングプロトコルなどを変更して、デバイスの設定を更新することを計画します。ネットワークの自動化なしの場合、ネットワークエンジニアは、時間経過に伴うネットワークトラフィックフローの統計データを収集します。トラフィックフローに影響を与えるような方法でネットワークに変更を加えた後、ネットワークエンジニアは、再びトラフィックフロー情報を収集して、変更によってネットワークトラフィックに悪影響が出ていないことを検証します。そのプロセスは、以下のような手順になります。

1. 一定期間、可能であれば一定間隔で、トラフィックフローデータを収集します。
   a. NetFlowエクスポーターにログオンします。
   b. NetFlowエクスポーターでコマンド (たとえば、show) を実行し、変更するデバイスのNetFlow統計データを観察します。
   c. トラフィック統計情報を記録します。
   d. 一定期間、この手順を繰り返します。
2. トラフィックのルーティングに影響を与えるようにネットワーク設定を変更します。
3. データ収集プロセスを繰り返し行います。
4. ネットワークの変更後にトラフィックが再集中したことを検証するには、ネットワークの変更前後のトラフィックフローデータを比較します。

HPE NNMi–HPE NA統合ありのプロセス

このシナリオでは、以下の製品の機能を使用します。

- NNMi
- NA
- NNMi SPI Performance for Traffic

統合シナリオの前提条件

- デバイスはNNMiトポロジに含まれている必要があります。
- ネットワークエリア内の少なくとも1つのデバイスで、1つのフロープロトコル (NetFlow、sFlow、ipfix、jflowなど) が有効になっている必要があります。

このシナリオ例を有効にするために追加の設定は不要です。

統合シナリオの概要

シナリオの前提条件を満たした後は、以下のようにしてHPE NNMi–HPE NA統合を使用できます。

1. NNMiコンソールで、再構築するネットワーク領域でのトラフィックフローのソースノードとデスティネーションノードを表すトラフィックパスビューを開きます (**[アクション] > [トラフィックマップ] > [Trafficパスビュー]**)。
2. フロー対応インタフェースを選択し、次に分析ペインで [**パフォーマンス**] タブを開きます。

   ヒント: 比較を行うため、トラフィックグラフの画面キャプチャを取得します。

3. トラフィックのルーティングに影響を与えるようにネットワーク設定を変更します。
4. ネットワークの変更後にトラフィックが再集中したことを確認するには、[**パフォーマンス**] タブをリフレッシュして更新されたトラフィックのグラフを表示します。

利点

このシナリオにおいて、HPE NNMi–HPE NA統合には以下の利点があります。

- トラフィックフローデータの収集プロセスが簡素化される。
- 転記エラーのリスクがない。
- トラフィックフローを視覚化できる。

シナリオ4:IPv4アドレスを対応するIPv6アドレスに再割り当てする

IPv4ネットワークのアドレスを再割り当てしてIPv6アドレスを使用するプロセスを手動で行うと、時間がかかり、誤りが入り込みやすくなります。HPE NNMi–HPE NA統合では、現在使用中のIPv4アドレスの収集と管理対象デバイス上のIPv6アドレスの設定の両方を自動化することができます。

HPE NNMi–HPE NA統合なしのプロセス

この例の場合、ネットワークエンジニアは、各デバイスからIPv4情報を手動で収集し、次にIPv6アドレスを使用して各インタフェースを手動で設定します。そのプロセスは、以下のような手順になります。

1. 各デバイスの現在のIPv4アドレスを確認します。
   a. デバイスにログオンします。
   b. 各インタフェースのIPアドレスを確認し、スプレッドシートファイルに記録します。
2. スプレッドシートファイルで、各IPv4アドレスをIPv6アドレスにマップします。
3. IPv6アドレスで各デバイスを設定します。
   a. デバイスにログオンします。
   b. スプレッドシートファイルを参照しながら、各インタフェースで正しいIPv6アドレスを設定します。
   c. 設定を目視で検査して正しいことを確認します。

HPE NNMi–HPE NA統合ありのプロセス

このシナリオでは、以下の製品の機能を使用します。

- NNMi
- NA

統合シナリオの前提条件

- アドレスを再割り当てするネットワークの対象エリアは、NNMiトポロジとNAインベントリに含まれている必要があります。
- 利用可能なIPv6アドレスの一覧を作成します。

統合シナリオの概要

シナリオの前提条件を満たした後は、以下のようにしてHPE NNMi–HPE NA統合を使用できます。

1. NNMiコンソールで [IPアドレス] インベントリビューをフィルターして、アドレスを再割り当てするネットワークの領域のみを表示し、そのリストをカンマ区切り値 (CSV) 形式でエクスポートします。
2. そのCSVファイルをスプレッドシートアプリケーションで開いた状態で、各IPv4アドレスを1つのIPv6アドレスにマップし、そのスプレッドシートファイルをCSV形式で保存します。
3. デバイス上で新しいIPv6アドレスを設定するスクリプトを作成します。

4. NAコンソールで、適 切 な時 刻 に適 切 なデバイスに対 してそのスクリプトを実 行 する、スケジュールされたタスクを割 り当 てます。
5. NNMiコンソールで、[IPアドレス] インベントリビューをCSV形 式 ファイルにエクスポートします。
6. 設 定 したIPv6アドレスと予 定 されているIPv6アドレスを比 較 します。

利 点

このシナリオにおいて、HPE NNMi–HPE NA統 合 には以 下 の利 点 があります。

- データ収 集 と設 定 のプロセスが自 動 化 される。
- アドレスの再 割 り当 てでの誤 りのリスクが抑 えられる。

シナリオ5:ネットワークのコンテキストからアプリケーションのパフォーマンス問題をトラブルシューティングする

重要なネットワークインタフェース間の予期せぬネットワークトラフィックは、アプリケーションのパフォーマンス問題の一般的な原因です。HPE NNMi–HPE NA統合では、重要なインタフェースの使用率を監視し、使用率が許容レベルを超えた場合には通知を生成することができます。HPE NNMi–HPE NA統合には、重要なインタフェースで許可されていないトラフィックをブロックするデバイス設定を更新するためのツールが用意されています。

