HP Automated Network Management

ソリューションバージョン : 9.20

設定ガイド

ドキュメントリリース日 : 2012 年 7 月
ソフトウェアリリース日 : 2012 年 7 月

ご注意

保証

HP 製品、またはサービスの保証は、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。ここに含まれる技術的、編集上の誤り、または欠如について、HP はいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

権利の制限

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 からの有効な使用許諾が必要です。商用コンピュータソフトウェア、コンピュータソフトウェアに関する文書類、および商用アイテムの技術データは、FAR 12.211 および 12.212 の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

© Copyright 2010–2012 Hewlett-Packard Development Company, L.P.

商標について

Adobe は、Adobe Systems Incorporated の商標です。

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

HP 9000 コンピューター上の HP-UX リリース 10.20 以降および HP-UX リリース 11.00 以降 (32 ビットおよび 64 ビット両方の環境) は、すべて Open Group UNIX 95 製品です。

Intel、Itanium、および Intel Xeon は、Intel Coporation の米国およびその他の国の登録商標です。

Microsoft および Windows は、Microsoft Corporation の米国登録商標です。

Oracle は、Oracle Corporation およびその関連会社の登録商標です。

UNIX は、The Open Group の登録商標です。

ドキュメントの更新情報

このマニュアルの表紙には、以下の識別番号が記載されています。

- ソフトウェアのバージョン番号は、ソフトウェアのバージョンを示します。
- ドキュメントリリース日は、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は、このバージョンのソフトウェアのリリース期日を表します。

最新の更新のチェック、またはご使用のドキュメントが最新版かどうかのご確認には、次のサイトをご利用ください。

http://support.openview.hp.com/selfsolve/manuals

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 の取得登録は、次の Web サイトから行なうことができます。

http://h20229.www2.hp.com/passport-registration.html (英語サイト)

または、HP Passport のログインページの [**New users - please register**] リンクをクリックします。

適切な製品サポートサービスをお申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、HP の営業担当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。

http://support.openview.hp.com

HP ソフトウェアが提供する製品、サービス、サポートに関する詳細情報をご覧いただけます。

HP ソフトウェアオンラインではセルフソルブ機能を提供しています。お客様の業務の管理に必要な対話型の技術支援ツールに素早く効率的にアクセスいただけます。HP ソフトウェアサポート Web サイトのサポート範囲は次のとおりです。

- 関心のある技術情報の検索
- サポートケースとエンハンスメント要求の登録とトラッキング
- ソフトウェアパッチのダウンロード
- サポート契約の管理
- HP サポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

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、ログ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 ID を登録するには、以下の Web サイトにアクセスしてください。

http://h20229.www2.hp.com/passport-registration.html (英語サイト)

アクセスレベルに関する詳細は、以下の Web サイトにアクセスしてください。

http://support.openview.hp.com/access_level.jsp

目次

1 ANM の要件 7
サポート製品バージョン 7
配備アーキテクチャー例 8
ハードウェアとソフトウェアの要件 11
Web ブラウザーとソフトウェアの要件 12
NNMi 管理サーバー 13
NA サーバー 15
NPS サーバー 16
トラフィックマスターサーバー 17
トラフィックリーフサーバー 18
NNM iSPI NET 診断サーバー 19
製品ドキュメント 20
ANM と製品ドキュメントの間のリンクの有効化 20

2 ANM の設定 23
ANM のインストールと設定 23
HP NNMi - HP NA 統合の検証 30
ANM のライセンス 31
ANM 9.10 から ANM 9.20 へのアップグレード 32

3 ANM シナリオ例の設定 35
例 1: 非適合デバイス変更を識別して修正する 36
シナリオ例の前提条件 36
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 36
NA SNMP トラップインシデントのカスタマイズ 36
デバイスの設定変更時にポリシー適合チェックタスクを実行するように NA を設定する 37
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 37
シナリオ例の概要 38
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 39
シナリオ例の前提条件 39
OSPFNbrStateChange インシデントの有効化 39
シナリオ例の概要 39
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 40
シナリオ例の前提条件 40
シナリオ例の概要 40

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 41
シナリオ例の前提条件 41
シナリオ例の概要 41
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 42
シナリオ例の前提条件 42
InterfaceInputUtilizationHigh および InterfaceInputUtilizationLow インシデントの有効化 42
シナリオ例の概要 42
例 6: エッジルーターで期待されるサービスレベルを確保する 44
シナリオ例の前提条件 44
シナリオ例の概要 44
例 7: 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 45
シナリオ例の前提条件 45
シナリオ例の概要 45
例 8: エラーレートと使用率の問題を識別して修正する 46
シナリオ例の前提条件 46
InterfaceInputErrorRateHigh および InterfaceInputUtilizationHigh インシデントの有効化 46
シナリオ例の概要 46
フィードバックをお待ちしております 49

1 ANM の要件

本章では、ANM のハードウェアおよびソフトウェア前提条件について説明します。

サポート製品バージョン

表 1 に、ANM 9.20 を構成するソフトウェア製品とバージョンの一覧を示します。表 2 には、ANM Advanced 9.20 を購入することによって有効になる追加ソフトウェア製品とバージョンの一覧を示します。

表 1 ANM 製品

製品名	製品の短縮名	バージョン
HP Network Node Manager i Software	NNMi	9.20
HP Network Automation	NA	9.20
HP Network Node Manager iSPI Performance for Quality Assurance Software	NNM iSPI Performance for QA	9.20
NNM iSPI Network Engineering Toolset Software	NNM iSPI NET	9.20
HP Network Node Manager iSPI Performance for Metrics Software	NNM iSPI Performance for Metrics	9.20
HP Network Node Manager iSPI Performance for Traffic Software	NNM iSPI Performance for Traffic	9.20

表 2 ANM Advanced のオプション追加統合製品

製品名	製品の短縮名	バージョン
HP Network Node Manager iSPI for MPLS Software	NNM iSPI for MPLS	9.20
HP Network Node Manager iSPI for IP Multicast Software	NNM iSPI for IP Multicast	9.20
HP Network Node Manager iSPI for IP Telephony Software	NNM iSPI for IP Telephony	9.20

以下の点に注意してください。

- ANM Advanced ライセンスにより、NNMi Advanced の機能も有効になります。

- HP NNMi - HP NA 統合は、重複する IP アドレスを区別できません。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。

配備アーキテクチャー例

図 1 に、ANM の配備アーキテクチャー例を示します。図の左側は、6 台のサーバーに ANM コンポーネントが分散することを示しています。図の右側は、6 台のサーバーに ANM Advanced コンポーネントが分散することを示しています。お持ちの ANM ライセンスに一致する図を参照してください。図の各ボックスは 1 台のサーバーを表しています。第 2 章、ANM の設定で説明する手順には、サーバーの番号が示されています。

このマニュアルに示す指示は、このアーキテクチャーを想定しています。このアーキテクチャーの前提は次のとおりです。

- データベースを必要とする各サーバーでは、その製品で利用可能な組み込みデータベースを使用する。
- すべてのサーバーが、間にファイアウォールを介することなく、同じネットワークセグメント上に配置されている。ソリューションサーバー間にファイアウォールが存在すると、製品のパフォーマンスに影響します。
- ネットワークに、サポートされているネットワークデバイスが配置されている。
- ネットワークに、サポートされるフローテクノロジが実行されているデバイスと、組み込み IP SLA 機能を持つデバイスが配置されている。

