

HP Network Node Manager i Software

Windows[®] および Linux[®] オペレーティングシステム用

ソフトウェアバージョン : NNMi 10.10

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

ドキュメントリリース日 : 2015 年 11 月
ソフトウェアリリース日 : 2015 年 11 月



ご注意

保証

HP 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。ここでの記載で追加保証を意図するものは一切ありません。HP では、ここに記載されている技術的、または編集上の不正確さや脱漏については責任を負いません。

ここに記載されている情報は、予告なく変更されることがあります。

権利制限について

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、HP 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。

著作権について

© Copyright 2008-2015 Hewlett-Packard Development Company, L.P.

商標に関する通知

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

Apple は、Apple Computer, Inc. の米国およびその他の国における登録商標です。

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

Google™ は、Google Inc. の登録商標です。

Intel®, Intel® Itanium®, Intel® Xeon®, および Itanium® は、Intel Corporation の米国およびその他の国の商標です。

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

Internet Explorer、Lync、Microsoft、Windows、および Windows Server は、Microsoft Corporation の米国およびその他の国における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。

Oracle テクノロジーの制限された権限に関する通知

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 社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。

2015年11月

謝辞

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

利用可能な製品ドキュメント

NNMi で入手可能なドキュメントの完全なリストについては、『HP Network Node Manager i Software ドキュメント一覧』を参照してください。このドキュメントは、HP マニュアル Web サイト上にあります。このファイルを使用して、このバージョンの NNMi の NNMi ドキュメントセットにある追加や改訂を調べることができます。リンクをクリックして、HP マニュアル Web サイト上のドキュメントにアクセスします。

HP マニュアル Web サイトでは、NNMi、NNMi Premium、NNMi Ultimate 用の完全なドキュメントセットの .zip ファイルも入手できます。これらのドキュメントパッケージは、『HP Network Node Manager i Software ドキュメント一覧』または HP マニュアル Web サイトから直接アクセスできます。

最近の更新を確認する場合、または最新のドキュメントを使用しているか確認する場合は、以下をご覧ください。

<https://softwaresupport.hp.com>

このサイトを利用するには、HP Passport への登録とサインインが必要です。HP Passport ID を登録するには、以下にアクセスします。

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

または、HP ソフトウェアサポートページの上にある [Register] リンクをクリックします。

製品のサポートサービスに登録すると、最新版を入手できます。詳細については、HP 営業担当者にお問い合わせください。

サポート

次の HP ソフトウェアサポートオンライン Web サイトを参照してください。

<https://softwaresupport.hp.com>

この Web サイトには、製品、サービス、および HP Software が提供するサポートの問い合わせ情報および詳細が記載されています。

HP ソフトウェアオンラインサポートには、お客様の自己解決機能が備わっています。ビジネスを管理するために必要な対話形式のテクニカルサポートツールにアクセスする迅速で効率的な方法が用意されています。お客様は、サポート Web サイトで以下の機能を利用できます。

- 関心のあるドキュメントの検索
- サポートケースおよび拡張リクエストの送信および追跡
- ソフトウェアパッチおよび関連パッチのドキュメントのダウンロード
- サポート契約の管理
- HP サポートの問合せ先の検索
- 利用可能なサービス情報の確認
- ソフトウェアを利用しているほかのユーザーとの情報交換
- ソフトウェアトレーニング情報の検索および参加登録

一部を除き、サポートのご利用には、HP Passport ユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HP Passport ユーザー ID のご登録は、以下の URL で行ってください。

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

アクセスレベルに関する詳細については、以下の URL で確認してください。

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

HP Software Solutions Now は、HPSW ソリューションおよび統合ポータル Web サイトにアクセスします。このサイトでは、ビジネスニーズに合った HP 製品ソリューションを調べることができ、HP 製品間の統合の完全なリストや ITIL プロセスのリストが含まれています。この Web サイトの URL は以下のとおりです。

<http://h20230.www2.hp.com/sc/solutions/index.jsp>

目次

HP NNMi-HP NA 統合	9
統合の概要.....	9
値.....	10
統合製品.....	11
統合設定の詳細.....	11
ドキュメント.....	11
統合アーキテクチャー.....	12
HP NNMi-HP NA 統合の有効化	19
準備.....	19
新規統合設定.....	19
NNMi 9.2x または NNMi 9.2x から NNMi 10.10 にアップグレードされた統合設定.....	22
NNMi と NA 間の SSL 通信の設定.....	23
NNMi と NA 間のシングルサインオンの設定.....	27
HP NNMi-HP NA 統合の使用法	31
NNMi と NA 間のインベントリ同期.....	31
定期的同期の考慮事項.....	33
HP Blade System Virtual Connect デバイスのサポート.....	33
統合が提供する NNMi 機能.....	34
NA コンソールのページの起動: NNMi コンソール.....	34
NNMi からの NA 診断のトリガー.....	35
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.....	36
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.....	36
不整合な状態のレイヤー 2 接続の特定.....	36
NNMi 分析ペインに表示される NA 情報.....	37
[ノードの設定] タブ.....	38
[ノード設定の履歴] タブ.....	38
ノードポリシーコンプライアンスタブ.....	39
[インタフェースの設定] タブ.....	40
NA 分析ペインのタブのノードインシデントタイプ.....	41
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.....	41
NNMi と NA の間のインタフェースの照合.....	41
統合が提供する NA 機能.....	42
NA コンソールからの NNMi コンソールのページの起動.....	42