HPE NNMi–HPE NA統合なしのプロセス

この例では、許可されていないトラフィックがネットワークインタフェースの帯域幅のかなりの部分を消費し、そのインタフェースを使用しているアプリケーションの応答時間が遅くなります。トラフィックの増加を知らせる自動通知機能なしの場合、ネットワークオペレーターは、アプリケーションユーザーがアプリケーションに対する不満を訴えるまで、トラフィックの増加に気付かないのが普通です。この時点で、ネットワークオペレーターは以下の手順を実行します。

1. アプリケーションが使用する通信経路とサーバーを特定します。
2. tracerouteを実行して、アプリケーショントラフィックの経路指定インフラストラクチャを特定します。
3. 経路指定インフラストラクチャ内の各ルーターを調べます。
   a. ルーターにログオンします。
   b. ルーティングテーブルを調べ、アプリケーション経路に関連付けられているインタフェースを特定します。
   c. そのルーターについて全体として、およびアプリケーション経路に関係する個々のインタフェースについて、パフォーマンスメトリックスを収集します。
4. アプリケーション経路に配備されているsnifferまたはプローブツールからトラフィックメトリックスを収集します。このデータを調べて、使用率が高いルーター全体にわたってターゲットのアプリケーショントラフィックを妨害している異常または許可されていないトラフィックを識別します。
5. 適切なネットワークデバイスにログオンして、許可されていないトラフィックをブロックするか、代替の、使用率の低いルーターを通過するようにアプリケーショントラフィックの経路指定を再度行います。

HPE NNMi–HPE NA統合ありのプロセス

このシナリオでは、以下の製品の機能を使用します。

- NNMi
- NA
- NNM iSPI Performance for Metrics
- NNMi SPI Performance for Traffic

統合シナリオの前提条件

- デバイスは、NNMiトポロジとNAインベントリに含まれている必要があります。
- インタフェースのパフォーマンス監視とインタフェース使用率のしきい値が、NNMiで有効にされ、設定されている必要があります。

- ネットワークエリア内の少なくとも1つのデバイスで、1つのフロープロトコル(NetFlow、sFlow、ipfix、jflowなど)が有効になっている必要があります。
- 「InterfaceInputUtilizationHighおよびInterfaceInputUtilizationLowインシデントの有効化」(55ページ)。

InterfaceInputUtilizationHighおよびInterfaceInputUtilizationLowインシデントの有効化

NNMiコンソールで、InterfaceInputUtilizationHighおよびInterfaceInputUtilizationLowインシデントの設定を有効にします。

1. NNMiコンソールの[設定]ワークスペースで、**[インシデント] > [管理イベントの設定]**をクリックします。
2. InterfaceInputUtilizationHighインシデントの設定を開きます。
3. [**有効にする**]チェックボックスをオンにします。
4. 設定を保存します。
5. InterfaceInputUtilizationLowインシデントの設定について、「InterfaceInputUtilizationHighインシデントの設定を開きます。」(55ページ)から「設定を保存します。」(55ページ)を繰り返します。

統合シナリオの概要

シナリオの前提条件を満たした後は、以下のようにしてHPE NNMi–HPE NA統合を使用できます。

1. NNMiは、重要なネットワークインタフェースについて、インタフェースの使用率が許容境界を超えたことを示す管理イベントインシデントを生成します。
2. トラフィックインベントリでNNMiインシデントのソースインタフェースを見つけ、分析ペインで[**上位アプリケーション - 受信**]タブを表示します。

   このタブには、トラフィックの大半を生成しているアプリケーションを示す円グラフが表示されます。このグラフにより、権限のないアプリケーションからの競合トラフィックが判明します。
3. NNMiインシデントから、NAコンソールを起動してデバイスの詳細ページを開きます([**HPE NAデバイス情報の表示**]を使用します)。
4. NAコンソールのデバイスの詳細ページから、ACL行のバッチ挿入タスクを実行して複数のACLを複数のデバイスに変更し、許可されていないトラフィックをブロックします。
5. そのインタフェース全体のネットワークトラフィックが許容レベルに戻り、NNMiコンソールでインタフェース使用率インシデントが自動的に終了します。

利点

このシナリオにおいて、HPE NNMi–HPE NA統合には以下の利点があります。

- ネットワーク使用率の問題を見越した管理により、ミッションクリティカルなアプリケーションでのサービスレベルが高められる。
- ネットワーク使用率問題の検出、トラブルシューティング、および原因の修正を一式のツールで実行することができ、これらによりMTTRが短縮される。
- ネットワーク全体にわたり、重要なサービスに影響するネットワーク設定問題を事前に修正できる。
- パフォーマンスおよびトラフィックデータが自動的に収集される。
- 許可されていないトラフィックを検出してブロックする。

シナリオ6:ベースラインデータを使用してシステム使用率の異常を識別する

不規則なトラフィックパターンは、ネットワークの使用状態が不適切であることを示す可能性があります。
HPE NNMi–HPE NA統合では、通常のトラフィックパターンを判別し、トラフィックパターンが通常の範囲外の場合には通知を生成することができます。

HPE NNMi–HPE NA統合なしのプロセス

この例の場合、会社のお客様は、会社のメインWebサイトにインターネットからアクセスするときの遅さについて不満を訴えます。この時点で、ネットワークオペレーターは以下の手順を実行します。

1. Webサーバーと外部ルーターのネットワーク使用率を調べ、使用率が高いことを確認します。
2. snifferを使用し、パフォーマンスツールを実行し、ファイアウォールのログを調べて遅さの原因を特定します。
3. そのWebサイトのURLが多くのHTTP要求とともにロードされていることを確認します。要求はWebサイトでの攻撃のように見えます。
4. Webサイトへのすべての接続を終了し、そのWebサイトを完全に停止させます。
5. その状況での支援を得るため、セキュリティのスペシャリストに連絡します。

HPE NNMi–HPE NA統合ありのプロセス

このシナリオでは、以下の製品の機能を使用します。

- NNMi
- NA
- NNM iSPI Performance for Metrics
- NNMi SPI Performance for Traffic