図 1　ANM の配備アーキテクチャー例

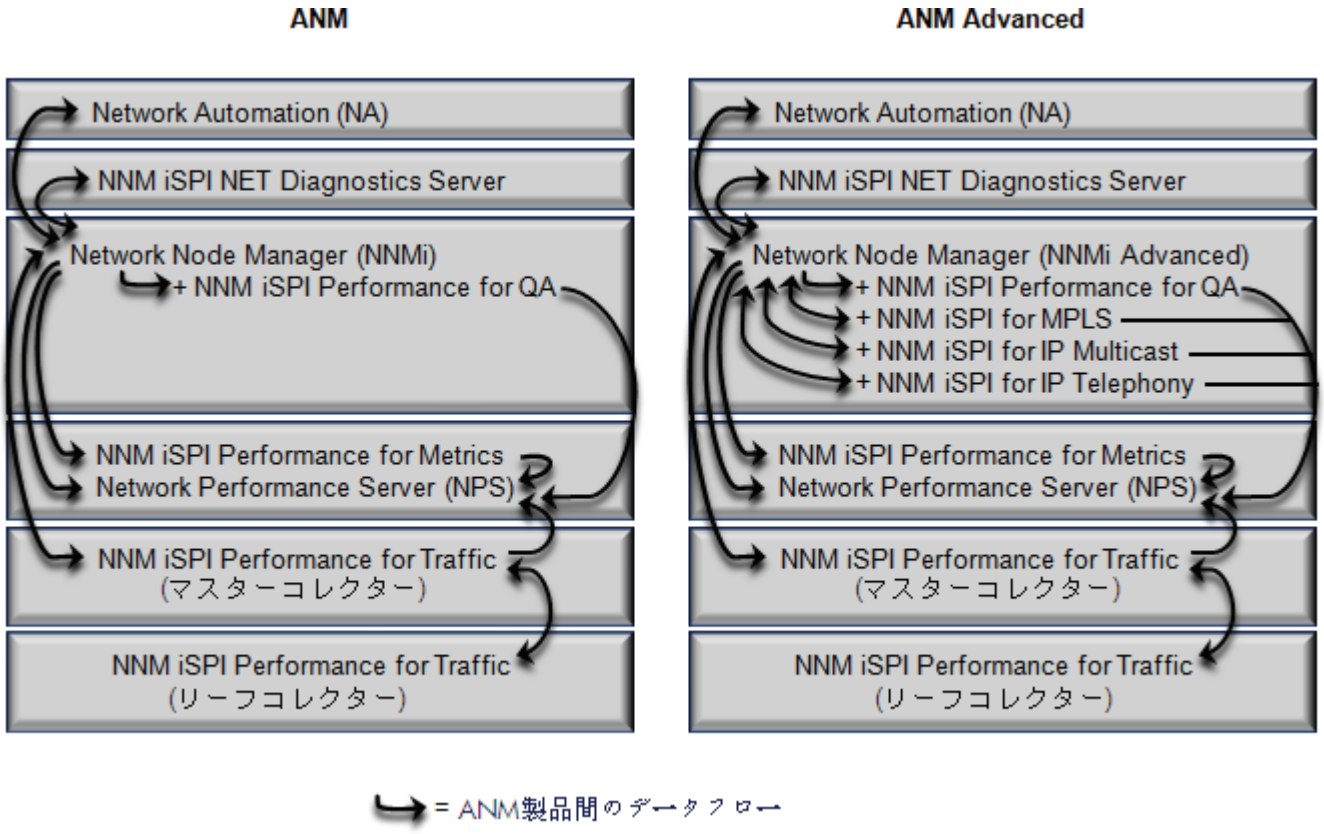


表 3 に、ANM の配備アーキテクチャー例で各サーバーにインストールされる製品についての別のビューを示します。1

表 3　配備サーバー例

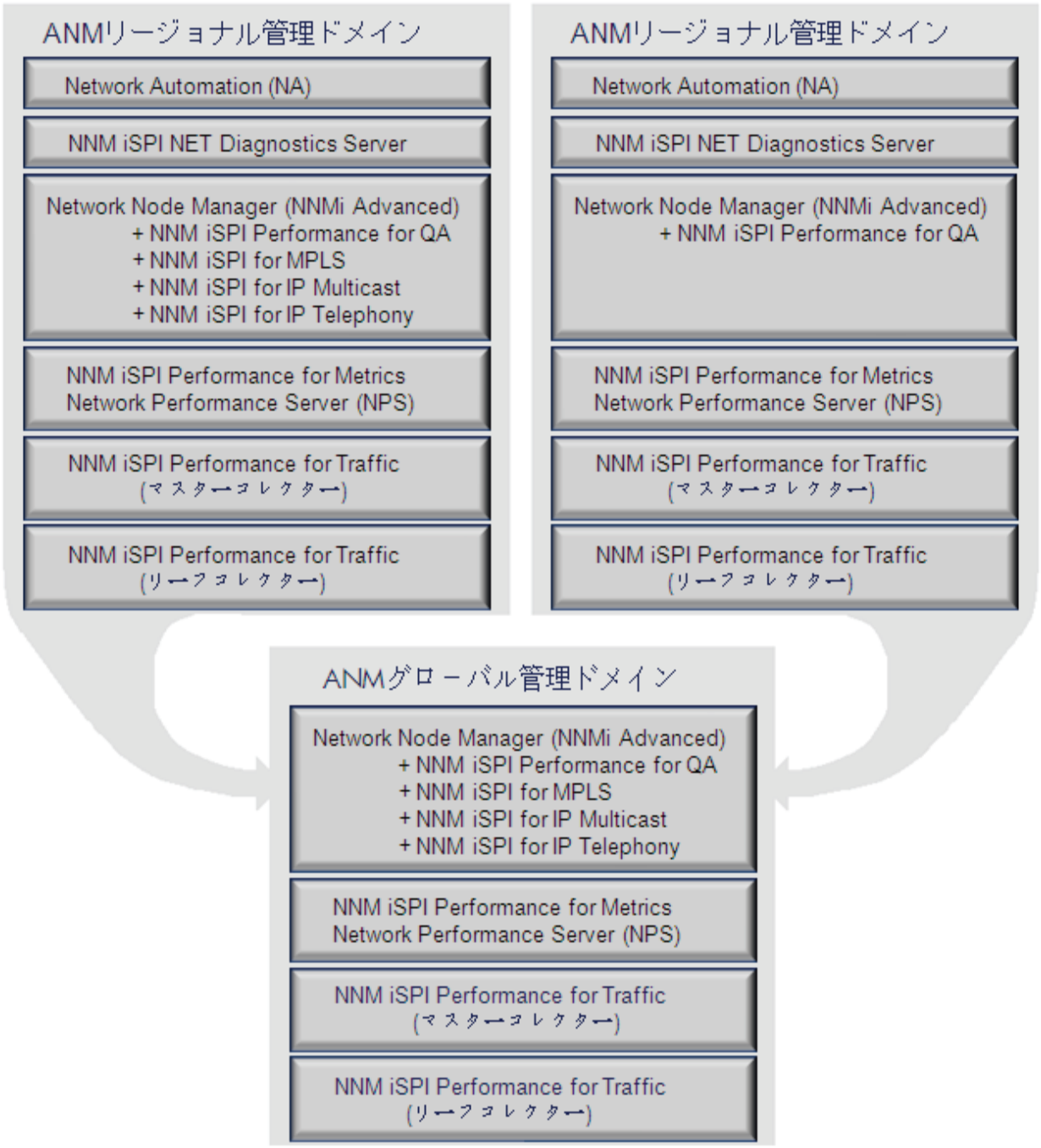
サーバー	インストールされるソフトウェア
NNMi 管理サーバー	• NNMi • NNM iSPI Performance for QA • NNM iSPI Performance for Traffic 拡張 • ANM Advanced のオプション統合製品 : — NNM iSPI for MPLS — NNM iSPI for IP Multicast — NNM iSPI for IP Telephony
NA サーバー	• NA
NPS サーバー	• NNM Performance iSPI のすべてが使用する Network Performance Server (NPS) • NNM iSPI Performance for Metrics
トラフィックマスターサーバー	• NNM iSPI Performance for Traffic マスターコレクター
トラフィックリーフサーバー	• NNM iSPI Performance for Traffic リーフコレクター
NNM iSPI NET 診断サーバー	• NNM iSPI NET

図 2 に、NNMi グローバルネットワーク管理機能上に構築された分散 ANM の配備アーキテクチャー例を示します。NNMi グローバルマネージャーには NNMi Advanced ライセンスが必要です。そのため、ANM グローバル管理ドメインには ANM Advanced ライセンスがあります。NNMi リージョナルマネージャーは、NNMi または NNMi Advanced のどちらかのライセンスを保持し、それにより ANM または ANM Advanced のどちらかのライセンスにマップされます。NNM Performance iSPI は、ANM グローバル管理ドメイン内のデータを統合できます。ANM リージョナル管理ドメインに ANM Advanced ライセンスがある場合は、NNM iSPI for MPLS、NNM iSPI for IP Multicast、および NNM iSPI for IP Telephony も ANM グローバル管理ドメイン内のデータを統合できます。

NA と NNM iSPI NET は、ANM グローバル管理ドメインではサポートされていません。

NA が水平方向の拡張性を持つように設定されている場合、NA サーバーの 1 つが ANM に参加できます。

図 2　分散 ANM のアーキテクチャー例



ハードウェアとソフトウェアの要件

本項では、次のようなパラメーターを示す中規模ネットワークの製品対応マトリックスからの情報を統合します。

- 管理対象デバイス 3,000 ～ 8,000
- 最大 60,000 のパフォーマンスポーリング対象インタフェースを 5 分間隔でポーリング
- 設定済み QA プローブ数 30,000
- 毎分 600,000 件のフローレコードを NNM iSPI Performance for Traffic マスターコレクターに送信
- 毎分 300,000 件のフローレコードを NNM iSPI Performance for Traffic リーフコレクターに送信