NNMi への SNMP トラップの送信.....	42
SNMP トラップの送信のカスタマイズ.....	43
SNMP トラップの送信の無効化.....	44
NA からの NNMi ノード設定ポーリングのトリガー.....	44
NNMi ノード設定ポーリングのトリガーのカスタマイズ.....	44
NNMi ノード設定ポーリングのトリガーの無効化.....	44
デバイス設定中のネットワーク管理の無効化.....	44
サービス停止中の動作のカスタマイズ.....	45
サービス停止中の動作の無効化.....	46
NA へのデバイスコミュニティ文字列の変更の伝達.....	46
HP NNMi-HP NA 統合の NA イベントルール.....	46
NA イベントルールの有効化.....	48
NA イベントルールの無効化.....	49
HP NNMi-HP NA 統合を最大限に活用するためのシナリオ例.....	51
例 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.....	52
HP NNMi-HP NA 統合なしのプロセス.....	52
HP NNMi-HP NA 統合ありのプロセス.....	52
統合シナリオの前提条件.....	52
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.....	53
NA SNMP トラップインシデントのカスタマイズ.....	53
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.....	54
ポリシーコンプライアンス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.....	54
統合シナリオの概要.....	55
利点.....	55
例 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.....	56
HP NNMi-HP NA 統合なしのプロセス.....	56
HP NNMi-HP NA 統合ありのプロセス.....	56
統合シナリオの前提条件.....	56
OSPFNbrStateChange インシデントの有効化.....	56
統合シナリオの概要.....	57
利点.....	57
例 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.....	58
HP NNMi-HP NA 統合なしのプロセス.....	58
HP NNMi-HP NA 統合ありのプロセス.....	58
統合シナリオの前提条件.....	58
統合シナリオの概要.....	59
利点.....	59
例 4: IPv4 アドレスを対応する IPv6 アドレスに再割り当てする.....	60
HP NNMi-HP NA 統合なしのプロセス.....	60

HP NNMi-HP NA 統合ありのプロセス	60
統合シナリオの前提条件	60
統合シナリオの概要	60
利点	61
例 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	62
HP NNMi-HP NA 統合なしのプロセス	62
HP NNMi-HP NA 統合ありのプロセス	62
統合シナリオの前提条件	63
InterfaceInputUtilizationHigh および InterfaceInputUtilizationLow インシデントの有効化	63
統合シナリオの概要	63
利点	64
例 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	65
HP NNMi-HP NA 統合なしのプロセス	65
HP NNMi-HP NA 統合ありのプロセス	65
統合シナリオの前提条件	65
統合シナリオの概要	65
利点	66
例 7: エラーレートと使用率の問題を識別して修正する	67
HP NNMi-HP NA 統合なしのプロセス	67
HP NNMi-HP NA 統合ありのプロセス	67
統合シナリオの前提条件	67
InterfaceInputErrorRateHigh および InterfaceInputUtilizationHigh インシデントの有効化	67
統合シナリオの概要	68
利点	68
HP NNMi-HP NA 統合の管理	69
HP NNMi-HP NA 統合の変更	69
HP NNMi-HP NA 統合の無効化	70
HP NNMi-HP NA 統合のトラブルシューティング	70
統合をテストする	70
NNMi インベントリから欠落した NA デバイス	72
アプリケーションフェイルオーバーと HP NNMi-HP NA 統合	73
HP NNMi-HP NA 統合リファレンス	75
HP NNMi-HP NA 統合で使用されるポート	75
[HP NNMi-HP NA 統合設定] フォームのリファレンス	76
NNMi 管理サーバー接続	76
NA コアサーバー接続	77
統合動作	77
NNMi 分析ペインの NA 情報への NNMi ユーザーアクセスの 設定	79
NA コンソールでの設定パラメーター	81
統合通信	81
その他の統合動作	82

HP NNMi-HP NA 統合

HP 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、高度な関連機能、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。

HP 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、HP 営業担当者にお問い合わせください。

この章では、HP NNMi-HP 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 ページ 9](#)
- [統合アーキテクチャー ページ 12](#)

統合の概要

HP NNMi-HP 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。



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。

HP NNMi-HP 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



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



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。



HP NNMi-HP 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。



HP NNMi-HP 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

HP NNMi-HP 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 — **HP NNMi-HP 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** コンソール内から **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 — HP NNMi-HP 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。



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、HP 営業担当者にお問い合わせください。



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』(NA Support Matrix) 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](#) ページ 12 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。



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。



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。

HP NNMi-HP 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、HP NNMi-HP 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

HP NNMi-HP 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。15 ページの [図 1](#) 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。16 ページの [図 2](#) 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 水平スケーラビリティガイド』(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。

17 ページの [図 3](#) 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 NA コアのみ接続されているため ([**HP NNMi-HP 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。
- HP NNMi-HP 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 NA 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 は、HP NNMi-HP 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	注	さらに参照	
NNMi インベントリを NA インベントリに同期する	NNMi	<ul style="list-style-type: none"> • NNMi グローバルマネージャでは、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 ページ 31	
NA インベントリを NNMi インベントリに同期する	NA	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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。 		NA コンソールのページの起動: NNMi コンソール ページ 34
NNMi から NA 診断をトリガーする	NNMi	<ul style="list-style-type: none"> • 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 ページ 35
不整合な状態のレイヤー 2 接続を特定する	NNMi	<ul style="list-style-type: none"> • 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 ページ 36

表 1 統合の機能 (続き)

統合の機能	開始サーバー	注	さらに参照
NNMi 分析ペインに NA データを表示する (権限あり)	NNMi	<ul style="list-style-type: none"> 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 ページ 37
NA コンソールから NNMi コンソールページを起動する	NA	<ul style="list-style-type: none"> 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。 	NA コンソールからの NNMi コンソールのページの起動 ページ 42
NA デバイスイベントの通知を NNMi に送信する	NA	<ul style="list-style-type: none"> 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 への SNMP トラップの送信 ページ 42
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	<ul style="list-style-type: none"> 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。 	NA からの NNMi ノード設定ポーリングのトリガー ページ 44
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 ページ 44
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 ページ 46
NNMi から NA に SSL 接続を使用する	NNMi	<ul style="list-style-type: none"> 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。 	NNMi と NA 間の SSL 通信の設定 ページ 23
NA から NNMi に SSL 接続を使用する	NA	<ul style="list-style-type: none"> 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 から NA にシングルサインオンする	NNMi	<ul style="list-style-type: none"> 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。 	NNMi と NA 間のシングルサインオンの設定 ページ 27
NA から NNMi にシングルサインオンする	NA	<ul style="list-style-type: none"> 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。 	