統合シナリオの前提条件

- デバイスは、NNMiトポロジとNAインベントリに含まれている必要があります。
- NNMi SPI Performance for Trafficサイトは、Webサイトの場所のIPアドレスに対して定義されている必要があります。

統合シナリオの概要

シナリオの前提条件を満たした後は、以下のようにしてHPE NNMi–HPE NA統合を使用できます。

1. NNMiは、Webサイトへのパスに含まれるインタフェースでの使用率に関して、通常の状態からの逸脱を示す管理イベントインシデントを生成します。
2. NNMi SPI Performance for Trafficは、Webサイトの場所を表すNNMi SPI Performance for Trafficサイトに大量のHTTPトラフィックが向かっていることを示す管理インシデントを生成します。
3. NNMi SPI Performance for Trafficインシデントから、分析ペインの[**上位アプリケーション - 受信**]タブを開いてインシデントで特定されるインタフェースを表示します。

   このタブには、トラフィックの大半を生成しているアプリケーションを示す円グラフが表示されます。

4. [トラフィック分析] ワークスペースのトラフィックレポートインタフェーステーブルで、NNMi SPI Performance for Trafficインシデントに示されているインタフェースをダブルクリックします。

   [**上位5のソース**] および [**上位5のデスティネーション**] タブに、限られたホストにおけるインタフェースの高い使用率が表示されます。
5. そのWebサイトのURLが多くのHTTP要求とともにロードされていることを確認します。要求はWebサイトでの攻撃のように見えます。
6. NNMiインシデントから、NAコンソールを起動してデバイスの詳細ページを開きます([**HPE NAデバイス情報の表示**] を使用します)。
7. NAコンソールのデバイスの詳細ページからACL行のバッチ挿入タスクを実行して、Webサーバーをホストしているデバイスの ACLを変更し、攻撃元からのトラフィックを拒否します。
8. そのインタフェース全体のネットワークトラフィックが許容レベルに戻り、NNMiコンソールでインタフェース使用率インシデントが自動的に終了します。

利点

このシナリオにおいて、HPE NNMi–HPE NA統合には以下の利点があります。

- ネットワーク使用率の問題を見越した管理により、お客様の満足度を高めることができる。
- ネットワーク使用率問題の検出、トラブルシューティング、および原因の修正を一式のツールで実行することができ、これらによりMTTRが短縮される。
- 許可されていないトラフィックを検出してブロックする。
- 高品質なサービスを提供する。

シナリオ7:エラーレートと使用率の問題を識別して修正する

インタフェースでのエラーレートが高いと、通常、そのインタフェースに接続されているワークステーション、サーバー、またはその他のデバイスの動作が著しく遅くなります。HPE NNMi–HPE NA統合では、インタフェースを監視し、エラーレート、使用率、またはその両方が定義済みのしきい値を超えた場合には通知を生成することができます。

HPE NNMi–HPE NA統合なしのプロセス

この例の場合、重要なアプリケーションの応答が遅くなり、最終的にタイムアウトしますが、問題は自然に解消されます。この障害はピーク使用期間中に断続的に発生するため、アプリケーションをより処理能力の高いサーバーに移動します。この変更を行っても、アプリケーションのタイムアウトは回避されません。最終的に、全二重の不一致が発見されます。全二重設定を修正すると、タイムアウト問題が解決します。

HPE NNMi–HPE NA統合ありのプロセス

このシナリオでは、以下の製品の機能を使用します。

- NNMi
- NA
- NNM iSPI Performance for Metrics

統合シナリオの前提条件

- デバイスは、NNMiトポロジとNAインベントリに含まれている必要があります。
- インタフェースのパフォーマンス監視としきい値が、NNMiで有効にされ、設定されている必要があります。
- 「InterfaceInputErrorRateHighおよびInterfaceInputUtilizationHighインシデントの有効化」(58ページ)。

InterfaceInputErrorRateHighおよびInterfaceInputUtilizationHighインシデントの有効化

NNMiコンソールで、InterfaceInputErrorRateHighおよびInterfaceInputUtilizationHighインシデントの設定を有効にします。

1. NNMiコンソールの[設定]ワークスペースで、**[インシデント] > [管理イベントの設定]**をクリックします。
2. InterfaceInputErrorRateHighインシデントの設定を開きます。
3. **[有効にする]**チェックボックスをオンにします。
4. 設定を保存します。
5. InterfaceInputUtilizationHighインシデントの設定について、「InterfaceInputErrorRateHighインシデントの設定を開きます。」(58ページ)から「設定を保存します。」(58ページ)を繰り返します。

統合シナリオの概要

シナリオの前提条件を満たした後は、以下のようにしてHPE NNMi–HPE NA統合を使用できます。

1. NNMiは、インタフェースでのエラーレートが高いことを示す管理イベントインシデントを生成します。インシデントの詳細タブの接続テーブルは、全二重の不一致を示します。
2. NNMiコンソールで、接続の両端にあるルーターのノードの詳細ページを開きます。各分析ペインで、[**ノード設定の履歴**] タブを開き、次に最新行の [**前と比較**] をクリックして、現在のデバイス設定と前のデバイス設定の比較を表示します。このインタフェースで設定されているデュプレックス、およびその設定が最近変更されたかどうかを確認します。
3. 修飾インタフェース名によってグループ化されたLAN衝突率メトリックスおよびLAN衝突カウントメトリックスについての、NNM iSPI Performance for Metricsインタフェースヘルスレポートを開きます。また、修飾インタフェース名によってグループ化されたLAN FCSエラーレートメトリックスおよびLAN FCSエラーカウントメトリックスについてのNNM iSPI Performance for Metricsインタフェースヘルスレポートも開きます。

   この組み合わせレポートには、接続の一方の側にエラーが多いが、他方の側には衝突数が多いことが示されます。この情報は、全二重の不一致を示すものです。
4. NNMiインシデントから、NAコンソールを起動してスイッチ設定を更新します。
5. NNM iSPI Performance for Metricsのレポートでインタフェースのパフォーマンス履歴を調べ、エラー問題が発生しなくなったことを検証します。