述べられている要件は、物理システムに適用されます。仮想システム、非組み込みデータベース、および異なる環境規模の要件などの詳細については、「製品ドキュメント」(20 ページ) で説明するように HP のマニュアル Web サイトから入手可能な製品対応マトリックスを参照してください。

本章で示す要件と、個々の製品対応マトリックスに示される要件の間に相違がある場合は、製品対応マトリックスの情報に従ってください。

各 ANM サーバーは同構造である必要はありません。本章で説明するいくつかの例外を除いて、各サーバーはそのソフトウェアでサポートされている任意のタイプにすることができます。

1 つのチップに 4 コア以上を搭載する CPU チップの場合は、Red Hat 5.5 以降が必要です (このコア数とコア総数を混同しないでください。この数は、単にチップあたりのコア数です)。

本項では、次のシステムの要件について説明します。

- 「Web ブラウザーとソフトウェアの要件」(12 ページ)
- 「NNMi 管理サーバー」(13 ページ)
- 「NA サーバー」(15 ページ)
- 「NPS サーバー」(16 ページ)
- 「トラフィックマスターサーバー」(17 ページ)
- 「トラフィックリーフサーバー」(18 ページ)
- 「NNM iSPI NET 診断サーバー」(19 ページ)

Web ブラウザーとソフトウェアの要件

表 4 に、Web ブラウザーの要件と、特定の ANM の機能を使用するために必要な追加のソフトウェアを示します。

表 4　ANM を使用する場合の Web ブラウザーとソフトウェアの要件

目的	要件
NNMi コンソール、NA コンソール、および NPS コンソールを実行する	次のいずれか : • Microsoft Internet Explorer バージョン 8 (互換表示モードで実行していない 32 ビット版または 64 ビット版) • Microsoft Internet Explorer バージョン 9 (互換表示モードで実行していない 32 ビット版または 64 ビット版) • Microsoft Windows または Linux 上の Mozilla Firefox 10.x 延長サポート版 (ESR) Firefox 延長サポート版 (ESR: Extended Support Release) ブラウザーは、**http://www.mozilla.jp/business/downloads/ から入手できます**
NNMi グラフ、NNMi MIB ブラウザー、および NA デバイスセレクターを表示する	• Adobe Flash Player Plug-in バージョン 10.2 (または以降のマイナーバージョン) またはバージョン 11.1 (または以降のマイナーバージョン) • 64 ビット版の Internet Explorer では、バージョン 11.1 以降が必要です
NA 概要レポートを表示する	• Microsoft Excel 2000 以降
エクスポートされたマップファイルを表示する	次のいずれか : • Microsoft Visio 2007 • Microsoft Visio 2010

いずれかの ANM コンソールを実行するために使用する Web ブラウザーは、それぞれ次のように設定する必要があります。

- すべてのポップアップウィンドウブロッカーを無効にする。
- Cookies を有効にする。
- JavaScript を有効にする。
- VML を有効にするように Internet Explorer を設定する。
- 新しいウィンドウをタブではなく別のウィンドウとして開くように Firefox を設定する。
- ディスプレイ解像度を最低でも 1024×768 に設定する。

NNMi 管理サーバー

表 5 に、次のソフトウェアを NNMi 管理サーバーにインストールする場合の複合要件を示します。

- NNMi
- NNM iSPI Performance for QA
- NNM iSPI Performance for Traffic 拡張

表 5　NNMi 管理サーバーの要件

エリア	最小要件
ハードウェア	**注 :** NNM iSPI Performance for QA Intelligent Response Agent (iRA) は、Windows および Linux オペレーティングシステムでのみ動作します。 • システム : — Windows または Linux: Intel 64 ビット (x86-64) または AMD 64 ビット (AMD64) ×10 CPU コア — HP-UX: Intel Itanium プロセッサーファミリー ×10 CPU コア — Solaris: Oracle SPARC64 VI 以降 ×10 CPU コア • RAM: NNMi と NNM iSPI Performance for QA を合わせて 24GB • 仮想メモリ : RAM の 2 倍の容量 • インストールおよび動作のためのディスク容量 : NNMi と NNM iSPI Performance for QA を合わせて 355MB 空き容量をオペレーティングシステムとは別のドライブに確保することをお勧めします。 **注 :** NNM iSPI for IP Multicast、NNM iSPI for IP Telephony、および NNM iSPI for MPLS は、NNMi と同時常駐する必要があります。これらの NNM iSPIs のいずれかをインストールする予定の場合は、NNMi 管理サーバーの要件値を次のように増加してください。 1 追加する各 NNM iSPI の対応マトリックスに基づいて、次の値を決定します。 — CPU コアの数 — RAM — インストールおよび実行時のディスク容量 2 これらの値を表 5 に示す値に追加します。 利用可能な仮想メモリの容量は、インストール製品すべての合計 RAM 要件の 2 倍にしてください。 製品対応マトリックスのダウンロードの詳細については、「製品ドキュメント」(20 ページ) を参照してください。

表 5　NNMi 管理サーバーの要件 (続き)

エリア	最小要件
オペレーティングシステム	注 : NNMi 管理サーバーが Windows オペレーティングシステム上で稼動する場合は、NPS サーバーも Windows オペレーティングシステム上で稼動する必要があります。 • Windows: — Windows Server 2008 x64 Datacenter Edition Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition Service Pack 1 — Windows Server 2008 x64 Enterprise Edition Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition Service Pack 1 — Windows Server 2008 x64 Standard Edition Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition Service Pack 1 • HP-UX: HP-UX 11i v3 • Linux: — Red Hat Enterprise Linux Server 6.0 (またはそれ以降の 6.x までのマイナーバージョン) — Red Hat Enterprise Linux Server 5.4 (またはそれ以降の 5.x までのマイナーバージョン) • Solaris: Oracle Solaris 10 SPARC

NA サーバー

表 6 に、NA を NA サーバーにインストールする場合の要件を示します。

表 6　NA サーバーの要件

エリア	最小要件
ハードウェア	• システム : Windows または Linux: — Inte® l 64 ビット (x86-64) ×6 CPU コア、12 論理プロセッサー、ハイパースレッディング実装 — AMD 64 ビット (AMD64) ×6 CPU コア、12 論理プロセッサー、ハイパースレッディング実装 • Solaris: — Oracle SPARC64 VI 以降 (M-Series) ×6 CPU コア、12 仮想プロセッサー — Oracle SPARC T4 以降 (T-Series) ×6 CPU コア、12 仮想プロセッサー • RAM: 16GB • 仮想メモリ : RAM の 2 倍の容量 • インストールおよび動作のためのディスク容量 : 512GB 空き容量をオペレーティングシステムとは別のドライブに確保することをお勧めします。
オペレーティングシステム	• Windows: — Windows Server 2008: x64 Datacenter Edition、Service Pack 2 — Windows Server 2008: R2 x64 Datacenter Edition、Service Pack 1 — Windows Server 2008: x64 Enterprise Edition、Service Pack 2 — Windows Server 2008: R2 x64 Enterprise Edition、Service Pack 1 — Windows Server 2008: x64 Standard Edition、Service Pack 2 — Windows Server 2008: R2 x64 Standard Edition、Service Pack 1 • Linux: — Red Hat Enterprise Linux Server AS 4.0 またはそれ以降のマイナーバージョン — Red Hat Enterprise Linux Server 5.4 またはそれ以降の 5.6 までのマイナーバージョン — Red Hat Enterprise Linux Server 6.0 またはそれ以降のマイナーバージョン — SUSE Linux Enterprise Server 9 — SUSE Linux Enterprise Server 11 Service Pack 1 • Solaris: Oracle Solaris 10 SPARC
Perl	• Perl SDK を使用する場合 : — Windows: ActivePerl 5.8.x — Linux または Solaris: Perl 5.8.x • SSH を有効にして NA 接続モジュールを使用する場合 : Perl Net::SSH::Expect モジュール • 注 : NA Perl API への SSH 接続には、Net::SSH::Expect モジュールが必要です。Windows での ActiveState ActivePerl の制限のため、NA Perl API は Windows システムからの SSH 接続をサポートしません。回避方法として、サポートされている Linux または Solaris システムに NA クライアントをインストールし、そのシステムから NA Perl API を実行してください。

NPS サーバー

表 7 に、次のソフトウェアを NPS サーバーにインストールする場合の複合要件を示します。

- NPS
- NNM iSPI Performance for Metrics レポートパック
- NNM iSPI Performance for QA レポートパック
- NNM iSPI Performance for Traffic レポートパック