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

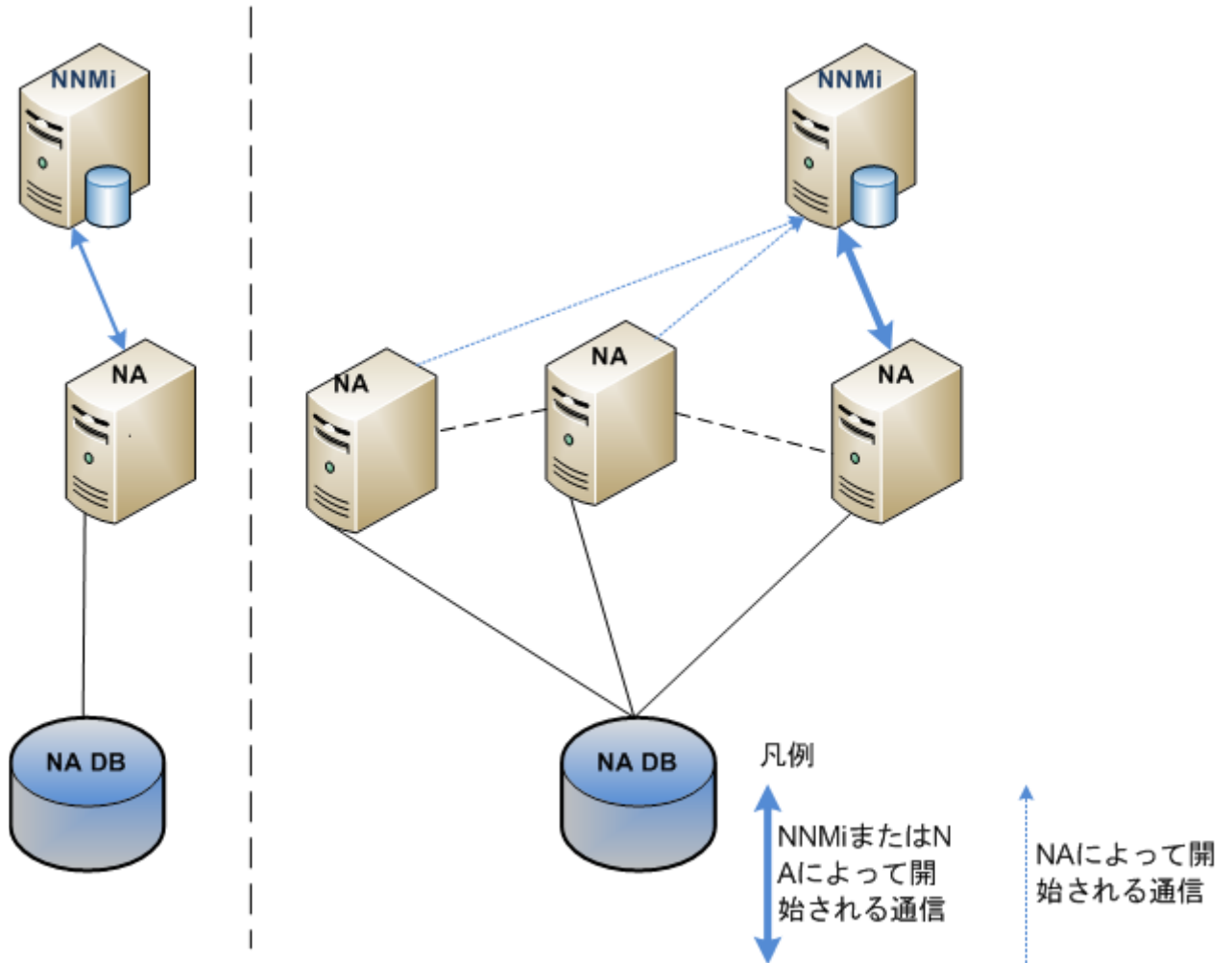


図2 配備アーキテクチャーの例: NNMi グローバルネットワーク管理から複数スタンドアロン NA コア

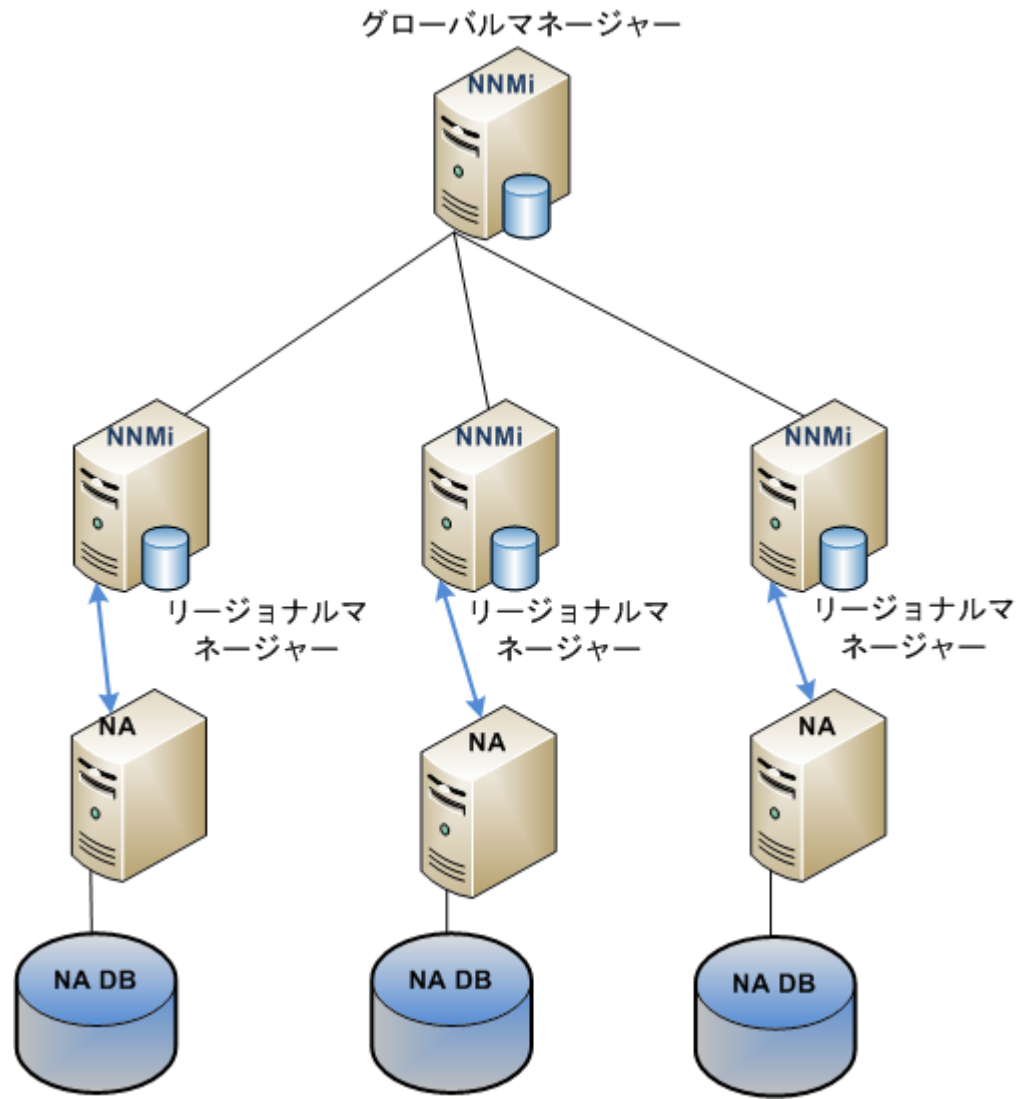
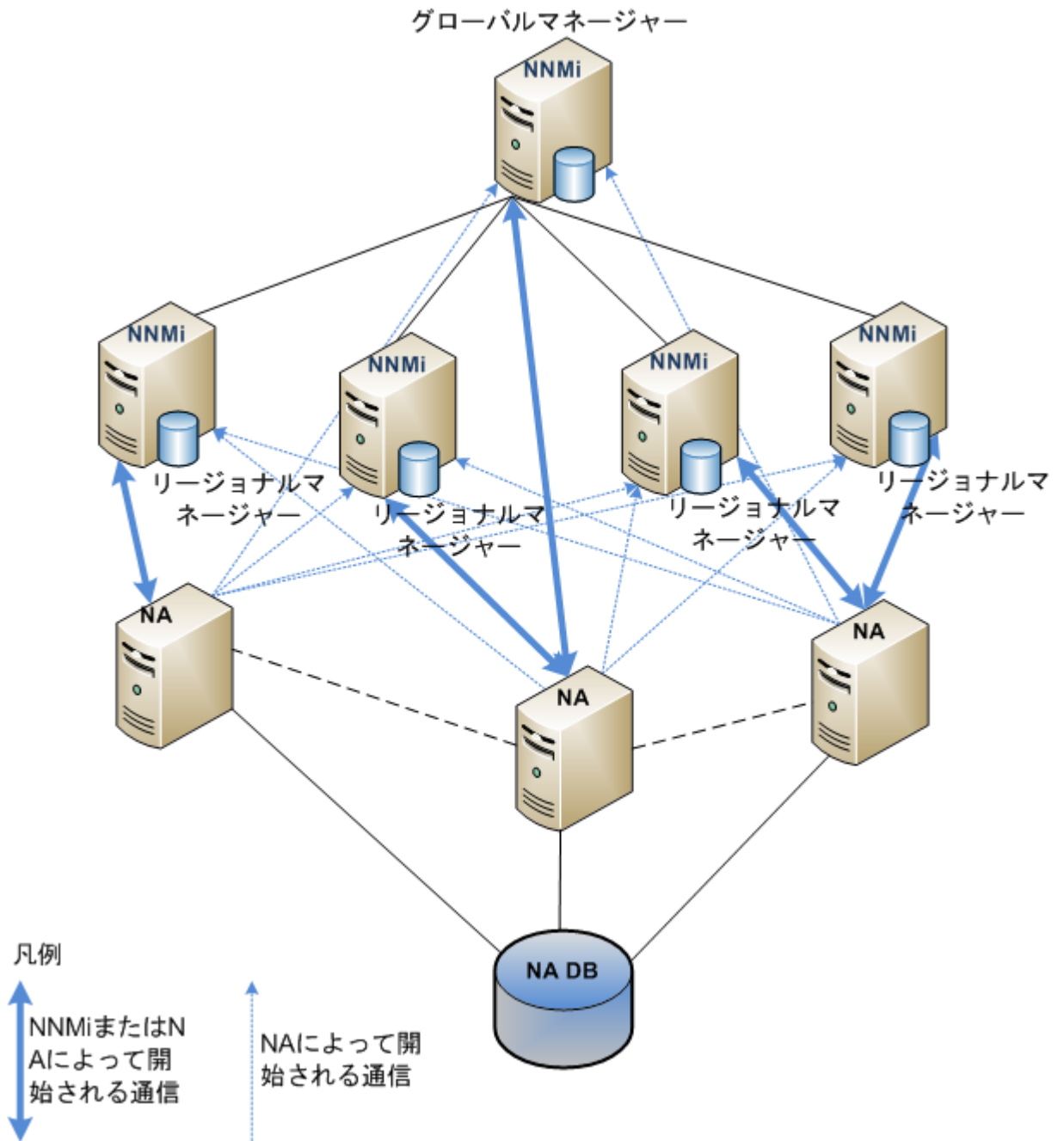


図3 配備アーキテクチャーの例：NNMi グローバルネットワーク管理から NA 水平スケーラビリティ



HP NNMi-HP NA 統合の有効化

HP NNMi-HP 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 ページ 19](#)
- [新規統合設定 ページ 19](#)
- [NNMi 9.2x または NNMi 9.2x から NNMi 10.10 にアップグレードされた統合設定 ページ 22](#)
- [NNMi と NA 間の SSL 通信の設定 ページ 23](#)
- [NNMi と NA 間のシングルサインオンの設定 ページ 27](#)