利点

このシナリオにおいて、HPE NNMi–HPE NA統合には以下の利点があります。

- アプリケーションのパフォーマンスに影響が出る前に、ネットワークの設定誤りを事前に検出できる。
- ネットワーク使用率問題の検出、トラブルシューティング、および原因の修正を一式のツールで実行することができ、これらによりMTTRが短縮される。

HPE NNMi–HPE NA統合の管理

この章では、HPE NNMi–HPE NA統合の管理の情報について説明します。内容は以下のとおりです。

HPE NNMi–HPE NA統合の変更

1. NAコンソールで、[**管理設定 - NA/NNMi統合**] ページを開きます (**[管理者] > [管理設定] > [NA/NNMi統合]**)。
   a. 該当するように値を変更します。このフォームのフィールドの詳細については、以下のリファレンスを参照してください。
      - 「NAからのNNMiノード設定ポーリングのトリガー」(38ページ)
      - 「デバイス設定中のネットワーク管理の無効化」(39ページ)
   b. ページの下にある [**保存**] をクリックします。
2. オプション。NAコンソールで、以下の参考資料の説明に従って、[SNMPトラップによるNA/NNMi統合 (NNMiサーバー)] イベントルールおよび [NA/NNMi統合 SNMPコミュニティ文字列伝達] イベントルールを変更します。
   - 「NNMiへのSNMPトラップの送信」(37ページ)
   - 「NAへのデバイスコミュニティ文字列の変更の伝達」(40ページ)
3. NNMiコンソールで、[**HPE NNMi–HPE NAの統合設定**] フォームを開きます (**[統合モジュールの設定] > [HPE NA]**)。
   a. 該当するように値を変更します。このフォームのフィールドの詳細については、「[HPE NNMi–HPE NAの統合設定] フォームのリファレンス」(64ページ)を参照してください。
   b. フォームの上部にある [**統合の有効化**] チェックボックスがオンであることを確認し、フォームの下部にある [**送信**] をクリックします。

HPE NNMi–HPE NA統合の無効化

1. NNMiコンソールで、[**HPE NNMi–HPE NAの統合設定**] フォームを開きます (**[統合モジュールの設定] > [HPE NA]**)。
2. フォームの上部にある [**統合の有効化**] チェックボックスをオフにし、フォームの下部にある [**送信**] をクリックします。これで、統合アクションを使用できなくなります。
3. オプション。今後統合を再度有効化しない場合は、NAコンソールで、[**イベントの通知とリスポンスルール**] ページからNAおよびNNMiのイベントルールを削除します (**[管理者] > [イベントの通知とリスポンスルール]**)。

HPE NNMi–HPE NA統合のトラブルシューティング

このセクションでは以下の内容について説明します。

統合をテストする

注: 統合が過去に正常に動作していた場合は、NNMiまたはNAのユーザーパスワードなどの一部の設定が最近変更された可能性があります。この手順全体を段階的に実行する前に、「[HPE NNMi–HPE NAの統合設定]フォームのリファレンス」(64ページ)で説明されているように統合設定を更新してください。

1. NNMiコンソールで、[**HPE NNMi–HPE NAの統合設定**]フォームを開きます(**[統合モジュールの設定] > [HPE NA]**)。

   このフォームのフィールドの詳細については、「[HPE NNMi–HPE NAの統合設定]フォームのリファレンス」(64ページ)を参照してください。
2. 統合のステータスを確認するには、[**HPE NNMi–HPE NAの統合設定**]フォームで、フォームの下にある[**送信**]をクリックします(設定の変更は行いません)。

   ヒント: 正常に動作すると、この手順によってNNMiとNAの間で完全なインベントリ同期が開始されます。

   新しいウィンドウにステータスメッセージが表示されます。

   メッセージにNAコアサーバーへの接続の問題が示されている場合、NNMiとNAは通信できていません。この手順の「NA資格情報の正確性とアクセスレベルを確認するには、[HPE NNMi–HPE NAの統合設定]フォームの[NAユーザー]の資格情報を使用して、NAコンソールにログオンします。」(61ページ)を続行します。
3. NA資格情報の正確性とアクセスレベルを確認するには、[**HPE NNMi–HPE NAの統合設定**]フォームの[**NAユーザー**]の資格情報を使用して、NAコンソールにログオンします。

   NAコンソールにログオンできない場合は、NA管理者に連絡してログオン資格証明を確認してください。
4. NAコアサーバーへの接続が正しく設定されていることを確認するには、NNMi管理サーバーのWebブラウザーで、以下のURLを入力します。

   http://<naserver>:<naport>/soap

   以下のように、変数が[**HPE NNMi–HPE NAの統合設定**]フォームの値に関係する場合:

   - <naserver>は[**NAホスト**]の値です。
   - <naport>は[**NAポート**]の値です。

   NA Webサーバーが指定されたサーバーとポートで実行している場合、NAコアサーバーは以下のようなメッセージで応答します。

   ```
   NAS SOAP API:Only handles HTTP POST requests
   ```

- 想定されるメッセージが表示されたら、「NNMiへの接続が正常に設定されていることを確認します。」(62ページ)に進みます。
- エラーメッセージが表示されたら、NAサーバーへの接続は正しく設定されていません。NA管理者に連絡してNA Webサービスへの接続情報を確認してください。期待されるメッセージが表示されるまで、NAへの接続のトラブルシューティングを続けます。

5. NNMiへの接続が正常に設定されていることを確認します。

   注: この手順の「NNMiコンソールで、[HPE NNMi–HPE NAの統合設定] フォームを開きます ([統合モジュールの設定] > [HPE NA])。」(61ページ)でNNMiコンソールに接続するために、この手順で説明してある情報を使用した場合は、NNMiコンソールに再接続する必要はありません。「NNMi管理者に連絡し、Webサービスクライアントロールでの [NNMiユーザー] の値、および対応する [NNMiパスワード] を確認します。」(62ページ)に進みます。

   a. NAコアサーバーのWebブラウザーで、以下のURLを入力します。

      <protocol>://<NNMiserver>:<port>/nnm/

      以下のように、変数が[**HPE NNMi–HPE NAの統合設定**]フォームの値に関係する場合:

      - [**NNMi SSLの有効化**] チェックボックスがオンの場合、<protocol> はhttpsです。
      - [**NNMi SSLの有効化**] チェックボックスがオフの場合、<protocol> はhttpです。
      - <NNMiserver> は [**NNMiホスト**] の値です。
      - <port> は [**NNMiポート**] の値です。

   b. プロンプトが表示されたら、管理者ロールでNNMiユーザーの資格認定を入力します。

      NNMiコンソールが表示されるはずです。NNMiコンソールが表示されない場合は、NNMi管理者に連絡してNNMiへの接続情報を確認してください。NNMiコンソールが表示されるまで、NNMiへの接続のトラブルシューティングを継続します。

      注: 「Webサービスクライアント」ロールを持つユーザーとしてNNMiコンソールにログオンすることはできません。

6. NNMi管理者に連絡し、Webサービスクライアントロールでの [**NNMiユーザー**] の値、および対応する [**NNMiパスワード**] を確認します。
7. この手順の「NAコアサーバーへの接続が正しく設定されていることを確認するには、NNMi管理サーバーのWebブラウザーで、以下のURLを入力します。」(61ページ)と「NNMiへの接続が正常に設定されていることを確認します。」(62ページ)で使用して正常に接続できた値で、[**HPE NNMi–HPE NAの統合設定**] フォームを更新します。また、「NNMi管理者に連絡し、Webサービスクライアントロールでの [NNMiユーザー] の値、および対応する [NNMiパスワード] を確認します。」(62ページ)で使用したNNMiユーザー名とパスワードをこのフォームに再入力します。

   詳細については、「[HPE NNMi–HPE NAの統合設定] フォームのリファレンス」(64ページ)を参照してください。
8. フォームの下部にある [**送信**] をクリックします。
9. 上記を実行してもステータスメッセージにNAコアサーバーへの接続の問題が示される場合は、以下の手順を実行します。
   a. Webブラウザーのキャッシュをクリアします。
   b. Webブラウザーから、すべての保存フォームまたはパスワードデータをクリアします。

c. Webブラウザーウィンドウを完全に閉じてから、もう一度開きます。

d. この手順の「この手順の「NAコアサーバーへの接続が正しく設定されていることを確認するには、NNMi管理サーバーのWebブラウザーで、以下のURLを入力します。」(61ページ)と「NNMiへの接続が正常に設定されていることを確認します。」(62ページ)で使用して正常に接続できた値で、[HPE NNMi–HPE NAの統合設定]フォームを更新します。また、「NNMi管理者に連絡し、Webサービスクライアントロールでの[NNMiユーザー]の値、および対応する[NNMiパスワード]を確認します。」(62ページ)で使用したNNMiユーザー名とパスワードをこのフォームに再入力します。」(62ページ)と「フォームの下部にある[送信]をクリックします。」(62ページ)を繰り返します。

10. 「HPE NNMi–HPE NA統合の使用法」(27ページ)にリストされたアクションの1つを起動して、設定をテストします。

NNMiインベントリから欠落したNAデバイス

注: このセクションの情報は、以下の条件の両方が満たされる場合のみ適用されます。

- 1つのNNMi管理サーバーのみがNAと統合されている。
- [デバイス追加のNA/NNMiトポロジ同期]イベントルールが有効になっている。

NAインベントリのデバイスがNNMiインベントリに表示されない場合、以下の手順を実行します。

1. NNMiノードインベントリを調べて、そのデバイスがインベントリにはあるが、別のノードグループに入っていないかどうかを確認します。

   別のグループに入っている場合、NNMi同期ノードグループの定義を更新して、そのデバイスが含まれるようにします。

2. NNMi IPアドレスのインベントリを調べて、NAで使用されているIPアドレスがNNMiにリストされているかどうかを確認します。

   IPアドレスがNNMiに含まれている場合、どのノードがそのIPアドレスをホストしているかを確認します。このノードは、NAデバイスと同期されている必要があります。NNMiで、NAが検出ヒントとして送信したIPアドレスとは異なる管理アドレスがそのノードに使用されている可能性があります。

3. NNMiインベントリ内ではなく、NAインベントリ内に存在するデバイスを含めるように、NNMi自動検出ルールを変更します。次に、統合を再度有効化します。

   NAは、統合が有効になっている場合に、新しいデバイスがNAインベントリに追加されたときのみ、検出ヒントを送信します。ネットワークの停止中、またはNNMi自動検出ルールが正しく組み込まれる前にデバイスがNAに追加された場合、統合を再度有効化すると、NAは検出ヒントを再送信します。

アプリケーションフェイルオーバーとHPE NNMi–HPE NA統合

NNMi管理サーバーがNNMiアプリケーションフェイルオーバーに参加する場合、HPE NNMi–HPE NA統合では、フェイルオーバーの発生後、新しいNNMi管理サーバーホスト名でNAコアサーバーが再設定されます。統合のユーザーにNNMiアプリケーションフェイルオーバーを意識させないようにしてください。

統合では、NAコアのフェイルオーバーがサポートされません。統合NAコアが別のNAコアにフェイルオーバーする場合、各NNMi管理サーバーの[**HPE NNMi–HPE NAの統合設定**]フォームを新しいNAコアへの接続情報で更新します。

HPE NNMi–HPE NA統合リファレンス

この章では、HPE NNMi–HPE NA統合の参照情報について説明します。内容は以下のとおりです。

HPE NNMi–HPE NA統合で使用されるポート

NNMi管理サーバーでは、HPE NNMi–HPE NA統合で以下のポートが使用されます。

- NNMi Webサービス呼び出しを受信するポート。デフォルトでは80 (非SSL) または443 (SSL) になります。
- NAからSNMPトラップを受信するポート162

NAコアサーバーでは、NA Webサービス呼び出しを受信するためにHPE NNMi–HPE NA統合で以下のポートが使用されます。

- NAがNNMiとは別のコンピューターに存在する場合、このポートは80 (非SSL) または443 (SSL) になります。
- NAがNNMiと同じコンピューターに存在する場合、このポートは8080 (非SSL) または8443 (SSL) になります。