表 7　NPS サーバーの要件

エリア	最小要件
ハードウェア	• システム : — Windows または Linux: Intel 64 ビット (x86-64) または AMD 64 ビット (AMD64) ×28 CPU コア • RAM: NPS、NNM iSPI Performance for Metrics、NNM iSPI Performance for QA、および NNM iSPI Performance for Traffic を合わせて 88GB • 仮想メモリ : RAM の 2 倍の容量 • インストールおよび動作のためのディスク容量 : NPS、NNM iSPI Performance for Metrics、NNM iSPI Performance for QA、および NNM iSPI Performance for Traffic を合わせて 6.5TB 空き容量をオペレーティングシステムとは別のドライブに確保することをお勧めします。 **注** : これは、最小保持期間の場合に適用される要件です。保持期間を長くする場合は、動作用のディスク容量を増加してください。 **注** : NNM iSPI for IP Multicast、NNM iSPI for IP Telephony、および NNM iSPI for MPLS は、NNMi と同時常駐する必要があります。これらの NNM iSPIs のいずれかをインストールする予定の場合は、NPS サーバーの要件値を次のように増加してください。 1　追加する各 NNM iSPI の対応マトリックスに基づいて、レポートデータのディスク容量要件を決定します。 2　この値を表 7 に示すディスク容量値に追加します。 利用可能な仮想メモリの容量は、インストール製品すべての合計 RAM 要件の 2 倍にしてください。 製品対応マトリックスのダウンロードの詳細については、「製品ドキュメント」(20 ページ) を参照してください。
オペレーティングシステム	**注** : NNMi 管理サーバーが Windows オペレーティングシステム上で稼動する場合は、NPS サーバーも Windows オペレーティングシステム上で稼動する必要があります。 • Windows: — Windows Server 2008 x64 Datacenter Edition Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition Service Pack 1 — Windows Server 2008 x64 Enterprise Edition Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition Service Pack 1 — Windows Server 2008 x64 Standard Edition Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition Service Pack 1 • Linux: — Red Hat Enterprise Linux Server 6.0 (またはそれ以降の 6.x までのマイナーバージョン) — Red Hat Enterprise Linux Server 5.4 (またはそれ以降の 5.x までのマイナーバージョン)

トラフィックマスターサーバー

表 8 に、NNM iSPI Performance for Traffic マスターコレクターをトラフィックマスターサーバーにインストールする場合の要件を示します。

表 8　トラフィックマスターサーバーの要件

エリア	最小要件
ハードウェア	• システム : — Windows または Linux: Intel 64 ビット (x86-64) または AMD 64 ビット (AMD64) ×8 CPU コア • RAM: 16GB • 仮想メモリ : RAM の 2 倍の容量 • インストールおよび動作時のディスク容量 : 800MB 空き容量をオペレーティングシステムとは別のドライブに確保することをお勧めします。
オペレーティングシステム	注 : NNM iSPI Performance for Traffic マスターコレクターと NNM iSPI Performance for Traffic リーフコレクターは、同じオペレーティングシステム上で実行することをお勧めします。 • Windows: — Windows Server 2008 x64 Datacenter Edition Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition Service Pack 1 — Windows Server 2008 x64 Enterprise Edition Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition Service Pack 1 — Windows Server 2008 x64 Standard Edition Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition Service Pack 1 • Linux: — Red Hat Enterprise Linux Server 6.0 (またはそれ以降の6.xまでのマイナーバージョン) — Red Hat Enterprise Linux Server 5.4 (またはそれ以降の5.xまでのマイナーバージョン)

トラフィックリーフサーバー

表 9 に、NNM iSPI Performance for Traffic リーフコレクターをトラフィックリーフサーバーにインストールする場合の要件を示します。

表 9　トラフィックリーフサーバーの要件

エリア	最小要件
ハードウェア	• システム : — Windows または Linux: Intel 64 ビット (x86-64) または AMD 64 ビット (AMD64) ×4 CPU コア • RAM: 16GB • 仮想メモリ : RAM の 2 倍の容量 • インストールおよび動作時のディスク容量 : 800MB 空き容量をオペレーティングシステムとは別のドライブに確保することをお勧めします。
オペレーティングシステム	注 : NNM iSPI Performance for Traffic マスターコレクターと NNM iSPI Performance for Traffic リーフコレクターは、同じオペレーティングシステム上で実行することをお勧めします。 • Windows: — Windows Server 2008 x64 Standard Edition Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition Service Pack 1 — Windows Server 2008 x64 Datacenter Edition Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition Service Pack 1 — Windows Server 2008 x64 Enterprise Edition Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition Service Pack 1 — • Linux: — Red Hat Enterprise Server AS 5.2 (またはそれ以降のマイナーバージョンから 5.x まで) — Red Hat Enterprise Server ES 5.2 (またはそれ以降のマイナーバージョンから 5.x まで)

NNM iSPI NET 診断サーバー

表 10 に、NNM iSPI NET を NNM iSPI NET 診断サーバーにインストールする場合の要件を示します。

表 10 NNM iSPI NET 診断サーバーの要件

エリア	最小要件
ハードウェア	• システム : — Windows: Intel 64 ビット (x86-64) または AMD 64 ビット (AMD64) • RAM: 2GB • インストールおよび動作時のディスク容量 : 2GB 空き容量をオペレーティングシステムとは別のドライブに確保することをお勧めします。
オペレーティングシステム	• Windows: — Windows Server 2008 x64 Datacenter Edition Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition Service Pack 1 — Windows Server 2008 x64 Enterprise Edition Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition Service Pack 1 — Windows Server 2008 x64 Standard Edition Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition Service Pack 1

製品ドキュメント

便宜上、HP 製品マニュアルの Web サイトにある Automated Network Management Suite カテゴリには、このマニュアル『ANM 設定ガイド』で参照している製品ドキュメントを含む ANM_Product_Docs_ja.zip ファイルが含まれています。製品ドキュメントは必要に応じて更新されます。ANM_Product_Docs_ja.zip ファイルは、ドキュメントの変更が含まれるように定期的に更新されます。

各 ANM 製品の完全で最新のドキュメントのセットは、HP 製品マニュアルの Web サイトから入手できます。21 ページの表 11 に、各 ANM 製品の検索カテゴリを示します。特定の製品のドキュメントを見つけるには、表 11 から製品名を選択し、製品バージョン **9.20** を選択して、それからオペレーティングシステムを選択します。使用しているソフトウェアバージョン (たとえば、9.20) と一致するドキュメントのバージョンを選択します。

HP 製品マニュアルの Web サイトにアクセスします。

http://support.openview.hp.com/selfsolve/manuals

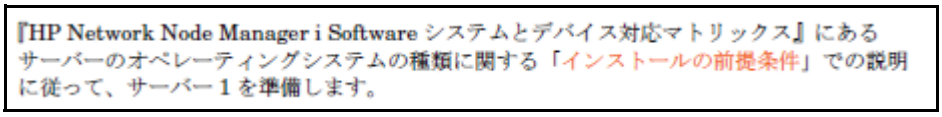
HP Passport アカウントを使用してこのサイトにアクセスするか、新しい HP Passport ID を登録してください。

ANM と製品ドキュメントの間のリンクの有効化

ANM のドキュメントとその関連製品のドキュメント (たとえば、Network Automation Software や Network Node Manager i Software) には、このドキュメントから関連製品ドキュメント内の特定の項や章に移動できるマーカーが組み込まれています。

別のPDFに移動する各リンクは、図 3に示すようなオレンジのテキストで見分けることができます。

図 3　外部 PDF へのリンクのフォーマット



この移動方法では、各製品ドキュメントの PDF ファイルに固有の名前が必要です。表 11 に、期待される名前を示します。ANM_Product_Docs_ja.zip ファイルに含まれるファイル名は、可能な限り正しい名前です。場合によっては、リンクを有効にするために、ファイル名に多少の変更を加える必要があります。

本項で説明する手順に従わない場合、関連製品ドキュメントの特定の項や章へのリンクは機能しません。その場合は、ANM のドキュメントで指定されている各項や各章に手動で移動できます。

ANM のドキュメントとその関連製品ドキュメントの間のリンク機能を有効にするには、次の手順を実行します。

1. ANMのドキュメントと関連製品のドキュメント用のディレクトリを作成します。次に例を示します。

   ```
   anm_docs
   ```

2. HP 製品マニュアルの Web サイトに接続します。

   http://support.openview.hp.com/selfsolve/manuals

3 Automated Network Management Suite カテゴリから、手順 1 で作成したディレクトリに次のファイルをダウンロードします。

- Automated Network Management コンセプトガイド
- Automated Network Management 設定ガイド
- ANM_Product_Docs_ja.zip