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

HP NNMi-HP 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 ページ 19](#) で説明されているプロセスを実行します。
- 2 省略可能。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 ページ 23](#) 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 [**HP NNMi-HP 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**] > [**HP 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 省略可能。[**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、19 ページの **手順 2** 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 ページ 76](#) 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 ページ 77](#) 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 ページ 77](#) 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 省略可能。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、20 ページの **手順 4** から 20 ページの **手順 7** までを繰り返します。

- 9 NA 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 NA 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 NA 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、NA インベントリのデバイスと通信する方法を指定します。
-  この時点で NA 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](#) ページ 48 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、[**HP NNMi-HP 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**] > [**HP 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 省略可能。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](#) ページ 81 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 省略可能。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 - ドライバーの検出**] 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ーを検出します。

- 12 省略可能。NNMi と NA 間のシングルサインオンの設定 ページ 27 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。



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 9.2x または NNMi 9.2x から NNMi 10.10 にアップグレードされた統合設定

NNMi 9.2x/10.0x または NA 9.2x/10.0x のいずれかをバージョン 10.1x 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 10.10 および NA 10.00 または NA 10.01 を使用するために HP NNMi-HP NA 統合をアップグレードして有効にするには、以下の手順を実行します。

- 1 各統合 NNMi 管理サーバーの NNMi コンソールで、HP NNMi-HP NA 統合を無効にします。HP NNMi-HP NA 統合の無効化 ページ 70 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 10.1x 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。



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` 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。



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、HP NNMi-HP NA 統合を有効にしないでください。

- 3 新規統合設定 ページ 19 の説明に従って、HP NNMi-HP NA 統合を設定します。以下の点に注意してください。
 - [HP NNMi-HP 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せん。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 [分析ペインデータのための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 [分析ペインデータのための最小 NNMi ロール] フィールドと相互作用します。NNMi のアップグレードにより、[分析ペインデータのための最小 NNMi ロール] フィールドの値が繰り越され、[分析ペインデータのための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。[分析ペインデータのための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 ページ 79 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。
- **[NNMi - NA 統合レベル]** フィールドは、NA 9.22 の NA コンソールの **[システム管理設定 - NA/NNMi 統合]** ページに追加され、NA 10.00 で削除されました。NA 9.22 以降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。



統合に関係するすべての NNMi 管理サーバーと 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。



この手順において、**手順 2** および **手順 5** 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 管理ガイド』(NA Administration Guide) の「NA での証明書の使用法」(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:*

```
<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:*

```
<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 手順 2 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:*

```
%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:*

```
$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。以下のプログラム一覧は、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:*

```
%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -v -list
-keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore
-storepass nnmkeypass
```

- *Linux:*

```
<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、手順 6 でコマンドから出力された値を使用します。

- *Windows:*
`%NnmInstallDir%\nonOV\hpsw\bin\keytool.exe -export
 -alias <alias> -file <directory>\nnm.cer
 -keystore %NNMDataDir%\shared\nnm\certificates\nnm.keystore
 -storepass nnmkeypass`
 - *Linux:*
`<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、手順 6 でコマンドから出力された値を使用します。
- *Windows:*
`<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:*
`<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。以下のプログラム一覧は、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: [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 省略可能。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

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 HP エンタープライズ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ります。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。



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
- **タスク 2:** シングルサインオン用の NA の設定

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 以下のファイルをテキストエディターで開きます。
 - **Windows:** %NNM_PROPS%\nms-ui.properties
 - **Linux の場合:** \$NNM_PROPS/nms-ui.properties

SSO を有効にする

- 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
```

NNMi 初期化スト リング

- 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。

```
nnmssso.ovpl -reload
```

詳細については、`nnmssso.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。

- 以下のファイルをテキストエディターで開きます。
 - Windows:**
`<NA_HOME>\server\ext\jboss\server\default\conf\lwssofmconf.xml`
 - Linux:**
`<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:** `C:\na`
 - Linux の場合:** `/opt/NA`

SSO を有効にする

- `enableLWSSO` タグで、`enableLWSSOFramework` 属性を `true` に設定します。


```
enableLWSSOFramework="true"
```

- `lwssValidation` 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。



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。

NA 初期化ストリング



- `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。

`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。
- `trustedHosts` ブロックで、以下の例のように、`DNSDomain` タグを `lwssValidation` ブロックのドメインタグの値に設定します。


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

- 6 手順 5 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: 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ーフェースから自動的にユーザーがログアウトされます。HP NNMi-HP 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。



NNMi または NA で自動的にユーザーインター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。30 分の値を使用することをお勧めします。HP NNMi-HP 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 既存の値を手順 a 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、既存の値を手順 **a** 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。

```
nnmssso.ovpl -reload
```

詳細については、`nnmssso.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。

HP NNMi-HP NA 統合の使用法

HP NNMi-HP 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 ページ 31
- 統合が提供する NNMi 機能 ページ 34
- 統合が提供する NA 機能 ページ 42

NNMi と NA 間のインベントリ同期

HP NNMi-HP 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

HP NNMi-HP 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

HP NNMi-HP 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、[HP NNMi-HP 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、[HP NNMi-HP 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も常に 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も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。

ベストプラクティス

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。



NA 10.00 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。



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



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



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。



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。



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ตอบสนอง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

HP NNMi-HP 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行います。HP NNMi-HP 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。HP NNMi-HP 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。

[HP NNMi-HP 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。

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

HP 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 手順 1 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、[HP NNMi-HP 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 ページ 77](#) を参照してください。

統合が提供する NNMi 機能

HP NNMi-HP 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。

- [NA コンソールのページの起動 : NNMi コンソール ページ 34](#)
- [NNMi からの NA 診断のトリガー ページ 35](#)
- [不整合な状態のレイヤー 2 接続の特定 ページ 36](#)
- [NNMi 分析ペインに表示される NA 情報 ページ 37](#)

NA コンソールのページの起動 : NNMi コンソール

HP NNMi-HP 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。

HP NNMi-HP 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。

- [\[HP NA 診断の結果の表示\]](#) - NNMi インシデントのデバイスにスケジュールされた NA 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 ページ 36](#) を参照してください。
- [\[HP NA 診断を再実行\]](#) — 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 ページ 36](#) 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 ページ 36](#) を参照してください。