[HPE NNMi–HPE NAの統合設定] フォームのリファレンス

NNMiコンソールの [**HPE NNMi–HPE NAの統合設定**] フォームには、NNMiからNAの通信を設定するためのパラメーターが含まれています。このフォームは、[**統合モジュールの設定**] ワークスペースから使用できます。このフォームの通信パラメーターには、NAコンソールの [NA/NNMi統合] ページにある [統合サーバーリスト] の行が入力されます。

> **注:** 管理者ロールのNNMiユーザーのみが [**HPE NNMi–HPE NAの統合設定**] フォームにアクセスできます。

[**HPE NNMi–HPE NAの統合設定**] フォームは、以下の一般領域に関する情報を収集します。

統合設定に変更を適用するには、[**HPE NNMi–HPE NAの統合設定**] フォームの値を更新し、[**送信**] をクリックします。

NNMi管理サーバー接続

「表5 NNMiコンソールのNNMi管理サーバー情報」(65ページ)に、NAからNNMi管理サーバーに接続するためのパラメーターを示します。これらの値の多くを決定するには、NNMiコンソールセッションを起動するURLを調べます。NNMi管理者と協力し、設定フォームのこのセクションに適切な値を決定します。

表5 NNMiコンソールのNNMi管理サーバー情報

フィールド	説明
NNMi SSL NA SSL	SSL通信の場合は、これらのいずれかのチェックボックスをオンにする前に、「オプション。NNMi WebサービスまたはNA WebサービスとのSSL通信を使用するには、「NNMiとNA間のSSL通信の設定」(19ページ)の説明に従って、NNMiサーバーとNAサーバーの間で証明書を交換します。」(16ページ)で証明書を交換したことを確認します。
NNMiホスト	NNMi管理サーバーの正式な完全修飾ドメイン名。このフィールドは読み取り専用です。 **メモ**: 統合により、以下のファイルのnmsas.server.port.web.httpの値が判断されて、NNMiコンソールに接続するためのポートが選択されます。 • Windowsの場合: %NnmDataDir%\Conf\nnm\props\nms-local.properties • Linuxの場合: $NnmDataDir/conf/nnm/props/nms-local.properties
NNMiユーザー	NNMi Webサービスに接続するためのユーザー名。このユーザーにはNNMi Web Service Clientロールが必要です。 ベストプラクティス: Webサービスクライアントロールを持つNNMiIntegrationユーザーアカウントを作成して使用します。
NNMiパスワード	指定のNNMiユーザーのパスワード。

NAコアサーバー接続

「表6 NNMiコンソールのNAコアサーバー情報」(65ページ)に、NAコアサーバー上のWebサービスに接続するためのパラメーターを示します。NA管理者と協力し、設定フォームのこのセクションに適切な値を決定します。

表6 NNMiコンソールのNAコアサーバー情報

NAコアサーバーパラメーター	説明
NNMi SSL NA SSL	SSL通信の場合は、これらのいずれかのチェックボックスをオンにする前に、「オプション。NNMi WebサービスまたはNA WebサービスとのSSL通信を使用するには、「NNMiとNA間のSSL通信の設定」(19ページ)の説明に従って、NNMiサーバーとNAサーバーの間で証明書を交換します。」(16ページ)で証明書を交換したことを確認します。
NAホスト	NAコアサーバーの完全修飾ドメイン名またはIPアドレス。
NAポート	NA Webサービスへの接続ポート。 デフォルトのNAポートは以下のとおりです。 • 443 - NNMiとは別のコンピューターにあるNAにSSL接続する場合

表6 NNMiコンソールのNAコアサーバー情報 (続き)

NAコアサーバーパラメーター	説明
	• 8443 - NNMiと同じコンピューターにあるNAにSSL接続する場合 • 80 - NNMiとは別のコンピューターにあるNAに非SSL接続する場合 • 8080 - NNMiと同じコンピューターにあるNAに非SSL接続する場合
NAユーザー	NA管理者ロールを持つ有効なNAユーザーアカウント名。 **注:** このユーザー名のパスワードはクリアテキストで渡されます。 ベストプラクティス: NAIntegrationユーザーアカウントを作成して使用します。
NAパスワード	指定のNAユーザーのパスワード。

統合動作

「表7 NNMiコンソールの統合動作情報」(66ページ)には、HPE NNMi–HPE NA統合の動作を設定するためのNNMiコンソールパラメーターを示します。

表7 NNMiコンソールの統合動作情報

パラメーター	説明
トポロジフィルターノードグループ	NAインベントリと同期するノードのセットを含むNNMiノードグループ。統合により、このノードグループのすべてのノードに関する情報がNAインベントリに入力されます。 このNNMi管理サーバーのノードグループのリストからノードグループを選択します。デフォルトの選択は、ネットワーキングインフラストラクチャデバイスノードグループです。 ノードグループが指定されていない場合は、統合により、NNMiインベントリ全体がNAインベントリと同期されます。
トポロジ同期間隔 (時間)	「NNMiとNA間のインベントリ同期」(27ページ)で説明されているように、NNMiがNAとの完全インベントリ同期を実行する頻度。接続チェックのデフォルトの周期は24時間です。 定期インベントリ同期を無効にするには、この値を0に設定します。
NAのデバイスドライバの検出	NA設定の指定。 [**NAのデバイスドライバを検出する**] チェックボックスがオンの場合、NAはNNMiとのインベントリ同期の結果として、NAに追加されたデバイスのデバイスドライバを自動的に検出します。デフォルト設定はオンです。 [**NAのデバイスドライバの検出**] チェックボックスがオフの場合は、デバイスドライバの検出を手動で開始できます。NAインベントリにNNMiインベントリがすでに含まれている場合は、デバイスドライバを再度検出する必要はありません。
NNMiセキュリティグループをNAパーティションにマップします	[**NNMiセキュリティグループをNAパーティションにマップします**] チェックボックスがオンの場合、NNMiからNAに同期されたデバイスは、そのノードを含むNNMiセキュリティグループと同じ名前で常にNAパーティションに追加されるか更新されます。 [**NNMiセキュリティグループをNAパーティションにマップします**] チェックボックスがオフ (デフォルト) の場合、NAインベントリに現在存在しないNNMiノードがNAデフォルトサイ