4 手順 1 で作成したディレクトに ANM_Product_Docs_ja.zip ファイルを解凍します。

5 表 11 の [**ファイルの保存名**] 列の値に突き合わせて、ファイル名を確認します。必要に応じて、ファイル名を次のように変更します。

- オペレーティングシステムの識別子をファイル名から削除します。たとえば、iSPI_Metrics_Install_Linux.pdf を iSPI_Metrics_Install.pdf に変更します。
- ローカライズされた言語の識別子をファイル名から削除します。たとえば、NA_Install_ko.pdf を NA_Install.pdf に変更します。

ファイル名は、大文字と小文字の表記を含め、指定した名前と一致する必要があります。

6 オプション。ANM_Product_Docs_ja.zip ファイルより新しい製品ドキュメントの場合は、HP 製品マニュアルの Web サイトにある製品の検索カテゴリからファイルをダウンロードし、表 11 の [**ファイルの保存名**] 列の値に従って名前を変更します。

表 11 ANM のドキュメントからリンクされる製品ドキュメント

製品の検索カテゴリ	参照ドキュメント	ファイルの保存名
network automation	HP Network Automation Support Matrix	NA_SupportMatrix.pdf
	HP Network Automation インストールおよびアップグレードガイド	NA_Install.pdf
	HP Network Automation ユーザーガイド	NA_User.pdf
network node manager	HP Network Node Manager i Software システムとデバイス対応マトリックス	NNMi_SupportMatrix.pdf
	HP Network Node Manager i Software 管理者用のヘルプ	NNMi_HelpAdmin.pdf
	HP Network Node Manager i Software デプロイメントリファレンス	NNMi_Deploy.pdf
	HP Network Node Manager i Software - HP Network Automation 統合ガイド	NNMi_NA_Integrate.pdf
	HP Network Node Manager i Software アップグレードリファレンス	NNMi_Upgrade.pdf
network node manager iSPI for NET	HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide	iSPI_NET_Install.pdf
	HP NNM iSPI Network Engineering Toolset Software Release Notes	iSPI_NET_ReleaseNotes.pdf

表 11 ANM のドキュメントからリンクされる製品ドキュメント (続き)

製品の検索カテゴリ	参照ドキュメント	ファイルの保存名
network node manager iSPI Performance for Metrics	HP Network Node Manager iSPI Performance for Metrics Software インストールガイド	iSPI_Metrics_Install.pdf
network node manager iSPI Performance for QA	HP Network Node Manager iSPI Performance for Quality Assurance Software インストールガイド	iSPI_QA_Install.pdf
	HP Network Node Manager iSPI Performance for Quality Assurance Software Intelligent Response Agent Installation Guide	iSPI_QA_iRA_Install.pdf
	HP Network Node Manager iSPI Performance for Quality Assurance 管理者用のヘルプ	iSPI_QA_HelpAdmin.pdf
network node manager iSPI Performance for Traffic	HP Network Node Manager iSPI Performance for Traffic Software インストールガイド	iSPI_Traffic_Install.pdf
	HP Network Node Manager iSPI Performance for Traffic オンラインヘルプ	iSPI_Traffic_Help.pdf
network node manager SPI for IP Multicast	HP Network Node Manager iSPI for IP Multicast Software Installation Guide	iSPI_Mcast_Install.pdf
network node manager SPI for IP Telephony	HP Network Node Manager iSPI for IP Telephony Software Installation Guide	iSPI_IPT_Install.pdf
network node manager SPI for MPLS VPN	HP Network Node Manager iSPI for MPLS Software Installation Guide	iSPI_MPLS_Install.pdf

2 ANM の設定

本章では、ANM のインストールおよび設定プロセスの概要を示します。

新規インストールの場合は、次の項のすべての手順を実行します。

- 「ANM のインストールと設定」(23 ページ)
- 「HP NNMi - HP NA 統合の検証」(30 ページ)
- 「ANM のライセンス」(31 ページ)

ANM 9.00 または 9.10 から ANM 9.20 へのアップグレードでは、次の項のすべての手順を実行します。

- 「ANM 9.10 から ANM 9.20 へのアップグレード」(32 ページ)
- 「HP NNMi - HP NA 統合の検証」(30 ページ)

ANM のインストールと設定

本項では、8 ページの図 1 の導入アーキテクチャー例の場合に ANM をインストールして設定する手順の概要を示します。詳細については、製品マニュアルを参照してください。製品マニュアルは、「製品ドキュメント」(20 ページ) の説明にある HP のマニュアル Web サイトから入手できます。

以下の点に注意してください。

- このソリューションを本稼働環境に配備する前に、テストラボで ANM を実行してみることをお勧めします。
- 特定の環境における ANM の設定について支援が必要な場合は、HP Professional Services Organization に連絡してください。
- ANM 製品に対する管理者アクセス権限を使用して、すべての設定手順を実行します。
- ANM 製品間でのシングルサインオンにより、繰り返しログオンしなくてもコンソールから別のコンソールに移動できます。ANM 設定プロセス中、管理者は NNMi と NA に別々にログオンする必要があります。
- ウイルス対策およびバックアップ用ソフトウェアが製品の実行中にファイルをロックし、製品の動作が妨げられる可能性があります。ファイルをロックするアプリケーションは、インストールおよびデータのディレクトリ (インストールプロセス時に選択) を除外するように設定してください。
- Windows 2008 には、ユーザーアクセス制御 (UAC) の概念が組み込まれています。管理者グループの一員になっているユーザーでも、完全な管理者権限を付与されていない場合があります。製品に関連付けられているすべてのスクリプトとコマンドでは、ユーザーに権限がないことを検出し、警告を表示します。スクリプトとコマンドは、完全な管理者アクセス権限で実行する必要があります。完全な管理者アクセス権限を獲得するには、**コマンドツール**アイコンを右クリックして、[**管理者として実行**] をクリックします。

ANM をインストールして設定するには、次のタスクを実行します。

- タスク 1: Web ブラウザーの準備
- タスク 2: NNMi のインストールと設定
- タスク 3: NPS および NNM iSPI Performance for Metrics のインストールと設定
- タスク 4: NNM iSPI Performance for QA のインストールと設定
- タスク 5: NNM iSPI Performance for Traffic マスターコレクターのインストール
- タスク 6: NNM iSPI Performance for Traffic リーフコレクターのインストールと設定
- タスク 7: NNM iSPI NET のインストールと設定
- タスク 8: NA のインストールと設定
- タスク 9: HP NNMi - HP NA 統合の設定

タスク 1: Web ブラウザーの準備

ANM サーバーにアクセスできるシステムで、『HP Network Node Manager i Software インタラクティブインストールガイド』の「NNMi コンソールにアクセスするための Web ブラウザーの設定」にある説明に従って、サポートされている Web ブラウザーを設定します。

ANM 製品間でシングルサインオンを利用するには、常に NNMi 管理サーバーの完全修飾ドメイン名を含んだ URL を指定して NNMi コンソールを起動してください。

タスク 2: NNMi のインストールと設定

まず NNMi をインストールし、それから他の ANM 製品をインストールします。

NNMi をインストールして設定するには、次の手順を実行します。

1 NNMi 管理サーバーが 13 ページの表 5 の一覧にある要件を満たしていることを確認します。

2 UNIX NNMi 管理サーバーのみ。『HP Network Node Manager i Software システムとデバイス対応マトリックス』にあるサーバーのオペレーティングシステムの種類 (HP-UX、Linux、または Solaris) に関する「インストールの前提条件」の説明に従って、NNMi 管理サーバーを準備します。

3 NNMi 管理サーバーで、『HP Network Node Manager i Software インタラクティブインストールガイド』の「NNMi 管理サーバーの準備」にある説明に従って、サーバー設定を確認します。

4 NNMi 管理サーバーで、『HP Network Node Manager i Software インタラクティブインストールガイド』の「NNMi の手動インストール」にある説明に従って、NNMi をインストールします。

5 NNMi コンソールで、使用するネットワークのさまざまなデバイスとエリアについて、アクセス資格証明および適切なタイムアウト値と再試行値を指定して NNMi を設定します。詳細については、NNMi の『管理者用のヘルプ』の「通信プロトコルを設定する」を参照してください。

6 NNMi コンソールで、NNMi の検出を設定します。詳細については、NNMi の『管理者用のヘルプ』の「検出を設定する」を参照してください。

7 NNMi 管理サーバーで、『HP Network Node Manager i Software デプロイメントリファレンス』の「1 つのドメインに対する SSO の有効化」にある説明に従って、NNMi のシングルサインオンを有効にします。