- **HP 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。
- **HP 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。



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。

- **HP 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。
- **HP 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 デバイス設定の履歴**] ページを開きます。
- **HP 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。



コンプライアンス情報には、NA Ultimate ライセンスが必要です。

- **HP 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。
- **HP 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。
- **HP NA の起動** — NA コンソールを開きます。
- **HP 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。
- **HP 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、『HP Network Automation ユーザーガイド』を参照してください。

NNMi からの NA 診断のトリガー

HP NNMi-HP 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 診断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 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 NNMi NA 診断で設定されたインシデント

NNMi インシデント	NA Diagnostic
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
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 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 [HP NA 診断の結果の表示] と [HP 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]>[HP 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]>[HP 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。[HP 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

HP NNMi-HP 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。



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、21 ページの **手順 11** 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 管理ガイド』の「重複 MAC アドレスを保存するための NA の設定」を参照してください。

[アクション]>[不整合の接続を表示] コマンドでは、図 4 で示すように、速度の不整合が全二重の不整合、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。

図4 不整合接続テーブルの例

Layer 2 Connection	Speed Comparison (configured/negotiated : configured/negotiated)	Duplex Comparison (configured/negotiated : configured/negotiated)
c3745-3[Gi1/0/1].iptr3[Gi0/1.1]	POSSIBLE_MISMATCH (auto-negotiated/null : 1000/null)	POSSIBLE_MISMATCH (auto-negotiated/null : full/null)
Small Subnets-cisco6506core1[Fa1/24].junoscore6350[ge-0/0/3.0]	POSSIBLE_MISMATCH (auto-negotiated/null : /100)	POSSIBLE_MISMATCH (auto-negotiated/null : /full)
Small Subnets-cisco6506pe1[Fa1/2].junoscore6350[ge-0/0/2.0]	POSSIBLE_MISMATCH (/null : auto-negotiated/null)	POSSIBLE_MISMATCH (/null : auto-negotiated/null)
Small Subnets-ciscocore6524[Fa1/1].junoscore6350[ge-0/0/1.0]	POSSIBLE_MISMATCH (/100 : auto-negotiated/null)	POSSIBLE_MISMATCH (/full : auto-negotiated/null)
Small Subnets-ciscocore6524[Fa1/4].junospe4350[ge-0/0/1.0]	POSSIBLE_MISMATCH (auto-negotiated/null : /100)	POSSIBLE_MISMATCH (auto-negotiated/null : /full)
Small Subnets-ciscope2691[Fa1/0].mplscoe05[Et1/0]	POSSIBLE_MISMATCH (auto-negotiated/null : 10/null)	MATCH (half/null : half/null)

疑わしい接続について、テーブルは、接続のいずれか一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リストします。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。

[HP NNMi-HP 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、HP NNMi-HP 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 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
<ul style="list-style-type: none"> • [ノード] インベントリビュー • [ノード詳細] フォーム 	<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • [インシデントの参照] ビュー • [インシデント] フォーム <p>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 ページ 41 を参照してください。</p>	<ul style="list-style-type: none"> • ノードの設定 • ノード設定の履歴
<ul style="list-style-type: none"> • [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 	<ul style="list-style-type: none"> • インタフェースの設定
<ul style="list-style-type: none"> • [インシデントの参照] ビュー • [インシデント] フォーム <p>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 ページ 41 を参照してください。</p>	<ul style="list-style-type: none"> • インタフェースの設定

- ▶ 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](#) ページ 79 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。[図 5](#) を参照してください。

[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](#) ページ 41 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] > [HP Network Automation] > [HP NA デバイス設定の表示] を選択します。

図 5 [ノードの設定] タブ

```

!
! Last configuration change at 11:19:05 IST Wed Sep 16 2015
! NVRAM config last updated at 12:51:07 IST Tue Jun 30 2015
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service udp-small-servers
service tcp-small-servers
service sequence-numbers
!
hostname

```

[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。[図 6](#) を参照してください。

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](#) ページ 41 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]** > **[HP Network Automation]** > **[HP NA デバイス設定の履歴の表示]** を選択します。

図 6 [ノード設定の履歴] タブ

Create Date	Changed By	Comments	Actions
Wed Sep 16 04:49:14 PDT 2015	N/A		Compare to Previous View Config
Tue Sep 22 07:07:08 PDT 2015	N/A		Compare to Previous View Config

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。[図 7](#) を参照してください。



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。

図 7 ノードポリシーコンプライアンスタブ

Policy Name	In Compliance	Last Checked Date	Actions
Location	Yes	2013-10-31	View Policy Compliance in NA

[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。図 8 を参照してください。

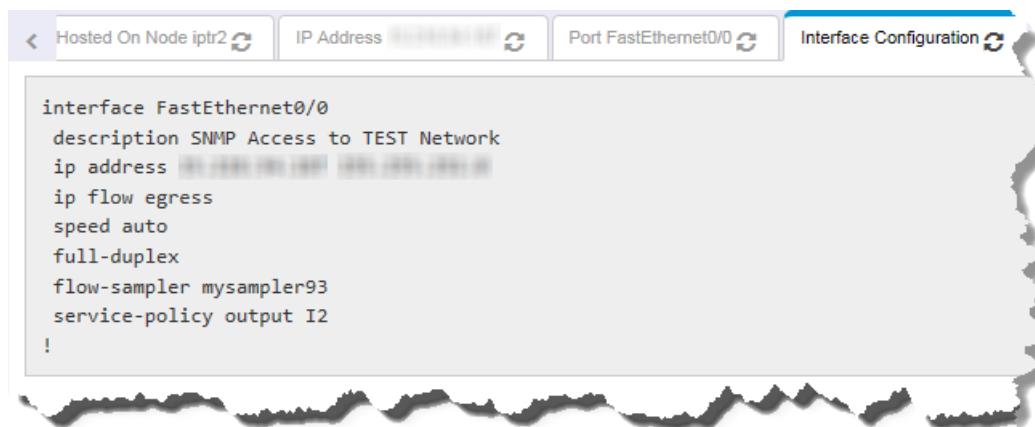
[インタフェース設定] タブは、以下の NNMi ビューで使用できます。

- [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](#) ページ 41 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](#) ページ 41 を参照してください。