表7　NNMiコンソールの統合動作情報 (続き)

パラメーター	説明
	トパーティションに追加され、NAインベントリに現在存在するNNMiノードはNAに割り当てられたパーティションに残ります。 [**トポロジフィルターノードグループ**] フィールドでノードグループを指定した場合は、各NNMiセキュリティグループの一部のノードのみが、対応するNAパーティションと同期されます。NNMiインベントリ全体をNAインベントリと同期するには、[**トポロジフィルターノードグループ**] フィールドをオフにします。
NA接続チェック間隔 (時間)	「不整合な状態のレイヤー2接続の特定」(32ページ)の説明に従って、NNMiがNNMiトポロジのすべてのレイヤー2接続のインタフェースデータをNAで確認する頻度。接続チェックのデフォルトの周期は24時間です。 定期接続チェックを無効にするには、この値を0に設定します。
分析ペインデータを表示する最小NNMiロール	NNMi分析ペインにNA情報を表示するためのNNMiアクセスレベル。[**分析ペインデータを表示する最小NNMiロール**] フィールドに有効なオプションは、以下のとおりです。 • 機能を無効にする: NNMi分析ペインでのNAデータの表示をNNMiで無効にします。 • NNMi管理者: 管理者ロールを持つNNMiユーザーにNNMi分析ペインのNAデータが表示されます。 • NNMiレベル2オペレーター: オペレーターレベル2ロールまたは管理者ロールを持つNNMiユーザーにNNMi分析ペインのNAデータが表示されます。 • NNMiレベル1オペレーター: オペレーターレベル1ロール、オペレーターレベル2ロール、または管理者ロールを持つNNMiユーザーにNNMi分析ペインのNAデータが表示されます。 • NNMiゲストユーザー: すべてのNNMiユーザーにNNMi分析ペインのNAデータが表示されます。 詳細については、「NNMi分析ペインのNA情報へのNNMiユーザーアクセスの設定」(68ページ)を参照してください。
分析ペインデータを表示する最小オブジェクトアクセス権限	NNMi分析ペインにNA情報を表示するためのNNMiオブジェクトアクセスレベル。[**分析ペインデータを表示する最小オブジェクトアクセス権限**] フィールドに有効なオプションは、以下のとおりです。 • オブジェクト管理者: NNMiノードに対してオブジェクト管理者権限を持つNNMiユーザーにNNMi分析ペインのNAデータが表示されます。 • オブジェクトオペレーターレベル2: NNMiノードに対してオブジェクトオペレーターレベル2権限またはオブジェクト管理者権限を持つNNMiユーザーにNNMi分析ペインのNAデータが表示されます。 • オブジェクトオペレーターレベル1: NNMiノードに対してオブジェクトオペレーターレベル1権限、オブジェクトオペレーターレベル2権限、またはオブジェクト管理者権限を持つNNMiユーザーにNNMi分析ペインのNAデータが表示されます。 • オブジェクトゲスト: すべてのNNMiノードについて、最小限のロールフィルターにパスしたすべてのNNMiユーザーにNNMi分析ペインのNAデータが表示されます。NNMiでセキュリティグループが設定されていない場合は、このオプションを選択します。 詳細については、「NNMi分析ペインのNA情報へのNNMiユーザーアクセスの設定」(68ページ)を参照してください。

NNMi分析ペインのNA情報へのNNMiユーザーアクセスの設定

NAインベントリと同期されたNNMiノードの場合、NNMi管理者は、NNMi分析ペインに表示されるこれらのノードのNA情報に対して、NNMiユーザーアクセスを制限できます。この制限は、[**HPE NNMi–HPE NAの統合設定**] フォームで以下の両方のフィールドを使用して実現できます。

- **分析ペインデータを表示する最小NNMiロール**
- **分析ペインデータを表示する最小オブジェクトアクセス権限**

NNMiユーザーがNNMi分析ペインにNA情報を表示するには、NNMiノードの最小ロールと最小オブジェクトアクセス権限の両方を満たしている必要があります。

- すべてのNNMiユーザーに対して、すべてのNNMiノードの分析ペインにすべてのNA情報の表示を許可するには、[**分析ペインデータを表示する最小NNMiロール**] フィールドを [機能を無効にする] に設定します。この設定により、[**分析ペインデータを表示する最小オブジェクトアクセス権限**] フィールドを使用できなくなります。
- NNMiロールのみを使用してアクセスを制御するには、以下の手順を実行します。
  - [**分析ペインデータを表示する最小NNMiロール**] フィールドを、いずれかの制限オプション ([NNMi管理者]、[NNMiレベル2オペレーター]、または [NNMiレベル1オペレーター]) に設定します。
  - [**分析ペインデータを表示する最小オブジェクトアクセス権限**] フィールドを [オブジェクトゲスト] に設定します。
- オブジェクトアクセス権限のみを使用してアクセスを制御するには、以下の手順を実行します。
  - [**分析ペインデータを表示する最小NNMiロール**] フィールドを [NNMiゲストユーザー] に設定します。
  - [**分析ペインデータを表示する最小オブジェクトアクセス権限**] フィールドを、いずれかの制限オプション ([オブジェクト管理者]、[オブジェクトオペレーターレベル2]、または [オブジェクトオペレーターレベル1]) に設定します。
- NNMiロールとオブジェクトアクセス権限の両方を使用してアクセスを制御するには、以下の手順を実行します。
  - [**分析ペインデータを表示する最小NNMiロール**] フィールドを、いずれかの制限オプション ([NNMi管理者]、[NNMiレベル2オペレーター]、または [NNMiレベル1オペレーター]) に設定します。
  - [**分析ペインデータを表示する最小オブジェクトアクセス権限**] フィールドを、いずれかの制限オプション ([オブジェクト管理者]、[オブジェクトオペレーターレベル2]、または [オブジェクトオペレーターレベル1]) に設定します。

    たとえば、以下の統合設定について考えてみます。
    - [**分析ペインデータを表示する最小NNMiロール**] は [NNMiレベル2オペレーター]。
    - [**分析ペインデータを表示する最小オブジェクトアクセス権限**] は [オブジェクトオペレーターレベル1]。

    HPE NNMi–HPE NA統合で同期されたNode1というノードの場合、以下のNNMiユーザーは、Node1の分析ペインおよびインタフェースにNA情報を表示できます。
    - 管理者ロールを持つすべてのNNMiユーザー。統合では、これらのユーザーのオブジェクトアクセス権限は無視されます。
    - Node1に対してオブジェクト管理者権限、オブジェクトオペレーターレベル2権限、またはオブジェクトオペレーターレベル1権限を持ち、オペレーターレベル2ロールを持つNNMiユーザー。

    以下のNNMiユーザーには、Node1の分析ペインおよびインタフェースにNA情報は表示されません。

- Node1に対してオブジェクトゲスト権限を持ち、オペレーターレベル2ロールを持つNNMiユーザー。
- オペレーターレベル1ロールまたはゲストロールを持つすべてのNNMiユーザー。

「表8 例: Node1の分析ペインにNA情報を表示できるユーザー」(69ページ)に、この情報をまとめます。

表8 例: Node1の分析ペインにNA情報を表示できるユーザー

NNMiオブジェクトのアクセス権限	NNMiロール			
	管理者	オペレーターレベル2	オペレーターレベル1	ゲスト
オブジェクト管理者	✓	✓		
オブジェクトオペレーターレベル2:	✓	✓		
オブジェクトオペレーターレベル1:	✓	✓		
オブジェクトゲスト	✓			

NNMiユーザーへのNNMiロールおよびノードオブジェクトアクセスレベルの割り当ての詳細については、以下の記載内容を参照してください。

- NNMiヘルプの「セキュリティの設定」
- 『NNMiデプロイメントリファレンス』の「NNMiセキュリティおよびマルチテナント」

NAコンソールでの設定パラメーター

NAコンソールの[**管理設定 - NA/NNMi統合**]ページには、NAからNNMiの通信を設定するためのパラメーターが含まれています。NNMiのサービス停止中トリガーおよびデバイス再検出(設定ポーリング)トリガーの統合動作を変更するには、このページにアクセスします。

[**管理設定 - NA/NNMi統合**]ページは、**[管理者] > [管理設定] > [NA/NNMi統合]**で表示できます。統合設定への変更を適用するには、このページの値を更新し、[**保存**]をクリックします。

注: 管理者ロールを持つNAユーザーのみが[**管理設定 - NA/NNMi統合**]ページにアクセスできます。

統合通信

「表9 NAコンソールの統合サーバーリストの列」(69ページ)に、[**管理設定 - NA/NNMi統合**]ページの[統合サーバーリスト]の列を示します。表の各行に、NAと1つのNNMi管理サーバー間の接続を示します。統合により、NNMiコンソールの[**HPE NNMi–HPE NAの統合設定**]フォームの情報が行に入力されます。

表9 NAコンソールの統合サーバーリストの列

フィールド	説明
統合が有効	[NNMiサーバー]列で識別されたNNMi管理サーバーとの統合のステータス。
NNMiサーバー	NNMi管理サーバーの正式な完全修飾ドメイン名。

表9　NAコンソールの統合サーバーリストの列 (続き)

フィールド	説明
NNMiシステムID	NNMi管理サーバーの一意のID。
NNMiプロトコル	NNMi Webサービスに接続するためのプロトコル。
NNMiポート	NNMi Webサービスへの接続ポート。
NNMiユーザー	NNMi Webサービスに接続するためのユーザー名。
NAユーザー	NA管理者ロールを持つ有効なNAユーザーアカウント名。

その他の統合動作

「表10　NAコンソールの統合動作情報」(70ページ)に、HPE NNMi–HPE NA統合の動作を設定するためのNAコンソールパラメーターを示します。

表10　NAコンソールの統合動作情報

フィールド	説明
デバイスをサービス停止中にするタスク	デバイスをサービス停止中にするようNNMiに要求するNAタスク。NNMiは、サービス停止中のデバイスに対してインシデントを生成しません。タスクの完了後、統合では[サービス停止完了の遅延]フィールドで指定された時間だけ待機してから、デバイスの管理の再開をNNMiに要求します。 統合により、タスク発生中にデバイスが[無効]状態に設定されるようにするNAタスク。デフォルトの選択は以下のとおりです。 • デバイスソフトウェアの更新 • パスワードの配布 • デバイスの再起動 この機能を無効にするには、タスクリストからすべての選択をクリアします。 詳細については、「デバイス設定中のネットワーク管理の無効化」(39ページ)を参照してください。
デバイスタスクが失敗した場合	サービス停止中イベントのデバイスタスク失敗復旧指定。デフォルト設定では、デバイスがNNMiのサービスに戻ります。
デバイス準拠確認が失敗した場合の処理	サービス停止中イベントのデバイスコンプライアンスチェック失敗復旧指定。デフォルト設定では、デバイスがNNMiのサービスに戻ります。 **注:** デバイス準拠確認は、NA Ultimateライセンスでのみ使用できます。
サービス停止完了の遅延	デバイスをサービス停止にするタスクが完了してからNNMiデバイス管理モードを復元するまでの、統合の待機時間 (分単位)。この遅延により、NAでタスクを完了してからデバイスを復元するまでの時間が提供されます。 デフォルト値は10分です。最大値は1440分 (24時間)です。 最大値を変更するには、NAの`adjustable_options.rcx`ファイルに`nnm/integration/max_out_of_service_delay`オプションを追加します。

表10　NAコンソールの統合動作情報 (続き)

フィールド	説明
NNMi設定ポーリングを要求するタスク	統合により、タスクの完了時にNNMiのデバイス検出が開始されるようにするNAタスク。デフォルトの選択は以下のとおりです。 • デバイスソフトウェアの更新 • パスワードの配布 • デバイスの再起動 • ドライバの検出 詳細については、「NAからのNNMiノード設定ポーリングのトリガー」(38ページ)を参照してください。

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。

HPE Network Node Manager i Software—HPE Network Automation統合ガイドに関するフィードバック (Network Node Manager i Software NNMi 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