8 NNMi コンソールで、Web Service Client ロールで 2 人の NNMi ユーザーを作成します。

- NNM iSPI Performance for QA 用に 1 人の NNMi ユーザー。
- NNM iSPI Performance for Traffic 用に 1 人の NNMi ユーザー。

詳細については、NNMi の『管理者用のヘルプ』の「セキュリティの設定」を参照してください。

タスク 3: NPS および NNM iSPI Performance for Metrics のインストールと設定

前提条件 : NNMi は NNMi 管理サーバーにインストールされている必要があります。

NPS と NNM iSPI Performance for Metrics をインストールして設定するには、次の手順を実行します。

1 NNMi 管理サーバーで、『HP Network Node Manager iSPI Performance for Metrics Software インストールガイド』の「NNMi 管理サーバーでの NPS の有効化」にある説明に従って、NNM iSPI Performance for Metrics イネーブルメントスクリプトを実行します。

NNMi データファイルフォルダーのパスをメモします。この情報は手順 6 で必要です。

2 NPS サーバーが 16 ページの表 7 の一覧にある要件を満たしていることを確認します。

3 NPS サーバーで、『HP Network Node Manager iSPI Performance for Metrics Software インストールガイド』の「NPS のインストール」にある説明に従って、NPS をインストールします。

インストールは、約 1 時間インタラクションなしで実行します。

インストール時には、NNM iSPI Performance for Metrics のインストールも選択します。

4 NPS サーバーで、『HP Network Node Manager iSPI Performance for Metrics Software インストールガイド』の「設定ファイルの検証」にある説明に従って、インストールを確認します。

5 NNMi コンソールで、障害およびパフォーマンスポーリングを設定します。 詳細については、NNMi の『管理者用のヘルプ』の次のトピックを参照してください。

- 「インタフェースのベースライン設定を設定する」
- 「ノードコンポーネントのベースライン設定を設定する」
- 「インタフェースのしきい値モニタリングを設定する」
- 「ノードコンポーネントのしきい値モニタリングを設定する」

6 NPS サーバーで、次のパラメーターを設定します。

- NNMi データファイルフォルダーのパス (手順 1 の NNM iSPI Performance for Metrics イネーブルメントスクリプト)
- NNMi 管理サーバーの共有ドライブにアクセスするための資格証明
- アーカイブデータテーブルのデータ保持期間

NNMi からデータを受信するように NPS を設定するには、『HP Network Node Manager iSPI Performance for Metrics Software インストールガイド』の「Configuration Utility を使用した NPS の設定」にある説明に従って、NPS 設定ユーティリティを実行します。

タスク 4: NNM iSPI Performance for QA のインストールと設定

前提条件 :

- NNMi は NNMi 管理サーバーにインストールされている必要があります。
- NPS は NPS サーバーにインストールされている必要があります。

NNM iSPI Performance for QA をインストールして設定するには、次の手順を実行します。

1 NNMi 管理サーバーで、『HP Network Node Manager iSPI Performance for Quality Assurance Software インストールガイド』の「NNMi 管理サーバーへのインストール」にある説明に従って、NNM iSPI Performance for QA をインストールします。

2 オプション。NNMi 管理サーバーで、『HP Network Node Manager iSPI Performance for Quality Assurance Software Intelligent Response Agent Installation Guide』の「Installing the iRA on a Windows System」または「Installing the iRA on a Linux System」にある説明に従って、NNM iSPI Performance for QA Intelligent Response Agent (iRA) をインストールします。

iRA は、Windows および Linux オペレーティングシステムでのみ動作します。

3 NNMi 管理サーバーで、『HP Network Node Manager iSPI Performance for Quality Assurance Software 管理者向けのヘルプ』の「シングルサインオンの有効化」にある説明に従って、NNMi と NNM iSPI Performance for QA の間のシングルサインオンを設定します。

この設定により管理者ロールを持つ NNMi ユーザーは、ログオン資格証明を入力せずに、Quality Assurance の設定コンソールを開くことができるようになります。

4 NNMi コンソールで、NNMi が既存の QA プローブを検出するまで待ちます。

検出されたプローブは、[品質保証] ワークスペースのプローブテーブルビューに表示されます。

または、『HP Network Node Manager iSPI Performance for Quality Assurance Software 管理者向けのヘルプ』の「nmsqadisco.ovpl コマンドを使用した QA プローブの検出」にある説明に従って、検出プロセスの速度を高めます。

5 NNMi コンソールで、『HP Network Node Manager iSPI Performance for Quality Assurance Software 管理者向けのヘルプ』の「[プローブ設定] フォームの起動」にある説明に従って、QA プローブを設定します。

または、『HP Network Node Manager iSPI Performance for Quality Assurance Software 管理者向けのヘルプ』の「nmsqaprobeconfig.ovpl コマンドを使用した QA プローブの設定」にある説明に従って、コマンドラインインタフェースを使用して QA プローブを設定します。

6 NNMi コンソールで、『HP Network Node Manager iSPI Performance for Quality Assurance Software 管理者向けのヘルプ』の「[しきい値設定] フォームを使用した新規しきい値設定の追加」にある説明に従って、QA プローブでしきい値を設定します。

タスク 5: NNM iSPI Performance for Traffic マスターコレクターのインストール

前提条件 :

- NNMi は NNMi 管理サーバーにインストールされている必要があります。
- NPS は NPS サーバーにインストールされている必要があります。

NNM iSPI Performance for Traffic マスターコレクターをインストールして設定するには、次の手順を実行します。

1 NNMi 管理サーバーで、『HP Network Node Manager iSPI Performance for Traffic Software インストールガイド』の「HP NNMi Extension for iSPI Performance for Traffic のインストール」にある説明に従って、NNM iSPI Performance for Traffic 拡張をインストールします。

2 トラフィックマスターサーバーが 17 ページの表 8 の一覧にある要件を満たしていることを確認します。

3 トラフィックマスターサーバーで、『HP Network Node Manager iSPI Performance for Traffic Software インストールガイド』の「マスターコレクターのインストール」にある説明に従って、NNM iSPI Performance for Traffic マスターコレクターをインストールします。

タスク 6: NNM iSPI Performance for Traffic リーフコレクターのインストールと設定

前提条件 :

- NNMi は NNMi 管理サーバーにインストールされている必要があります。
- NPS は NPS サーバーにインストールされている必要があります。
- NNM iSPI Performance for Traffic マスターコレクターはトラフィックマスターサーバーにインストールされている必要があります。

NNM iSPI Performance for Traffic リーフコレクターをインストールして設定するには、次の手順を実行します。

1 トラフィックリーフサーバーが 18 ページの表 9 の一覧にある要件を満たしていることを確認します。

2 トラフィックリーフサーバーで、『HP Network Node Manager iSPI Performance for Traffic Software インストールガイド』の「リーフコレクターのインストール」にある説明に従って、NNM iSPI Performance for Traffic リーフコレクターをインストールします。

3 トラフィックマスターサーバーとトラフィックリーフサーバーで、『HP Network Node Manager iSPI Performance for Traffic Software インストールガイド』の「インストール後のタスク」にある説明に従って、手順を実行します。

4 NNMi コンソールで、NNM iSPI Performance for Traffic リーフコレクターのシステムとインスタンスを設定します。また、NNM iSPI Performance for Traffic マスターコレクターも設定します。詳細については、NNM iSPI Performance for Traffic ヘルプの「NNM iSPI Performance for Traffic の設定」を参照してください。

5 フローが有効なインタフェースの場合は、フローレコードを NNM iSPI Performance for Traffic リーフコレクターに送信するためのフロープロトコルを有効にします。

タスク 7: NNM iSPI NET のインストールと設定

前提条件 : NNMi は NNMi 管理サーバーにインストールされている必要があります。

NNM iSPI NET をインストールして設定するには、次の手順を実行します。

1. NNM iSPI NET 診断サーバーが 19 ページの表 10 の一覧にある要件を満たしていることを確認します。
2. NNM iSPI NET 診断サーバーで、『HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide』の「Installing the NNM iSPI NET Diagnostics Server and Diagnostic Flows」にある説明に従って、NNM iSPI NET をインストールします。

   インストールは、約 1 時間インタラクションなしで実行します。

3. NNMi コンソールで、『HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide』の「NNMi Management Server Preparation」にある説明に従って、診断フローを実行するためのデバイス資格証明を指定します。
4. NNMi コンソールで、1 つ以上の NNMi インシデントについての NNM iSPI NET 診断を設定します。詳細については、『HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide』の「NNM iSPI NET Diagnostics」を参照してください。