図 8 [インタフェースの設定] タブ



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。



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

HP NNMi-HP 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](#) ページ 42
- [NNMi への SNMP トラップの送信](#) ページ 42
- [NA からの NNMi ノード設定ポーリングのトリガー](#) ページ 44
- [デバイス設定中のネットワーク管理の無効化](#) ページ 44
- [NA へのデバイスコミュニティ文字列の変更の伝達](#) ページ 46
- [HP NNMi-HP NA 統合の NA イベントルール](#) ページ 46



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

HP NNMi-HP 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

HP NNMi-HP 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。



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。



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 ページ 49](#) 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 ページ 49](#) 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、HP NNMi-HP 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回答し、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。



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](#) ページ 49 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。次に、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。



NA は、デバイスを管理するための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配布するとき、NNMi は更新を受信しません。



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。



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](#) ページ 48 を参照してください。

HP NNMi-HP 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。



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。

[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](#) ページ 44 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](#) ページ 44 を参照してください。

- **NA/NNMi 統合 SNMP コミュニティ文字列伝達**

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](#) ページ 46 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。HP NNMi-HP 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](#) ページ 42 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](#) ページ 32 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、[イベントの通知とレスポンスルール] ページ ([**管理者**] > [**イベントの通知とレスポンスルール**]) 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。



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。



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。

HP NNMi-HP 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 HP NNMi-HP 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 iSPI が 1 つ以上必要となるシナリオもあります。表 4 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リストします。

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
例 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 ページ 52	Premium	Ultimate
例 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 ページ 56	Premium	Premium
例 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 ページ 58	Ultimate	Premium
例 4: IPv4 アドレスを対応する IPv6 アドレスに再割り当てする ページ 60	Premium	Premium
例 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 ページ 62	Ultimate	Premium
例 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 ページ 65	Ultimate	Premium
例 7: エラーレートと使用率の問題を識別して修正する ページ 67	Premium	Premium

例 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。HP NNMi-HP 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。HP NNMi-HP 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。

HP NNMi-HP 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。

HP NNMi-HP 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 ページ 53。
- 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 ページ 53。

- 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 ページ 54。
- ポリシーコンプライアンス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 ページ 54。

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。



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。

ポリシーコンプライアンス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/NNM 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/NNM 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 HP NNMi-HP 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、HP NNMi-HP 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。

例 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。HP NNMi-HP 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。

HP NNMi-HP 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。

HP NNMi-HP 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 HP NNMi-HP 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、「例 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」で処理します。

利点

このシナリオにおいて、HP NNMi-HP 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。

例 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。HP NNMi-HP 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。

HP NNMi-HP 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。

HP NNMi-HP 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 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 HP NNMi-HP 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経路ビューを開きます ([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。



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、HP NNMi-HP 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。

例 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。HP NNMi-HP 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。

HP NNMi-HP 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。

HP NNMi-HP 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 HP NNMi-HP 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、HP NNMi-HP 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。

例 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。HP NNMi-HP 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。HP NNMi-HP 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。

HP NNMi-HP 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。

HP NNMi-HP 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
- NNM iSPI 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 ページ 63。

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、手順 2 から手順 4 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 HP NNMi-HP 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 ([**HP 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、HP NNMi-HP 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。

例 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。HP NNMi-HP 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。

HP NNMi-HP NA 統合なしのプロセス

この例の場合、会社のお客は、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。

HP NNMi-HP 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
- NNM iSPI 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。
- Web サイトの場所の IP アドレスについて、NNM iSPI Performance for Traffic サイトが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 HP NNMi-HP 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 NNM iSPI Performance for Traffic は、Web サイトの場所を表す NNM iSPI 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 NNM iSPI 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、NNM iSPI 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 ([HP 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、HP NNMi-HP 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。

例 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。HP NNMi-HP 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。

HP NNMi-HP 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。

HP NNMi-HP 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 ページ 67。

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、手順 2 から手順 4 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 HP NNMi-HP 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、HP NNMi-HP 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的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。

HP NNMi-HP NA 統合の管理

この章では、HP NNMi-HP 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。

- [HP NNMi-HP NA 統合の変更](#) ページ 69
- [HP NNMi-HP NA 統合の無効化](#) ページ 70
- [HP NNMi-HP NA 統合のトラブルシューティング](#) ページ 70
- [アプリケーションフェイルオーバーと HP NNMi-HP NA 統合](#) ページ 73

HP NNMi-HP 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](#) ページ 44
 - [デバイス設定中のネットワーク管理の無効化](#) ページ 44
 - b ページの下にある [[保存](#)] をクリックします。
- 2 省略可能。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](#) ページ 42
 - [NA へのデバイスコミュニティ文字列の変更の伝達](#) ページ 46
- 3 NNMi コンソールで、[[HP NNMi-HP 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](#)] > [[HP 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は、[[HP NNMi-HP NA 統合設定](#)] フォームのリファレンス ページ 76 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。

HP NNMi-HP NA 統合の無効化

- 1 NNMi コンソールで、[HP NNMi-HP 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] > [HP 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 省略可能。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])。

HP NNMi-HP 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 ページ 70
- NNMi インベントリから欠落した NA デバイス ページ 72

統合をテストする



過去に統合が正常に動作していた場合は、構成の何か (NNMi または NA のユーザーパスワードなど) 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、[HP NNMi-HP NA 統合設定] フォームのリファレンス ページ 76 の説明に従って統合設定を更新してください。

- 1 NNMi コンソールで、[HP NNMi-HP 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] > [HP NA])。

このフォームのフィールドの詳細は、[HP NNMi-HP NA 統合設定] フォームのリファレンス ページ 76 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、[HP NNMi-HP NA の統合設定] フォームで、フォームの下部にある [送信] をクリックします (設定の変更は行いません)。