タスク 8: NA のインストールと設定

NA をインストールして設定するには、次の手順を実行します。

1. NA サーバーが 15 ページの表 6 の一覧にある要件を満たしていることを確認します。
2. NA サーバーで、『HP Network Automation インストールおよびアップグレードガイド』の「NA のインストール」にある説明に従って、NA をインストールします。
3. NA サーバーで、『HP Network Automation インストールおよびアップグレードガイド』の「最新の NA ドライバパックのインストール」にある説明に従って、最新のドライバパックをインストールします。
4. NA デバイスのパスワードルールを設定します。詳細については、『HP Network Automation ユーザーガイド』の「デバイスパスワードルールの作成」を参照してください。
5. NA デバイスの設定を行います。詳細については、『HP Network Automation ユーザーガイド』の「デバイス構成の管理」を参照してください。
6. NA デバイスのポリシーを設定します。詳細については、『HP Network Automation ユーザーガイド』の「ポリシー保証の管理」を参照してください。

タスク 9: HP NNMi - HP NA 統合の設定

前提条件 :

- NNMi は NNMi 管理サーバーにインストールされている必要があります。
- NA は NA サーバーにインストールされている必要があります。

HP NNMi - HP NA 統合を設定するには、次の手順を実行します。

1 NNMi コンソールで、『HP Network Node Manager i Software - HP Network Automation 統合ガイド』の「新規統合設定」にある説明に従って、HP NNMi - HP NA 統合を設定します。

   - [HP NNMi - HP NA の統合設定] フォームで、次の選択を行います。
     - [**トポロジフィルターノードグループ**] は未設定のままにして、統合によって NNMi トポロジ全体が NA インベントリと同期されるようにします。
     - [**トポロジ同期間隔 (時間)**] を 0 以外の値に設定します。
     - [**NA のデバイスドライバの検出**] チェックボックスをオンにします。
     - [**NA 接続チェック間隔 (時間)**] を 0 以外の値に設定します。
     - [**分析ペインデータのための最小 NNMi ロール**] を、使用環境に適した NNMi ロールレベルの 1 つ (「なし」以外) に設定します。
   - NNMi と NA 間で Secure Sockets Layer (SSL) 通信を行うため、2 つの製品間で証明書を必ず交換します。

2 『HP Network Node Manager i Software - HP Network Automation 統合ガイド』の「NNMi と HP NA 間のシングルサインオンの設定」にある説明に従って、NNMi と NA 間のシングルサインオンを設定します。

HP NNMi - HP NA 統合の検証

HP NNMi - HP NA 統合が正常に有効化されたことを検証するには、次の手順を実行します。

1 管理者ロールを持つユーザーとして NNMi コンソールにログオンします。

2 NNMi コンソールで、NA SNMP トラップインシデントの設定が適切に行われていることを検証します。

a [SNMP トラップの設定] ビューを開きます ([**設定**] > [**インシデント**] > [**SNMP トラップの設定**])。

b 「**NASnmpTrapv1**」および「**NASnmpTrapv2**」という名前のトラップ定義を見つけます。

3 管理者権限を持つユーザーとして NA にログオンします。

4 NA コンソールで、NA インベントリが NNMi トポロジと一致することを確認します。

a ホームページ上部のメニューで、[**デバイス**] > [**インベントリ**] を選択します。

b NNMi の一覧にあるすべてのデバイスが NA にインポートされたことを確認します。

[**トポロジフィルターノードグループ**] 設定でノードグループを指定した場合は、そのノードグループのデバイスのみを NA にインポートする必要があります。

5 NA コンソールで、[**管理**] > [**サードパーティ統合**] > [**NNM 統合接続テスト**] をクリックします。

正常に終了したことを示すメッセージが表示されます。

エラーメッセージが表示された場合は、統合が正しく設定されていることを確認するか、サポート担当者に連絡してください。

ANM のライセンス

NNMi と NNM iSPIs の恒久ライセンスキーは、NNMi 管理サーバーの IP アドレスと関連付けられています。

NA の恒久ライセンスキーは、NA サーバーの IP アドレスと関連付けられています。

ANM のライセンスを取得するには、次の手順を実行します。

1 NNMi 管理サーバーで、次のライセンスキーを NNMi 管理サーバーにインストールします。

- ネットワーク内のすべてのノードの管理を有効にするために必要な、1 つ以上の NNMi ライセンスキー。手順については、『HP Network Node Manager i Software インタラクティブインストールガイド』の「NNMi のライセンス」を参照してください。
- 1 つの NNM iSPI NET ライセンスキー。手順については、『HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide』の「License NNM iSPI NET」を参照してください。
- ネットワーク内のすべてのノードのパフォーマンスレポートを有効にするために必要な、1 つ以上の NNM iSPI Performance for Metrics ライセンスキー。手順については、『HP Network Node Manager iSPI Performance for Metrics Software インストールガイド』の「NNM iSPI Performance ライセンス」を参照してください。
- 1 つ以上の iSPI ポイントライセンスキー。このライセンスキーは、NNM iSPI NET と NNM iSPI Performance for Metrics を除くすべての NNM iSPIs に適用されます。これらの NNM iSPIs を使用するための十分な iSPI ポイントを確保してください。iSPI ポイントが累積する仕組みとライセンスキーのインストール方法の詳細については、次のマニュアルを参照してください。
  - 『HP Network Node Manager iSPI Performance for Quality Assurance Software インストールガイド』の「ライセンスに関連する情報」
  - 『HP Network Node Manager iSPI Performance for Traffic Software インストールガイド』の「ライセンス」
  - 『HP Network Node Manager iSPI for IP Multicast Software Installation Guide』の「License-related Information」
  - 『HP Network Node Manager iSPI for IP Telephony Software Installation Guide』の「License Information」
  - 『HP Network Node Manager iSPI for MPLS Software Installation Guide』の「License-related Information」
- 各 NNM iSPI Performance for Traffic リーフコレクターの 1 つのコレクター接続ソフトウェア LTU ライセンスキー。手順については、『HP Network Node Manager iSPI Performance for Traffic Software インストールガイド』の「ライセンス」を参照してください。

2 NA サーバーで、NA ライセンスキーを 1 つインストールします。手順については、『HP Network Automation インストールおよびアップグレードガイド』の「NA ライセンスの取得と配布」を参照してください。

ANM 9.10 から ANM 9.20 へのアップグレード

本項では、8 ページの図 1 の導入アーキテクチャー例の場合に ANM をアップグレードする手順の概要を示します。詳細については、製品マニュアルを参照してください。製品マニュアルは、「製品ドキュメント」(20 ページ) の説明にある HP のマニュアル Web サイトから入手できます。

データ喪失を回避するには、次の点を確認します。

- この手順を完了する前に、NNM iSPI Performance for QA と NNM iSPI Performance for Traffic のバージョンが 9.11 (9.1x パッチ 1) になっている必要があります。
- NNM iSPI Performance for Traffic マスターまたはリーフが NNMi 管理サーバーにインストールされている場合は、この手順を完了する前に、NNMi が 9.1x パッチ 3 (以降) であり、NNM iSPI Performance for Traffic が 9.1x パッチ 2 (以降) になっている必要があります。

NPS、NNM iSPI Performance for Metrics、NNM iSPI Performance for Traffic マスターまたはリーフのいずれかが NNMi 管理サーバーにインストールされている場合は、アップグレード手順に追加の手順が含まれます。それらの製品ドキュメンのアップグレード手順に従ってください。

ANM 9.10 から ANM 9.20 にアップグレードするには、次の手順を実行します。

1 NPS サーバーで、次のコマンドを実行してすべての NPS データをバックアップします。

- Windows:

```
%NPSInstallDir%¥bin¥backup.ovpl -b <dir>
```

- UNIX:

```
/opt/OV/NNMPerformanceSPI/bin/backup.ovpl -b <dir>
```

スケジュールされたレポート用にレポートビューを作成した場合は、アップグレード中にビューが保存されます。Query Studio を使用して作成したスケジュール、ジョブ、クエリーも保存されます。ただし、ショートカットや他のオブジェクトタイプは保存されません。アップグレード結果を調べるには、ログディレクトリにある `Migration.log` ファイルのログエントリーを確認します。

2 NPS サーバーで、次のコマンドを実行して NPS プロセスを停止します。

- Windows:

```
%NPSInstallDir%¥bin¥stopALL.ovpl
```

- UNIX:

```
/opt/OV/NNMPerformanceSPI/bin/stopALL.ovpl
```

3 トラフィックリーフサーバーで、次のコマンドを実行してリーフコレクターを停止します。

- Windows:

```
%TrafficInstallDir%¥nonOV¥traffic-leaf¥bin¥
nmstrafficleafstop.ovpl
```

- UNIX:

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

4 トラフィックマスターサーバーで、次のコマンドを実行してマスターコレクターを停止します。

- Windows:

```
%TrafficInstallDir%¥nonOV¥traffic-master¥bin¥
nmstrafficmasterstop.ovpl
```

- UNIX:

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

5 『HP Network Node Manager i Software アップグレードリファレンス』の「NNMi 9.0x または 9.1x からのアップグレード」にある説明に従って、NNMi をアップグレードします。

6 『HP Network Node Manager iSPI Performance for Metrics Software インストールガイド』の「専用サーバーでの NPS のアップグレード」にある説明に従って、NPS と NNM iSPI Performance for Metrics をアップグレードします。

NPS 設定ユーティリティウィンドウが表示されたら、[**終了**] をクリックしてキャンセルします。

7 『HP Network Node Manager iSPI Performance for Quality Assurance Software インストールガイド』の「NNM iSPI Performance for QA のアップグレード」にある説明に従って、NNM iSPI Performance for QA をアップグレードします。

8 『HP Network Node Manager iSPI Performance for Traffic Software インストールガイド』の「NNM iSPI Performance for Traffic のアップグレード」にある説明に従って、NNM iSPI Performance for Traffic をアップグレードします。

9 NPS サーバーで、次のコマンドを実行して NPS プロセスを開始します。

- Windows:

```
%NPSInstallDir%¥bin¥startALL.ovpl
```

- UNIX:

```
/opt/OV/NNMPerformanceSPI/bin/startALL.ovpl
```

10 『HP NNM iSPI Network Engineering Toolset Software Release Notes』の「Upgrading from NNM iSPI NET diagnostics server version 9.10」にある説明に従って、NNM iSPI NET をアップグレードします。

11 『HP Network Automation インストールおよびアップグレードガイド』の「別のシステムからの NA 9.20 へのアップグレード」または「同一システムでの NA 9.20 へのアップグレード」にある説明に従って、NA をアップグレードします。

12 NNMi コンソールで、HP Network Node Manager i Software—HP Network Automation 統合ガイドの「NNMi 9.1x から NNMi 9.20 にアップグレードされた統合設定」にある説明に従って、HP NNMi ó HP NA 統合をアップグレードします。

NNMi と NA 間で Secure Sockets Layer (SSL) 通信を行うため、2 つの製品間で証明書を必ず交換します。

3 ANM シナリオ例の設定

本章では、ANM シナリオ例の設定プロセスの概要を示します。前提として、ANM が第 2 章、ANM の設定の説明に従って設定されているものとします。

内容は以下のとおりです。

- 「例 1: 非適合デバイス変更を識別して修正する」(36 ページ)
- 「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」(39 ページ)
- 「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」(40 ページ)
- 「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」(41 ページ)
- 「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」(42 ページ)
- 「例 6: エッジルーターで期待されるサービスレベルを確保する」(44 ページ)
- 「例 7: 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」(45 ページ)
- 「例 8: エラーレートと使用率の問題を識別して修正する」(46 ページ)

例 1: 非適合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。ANM 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、デバイス設定が期待される以外の設定になっている場合に通知を生成することができます。ANM 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、前の設定を使用するようにデバイスをリセットしたりするためのツールを用意しています。

シナリオ例の前提条件

- 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」(36 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。
- ANM 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」(36 ページ).
- 「デバイスの設定変更時にポリシー適合チェックタスクを実行するように NA を設定する」(37 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」(37 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、次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。

以下の手順に従ってください。

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適合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適合性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、次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 [**ポリシー適合チェック**] に設定します。

4 [新規タスク / テンプレート - ポリシー適合チェック] 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、ポリシー非適合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、次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。

シナリオ例の概要

シナリオ例の前提条件を満たした後は、次のようにして ANM 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、新しい設定で適合チェックを自動的に実行します。
2. NA は、非適合について記述した 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. 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。
4. NA コンソールで、実行設定への配備タスクを実行してデバイス設定をロールバックします。
5. NA がデバイスに適切な設定を復元し、新しい設定を収集します。次に NA は、自動的に新しい設定の適合性をチェックします。

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。ANM は、デバイスについてクエリーを自動的に実行することができ、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提供します。

シナリオ例の前提条件

- 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。
- ANM 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。

シナリオ例の概要

シナリオ例の前提条件を満たした後は、次のようにして ANM 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、診断レポートを開き、OSPF 近隣接続が INIT 状態のまま留まっているかどうか判断します。
4. NA コンソールで、OSPF 近隣接続ルーターの診断レポートを表示し、ACL 設定エラーを確認します。
5. 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。
6. 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: 非適合デバイス変更を識別して修正する」で処理します。

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。ANM 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します。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。

シナリオ例の前提条件

- デバイスは NNMi トポロジに含まれている必要があります。
- ネットワークの対象エリアの少なくとも 1 つのデバイスで、NetFlow または sFlow プロトコルが有効になっている必要があります。

  または、トラフィックフローエクスポートを使用できます。NetFlow プロトコルは、NetFlow エクスポートを NNM iSPI Performance for Traffic リーフコレクターサーバーに送信するように設定され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。

シナリオ例の概要

シナリオ例の前提条件を満たした後は、次のようにして ANM 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. NetFlow 対応の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、10 分待機してから [**パフォーマンス**] タブを更新して、更新されたトラフィックのグラフを表示します。

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。ANM は、現在使用中の IPv4 アドレスの収集と管理対象デバイスの IPv6 アドレスの設定の両方を自動的に処理できます。

シナリオ例の前提条件

- 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。

シナリオ例の概要

シナリオ例の前提条件を満たした後は、次のようにして ANM 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. 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。

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。ANM 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。ANM は、デバイス設定を更新して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ツールを提供します。

シナリオ例の前提条件

- 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。
- ネットワークの対象エリアの少なくとも 1 つのデバイスで、NetFlow または sFlow プロトコルが有効になっている必要があります。

  または、トラフィックフローエクスポートを使用できます。NetFlow プロトコルは、NetFlow エクスポートを NNM iSPI Performance for Traffic リーフコレクターサーバーに送信するように設定され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」(42 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、手順 2 から手順 4 を繰り返します。

シナリオ例の概要

シナリオ例の前提条件を満たした後は、次のようにして ANM 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 NA コンソールで、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。

4 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。

例 6: エッジルーターで期待されるサービスレベルを確保する

ネットワーク管理の観点からは、サーバーをすべてのユーザーが利用可能な状態で維持することが重要です。ビジネス管理の観点からは、インターネットサービスプロバイダー (ISP) から購入した一定レベルのサービスの提供を受けることが重要です。ANM は、企業のネットワークの外部にあるデバイスの応答性を監視し、応答性が許容レベルを下回った場合には通知を生成することができます。

シナリオ例の前提条件

- エッジルーターは NNMi トポロジに含まれている必要があります。
- IP SLA テストがエッジルーターで設定されている必要があります。
- IP SLA テストは NNM iSPI Performance for QA インベントリに含まれている必要があります。
- IP SLA テストのメトリックスのしきい値が設定されている必要があります。

シナリオ例の概要

シナリオ例の前提条件を満たした後は、次のようにして ANM を使用できます。

1. NNMi は、エッジルーターからの IP SLA テストの特定のメトリックス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. NNMi インシデントの分析ペインで、IP SLA テストの最近の値を示す QA グラフを表示した [**パフォーマンス**] タブを開きます。
3. ISP に問題を通知します。

例 7: 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。ANM 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になった場合には通知を生成することができます。

シナリオ例の前提条件

- 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。
- NNM iSPI 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。

シナリオ例の概要

シナリオ例の前提条件を満たした後は、次のようにして ANM 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 サイトに向かう HTTP トラフィックに関して、高ボリュームのデータを示す管理イベント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から、NNM iSPI Performance for Traffic インシデントで示されるインタフェースを開きます。

   [**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. NA コンソールで、Web サーバーをホストしているデバイスの ACL を変更して、攻撃元からのトラフィックを拒否します。
7. 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。

例 8: 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。ANM 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。

シナリオ例の前提条件

- 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」(46 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、手順 2 から手順 4 を繰り返します。

シナリオ例の概要

シナリオ例の前提条件を満たした後は、次のようにして ANM 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、接続の両端それぞれにあるルーターの [デバイス設定の違い] ページを開き、このインタフェースで設定されている全二重を確認し、デバイス設定が最近変更されたかどうかを調べます。
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 NA コンソールから、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。

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、**ovdoc-nsm@hp.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 : ANM 9.20

ドキュメントタイトル : ANM 設定ガイド

フィードバック :