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。この手順の手順 3 を継続します。

- 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、[HP NNMi-HP 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、NA 管理者にログオン資格情報を問い合わせてください。

- 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 [HP NNMi-HP 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

- 期待されるメッセージが表示されたら、**手順 5**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 管理者に問い合わせ、NA Web サービスに接続するために使用している情報を確認します。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。



この手順の**手順 1**で NNMi コンソールに接続するために、このステップ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。**手順 6**を継続します。

- 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>://<NNMIservice>:<port>/nnmi/

以下のように、変数が [HP NNMi-HP 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 が有効になっています] チェックボックスがオフになっている場合、<protocol> は http です。
- <NNMIservice> 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が、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。



「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**手順 4**と**手順 5**で使用して正常に接続できた値で、[HP NNMi-HP NA の統合設定] フォームを更新します。また、**手順 6**で使用した NNMi ユーザー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、[HP NNMi-HP NA 統合設定] フォームのリファレンス ページ 76 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 この手順の手順 7 と手順 8 を繰り返します。
- 10 **HP NNMi-HP NA 統合の使用法** ページ 31 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



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 HP NNMi-HP 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、HP NNMi-HP 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 [HP NNMi-HP NA の統合設定] フォームを新しい NA コアへの接続情報を使用して更新します。

HP NNMi-HP NA 統合リファレンス

この章では、HP NNMi-HP 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。

- HP NNMi-HP NA 統合で使用されるポート ページ 75
- [HP NNMi-HP NA 統合設定] フォームのリファレンス ページ 76
- NA コンソールでの設定パラメーター ページ 81

HP NNMi-HP NA 統合で使用されるポート

NNMi 管理サーバーでは、HP NNMi-HP 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 HP NNMi-HP 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。

[HP NNMi-HP NA 統合設定] フォームのリファレンス

NNMi コンソールの [HP NNMi-HP 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。



Administrator ロールの NNMi ユーザーのみが [HP NNMi-HP NA の統合設定] フォームにアクセスできます。

[HP NNMi-HP 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。

- NNMi 管理サーバー接続
- NA コアサーバー接続
- 統合動作
- NNMi 分析ペインの NA 情報への NNMi ユーザーアクセスの設定

統合設定に変更を適用するには、[HP NNMi-HP 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 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リストします。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 の管理サーバー情報 NNMi コンソール

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、19 ページの 手順 2 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。 注：統合により、以下のファイルの <code>nmsas.server.port.web.http</code> 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。 <ul style="list-style-type: none"> • Windows の場合：<code>%NnmDataDir%\Conf\nnm\props\nms-local.properties</code> • Linux の場合：<code>\$NnmDataDir/conf/nnm/props/nms-local.properties</code>
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 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リストします。NA 管理者と協力し、設定フォームのこのセクションに使用する適切な値を決定します。

表 6 NA コアサーバー情報 : NNMi コンソール

HP 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、19 ページの 手順 2 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 サービスに接続するためのポート。 デフォルトの NA ポートは以下のとおりです。 <ul style="list-style-type: none"> • 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 • 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	指定した NA ユーザーのパスワード。

統合動作

表 7 には、HP NNMi-HP 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リストします。

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 ページ 31 に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。

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
NA のデバイスドライバの検出	<p>NA 設定の指定。</p> <p>[NA のデバイスドライバの検出] 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。</p> <p>[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。</p>
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	<p>[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が常に NA パーティションに追加されるか更新されます。</p> <p>[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。</p> <p>[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。</p>
NA 接続チェック間隔 (時間)	<p>不整合な状態のレイヤー 2 接続の特定 ページ 36 の説明のように、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。</p> <p>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。</p>
分析ペインデータののための最小 NNMi ロール	<p>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。 [分析ペインデータののための最小 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。</p> <ul style="list-style-type: none"> 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。 <p>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 ページ 79 を参照してください。</p>

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
分析ペインデータのための最小オブジェクトアクセス権限	<p>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。[分析ペインデータのための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。</p> <ul style="list-style-type: none"> 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。 <p>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 ページ 79 を参照してください。</p>

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、**[HP NNMi-HP 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。

- 分析ペインデータのための最小 NNMi ロール
- 分析ペインデータのための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、**[分析ペインデータのための最小 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、**[分析ペインデータのための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。
 - [分析ペインデータのための最小 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。
 - [分析ペインデータのための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。
 - [分析ペインデータのための最小 NNMi ロール]** フィールドを [NNMi ゲストユーザー] に設定します。

- [分析ペインデータのための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。
 - [分析ペインデータのための最小 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。
 - [分析ペインデータのための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。

- [分析ペインデータのための最小 NNMi ロール] は [NNMi レベル 2 オペレーター]。
- [分析ペインデータのための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]。

HP NNMi-HP 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 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 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。



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 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 [**HP NNMi-HP 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。
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 サービスに接続するためのポート。
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 に、HP NNMi-HP 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リストします。

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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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 <p>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 ページ 44 を参照してください。</p>
デバイスタスクが失敗した場合	<p>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。</p>
デバイス準拠確認が失敗した場合の処理	<p>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。</p> <p>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。</p>
サービス停止完了の遅延	<p>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。</p> <p>デフォルト値は 10 分です。最大値は 1440 分 (24 時間) です。</p> <p>最大値を変更するには、NA の <code>adjustable_options.rcx</code> ファイルに <code>nnm/integration/max_out_of_service_delay</code> オプションを追加します。</p>
NNMi 設定ポーリングを要求するタスク	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>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 ページ 44 を参照してください。</p>

フィードバックをお待ちしております。

ご使用のシステムに電子メールクライアントが設定されている場合は、デフォルトで、ここをクリックすると電子メールウィンドウが開きます。

使用可能な電子メールクライアントがない場合は、Web メールクライアントの新規メッセージに以下の情報をコピーして、**network-management-doc-feedback@hpe.com** にこのメッセージを送信してください。

製品名およびバージョン: NNMi 10.10

ドキュメントタイトル: HP Network Node Manager i Software-HP Network Automation 統合ガイド、2015年11月

フィードバック: