テクニカルホワイトペーパー

NNMi を導入するためのステップバイステップガイド

Network Node Manager i Software 10.10

2015 年 11 月

内容

目的

このドキュメントでは、小規模なテストネットワークにおける新規の NNMi 10.10 インストールの導入について説明します。このドキュメントには、NNMi を本番ネットワークに導入する場合と同様の手順が記載されています。

このドキュメントを読み、『HP Network Node Manager iSoftware デプロイメントリファレンス』をリソースとしてご使用ください。このリファレンスには、このドキュメントの技術的な範囲を超えた詳細情報が多数記載されています。

注: 最新の『HP Network Node Manager iSoftware デプロイメントリファレンス』を見つけるには、以下を参照してください。h20230.www2.hp.com/selfsolve/manuals

---

基本ステップ: ロードマップ

このドキュメントでは、以下の前提条件を満たしていることが想定されています。

- NNMi がインストールされている。
- サーバーが http://h20230.www2.hp.com/selfsolve/manuals で入手できる『HP Network Node Manager i Software システムとデバイス対応マトリックス』に記載されたパッチ要件やカーネルパラメーターも含めて、システムの前提条件をすべて満たしている。

注: NNMi インストールスクリプトは、サーバーがシステムの前提条件を満たしているか確認しません。これらの前提条件を無視すると、インストール完了後に問題が発生する可能性があります。

このドキュメントには、NNMi が Linux サーバーにインストールされている場合の例が記載されています。NNMi が Windows サーバーにインストールされている場合は、パスやコマンドを Windows サーバー用に変換してください。

注: 最新の『HP Network Node Manager i Software デプロイメントリファレンス』を見つけるには、以下を参照してください。h20230.www2.hp.com/selfsolve/manuals

---

このドキュメントでは、以下のタスクについて説明します。

1. ライセンスの適用
2. 元の設定のバックアップ
3. NNMi へのサインインとユーザーの作成
4. 通信の設定
5. 検出の設定
6. モニタリングの設定
7. インシデント、トラップ、および自動アクションの設定
8. NNMi コンソールの設定
9. NNMi の保守
10. NNMi ヘルスの確認

また、ベストプラクティスや使用シナリオの例も含まれています。

以下のトピックについては、http://h20230.www2.hp.com/selfsolve/manuals にある『HP Network Node Manager i Software デプロイメントリファレンス』を参照してください。

- セキュリティグループおよびマルチテナント
- HP Operations Manager (HP OM)、HP Universal Configuration Management Database (HP UCMDB) などの他の HP 製品や他社製品との統合
- 高可用性またはアプリケーションフェイルオーバー
- リモート Oracle データベースの使用
- NNM iSPI (NNM iSPI for Performance や NNM iSPI for MPLS など)

NNMi iSPI をインストールするには、http://h20230.www2.hp.com/selfsolve/manuals にある以下のドキュメントを参照してください。

- NNM iSPI Performance for Metrics インタラクティブインストールガイド
- NNM iSPI Performance for Traffic インタラクティブインストールガイド
- NNM iSPI Performance for QA インタラクティブインストールガイド
- NNM iSPI Performance for QA Intelligent Response Agent インタラクティブインストールガイド

NNMi iSPI を導入するには、http://h20230.www2.hp.com/selfsolve/manuals にある以下のドキュメントを参照してください。

- NNM iSPI Performance for Metrics デプロイメントリファレンス
- NNM iSPI Performance for Traffic デプロイメントリファレンス
- NNM iSPI Performance for QA デプロイメントリファレンス

ライセンスの適用

インスタントオンライセンスを使用するか、より大きな一時ライセンスをHPから取得することができます。

NNMiのライセンス構造や、企業向けインストールにライセンス層を追加する方法の詳細については、HP 営業担当者または Hewlett-Packard 正規販売店にお問い合わせください。ライセンスキーを追加取得するには、HP ライセンスキー配信サービスサイト (https://webware.hp.com/welcome.asp)(英語サイト)を参照してください。

注: インスタントオンライセンスは NNMi Ultimate を対象としており、250 のノードで NNMi を有効にすることができます。後日 NNMi Premium をインストールすると、一部の機能が使用できなくなります。NNMi Ultimate および NNMi Premium の機能の詳細については、『HP Network Node Manager i Software リリースノート』 (http://h20230.www2.hp.com/selfsolve/manuals) を参照してください。

ライセンスはコマンドラインを使用してインストールできます。以下に、nnmlicense.ovpl スクリプトを使用してライセンスをインストールする場合のコマンド例を示します。

nnmlicense.ovpl NNM -f ./mylicense.key

元の設定のバックアップ

変更を行う前に、元の NNMi 設定のバックアップを作成します。こうすることで、必要に応じて元の設定に戻すことができます。

元の NNMi の設定をバックアップするには、以下の手順を実行します。

1. 元の設定ファイルを保持するディレクトリをNNMi管理サーバー上に作成します。この例では、/var/tmp/origconfig というディレクトリを作成します。
2. -c および-f オプションを使用して、nnmconfigexport.ovpl コマンドを実行します。–c オプションですべての設定を指定し、 –f オプションでディレクトリを指定します。

   以下に、 nnmconfigexport.ovpl スクリプトを実行する場合のコマンド例を示します。

   nnmconfigexport.ovpl -c all -f /var/tmp/origconfig/
   nnmconfigexport.ovpl スクリプトを実行すると、NNMi に以下のような出力が表示されます。
   /var/tmp/origconfig/incident.xml を正常にエクスポートしました。
   /var/tmp/origconfig/status.xml を正常にエクスポートしました。
   …
   /var/tmp/origconfig/account.xml を正常にエクスポートしました。
   /var/tmp/origconfig/securitymappings.xml を正常にエクスポートしました。
   /var/tmp/origconfig/security.xml を正常にエクスポートしました。

NNMi へのサインインとユーザーの作成

初期サインイン

Internet Explorer や Mozilla Firefox などのブラウザーを使用して、NNMi にアクセスします。以下のような URL を使用します (インストールプロセスで通信用として選択したサーバー名とポートを挿入)。

http://<serverName>:<port number>/nnm

図 1: NNMi サインイン画面

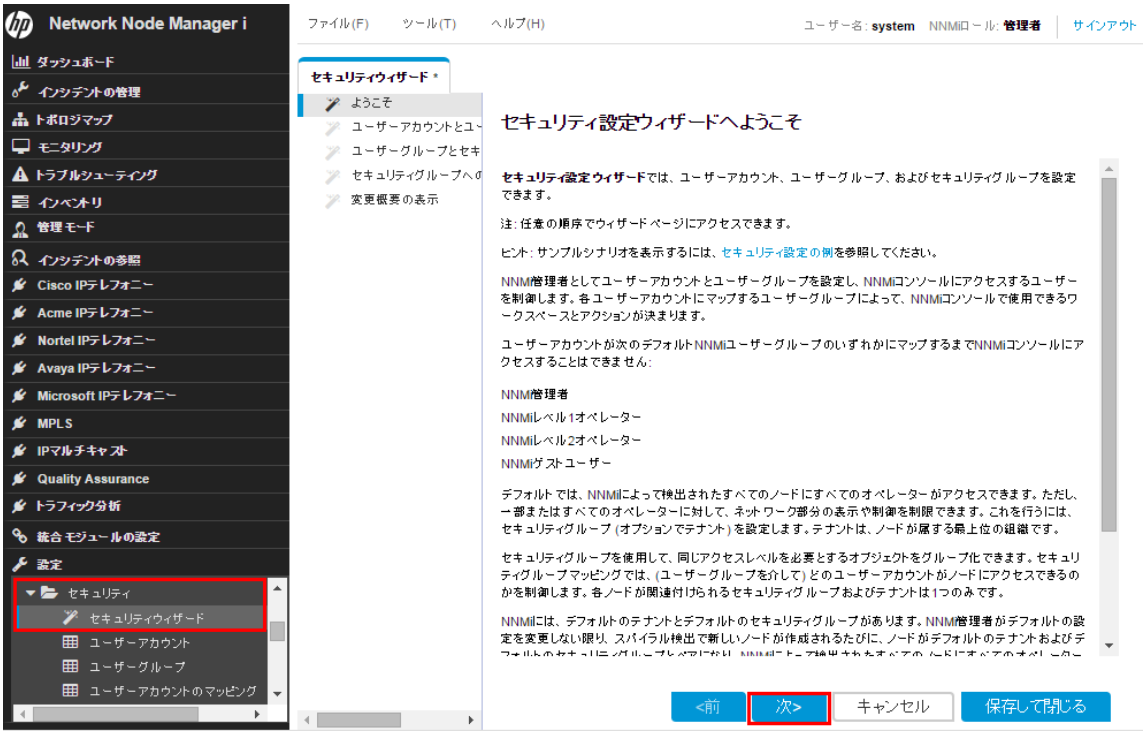
ユーザーアカウントとロールの作成

ほとんどの場合において、システムユーザー名は使用しないでください。作業のほとんどで利用可能な管理者アカウントを作成して使用するには、以下の手順を実行します。

1. ワークスペースのナビゲーションパネルで [**設定**] ワークスペースを選択します。
2. [**セキュリティ**] フォルダーを展開します。
3. [**セキュリティウィザード**] をクリックします。

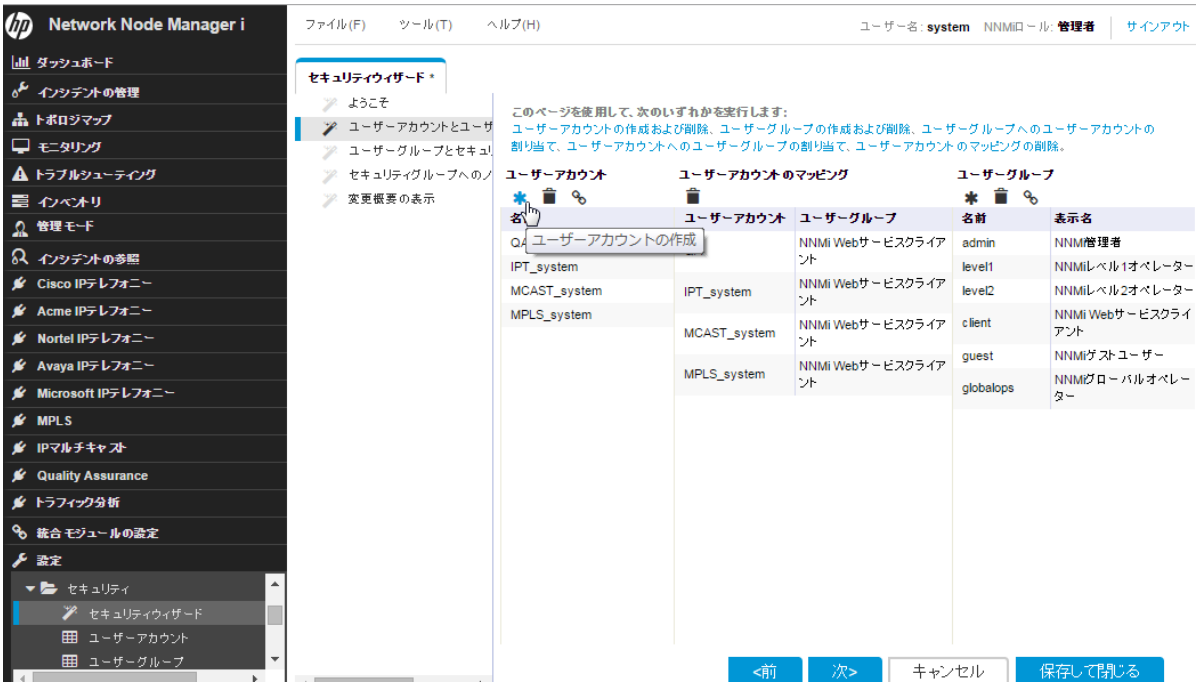
[**セキュリティウィザード**] の [ようこそ] ページが表示されます。

図 2: セキュリティウィザード: [ようこそ] ページ



4. [**ユーザーアカウントとユーザーグループのマップ**] ページの [**ユーザーアカウント**] で、✱ をクリックします。

図 3: セキュリティウィザード: ユーザーアカウントの作成



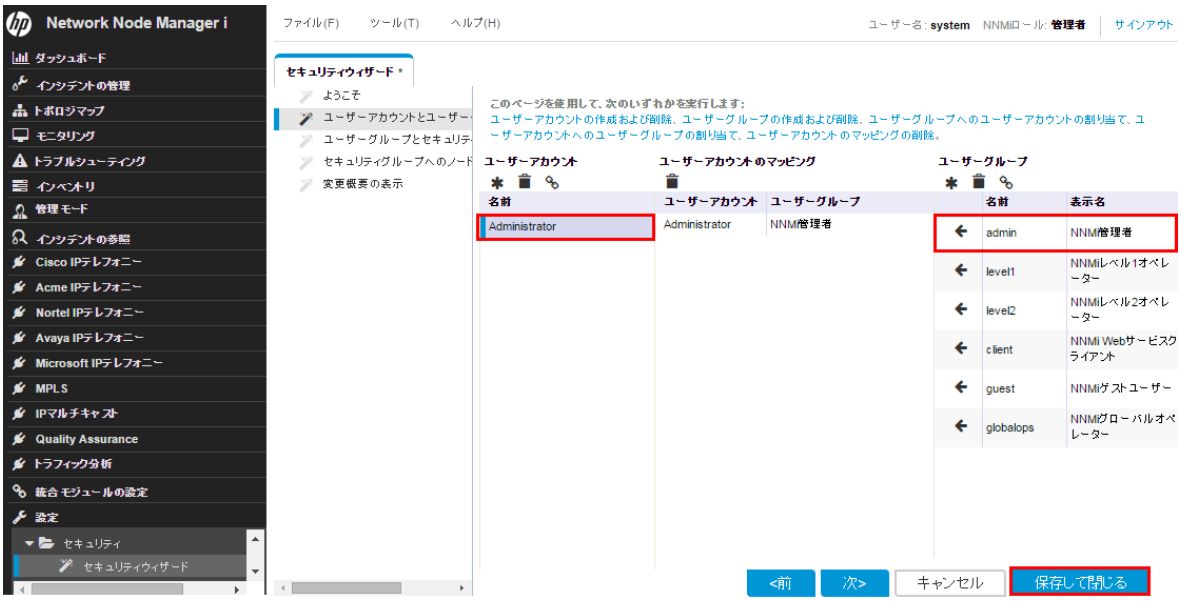
5. [**ユーザーアカウントの作成**] ダイアログボックスでアカウント情報を入力し、[**追加**] > [**閉じる**] をクリックします。

図 4: セキュリティウィザード: [ユーザーアカウントの作成] ダイアログボックス

6. [**ユーザーアカウント**] 列で新しいアカウント名をクリックし、適切なユーザーグループの横の ← アイコンをクリックして [**ユーザーアカウントのマッピング**] を作成します。
7. [**閉じる**] をクリックし、[**OK**] > [**OK**] をクリックして変更を受け入れます。**図 5** を参照してください。

ヒント: 旧バージョンの NNMi での「ロール」の概念は、ユーザーアカウントのマッピングで置き換えられています。

図 5: セキュリティウィザード: ユーザーアカウントへのユーザーグループのマップ



8. NNMi からサインアウトします。次に、新しいユーザーアカウント名を使用してサインインし、正しく動作することを確認します。

通信の設定

デフォルトで、NNMi は SNMP コミュニティ文字列の検出を実行します。この例では、このデフォルトの方法の使い方が説明されています。

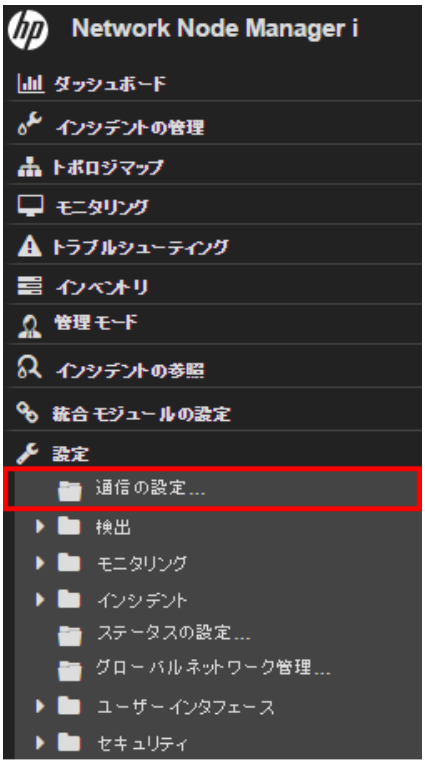
デフォルトで、NNMi はすべての可能なコミュニティ文字列を順番に試行します。NNMi によって、ノードからの応答になる最初のコミュニティ文字列がそのノードの SNMP コミュニティ文字列として選択されます。この例では、デフォルトのコミュニティ文字列のみが設定されています。この設定ではより複雑なソリューションを実装できますが、ほとんどの場合、この方法で十分です。

ヒント: コミュニティ文字列の数が少ない場合は、デフォルトのコミュニティ文字列のみ設定するのが最善です。

---

1. ワークスペースのナビゲーションパネルで [**設定**] ワークスペースを選択してから [**通信の設定**] をクリックします。

図 6: 通信の設定

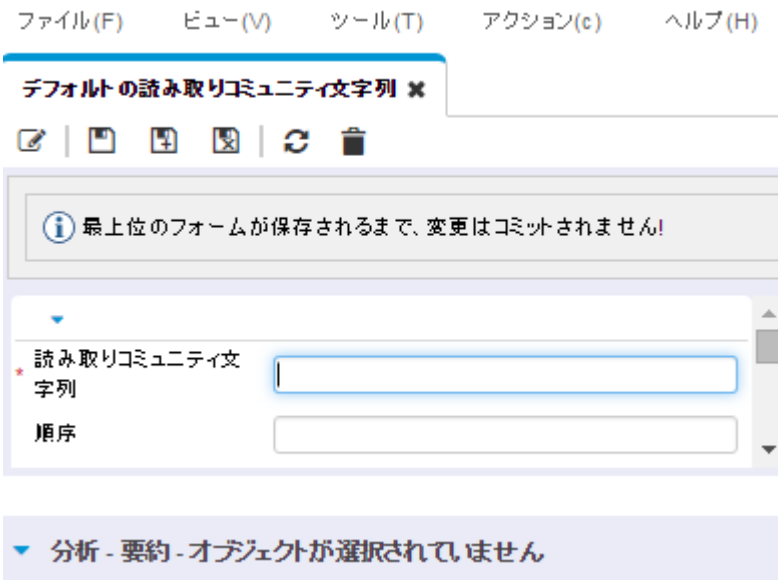


2. [**デフォルトの SNMPv1/v2 コミュニティ文字列**] タブをクリックし、 ✱ アイコンをクリックして新しいコミュニティ文字列を作成します。

図 7: 通信の設定: [デフォルトの SNMPv1/v2 コミュニティ文字列] タブ

3. コミュニティ文字列を入力し、 [**保存して閉じる**] をクリックします。

図 8: デフォルトの読み取りコミュニティ文字列



4. すべてのコミュニティ文字列に対して前の手順を繰り返します。

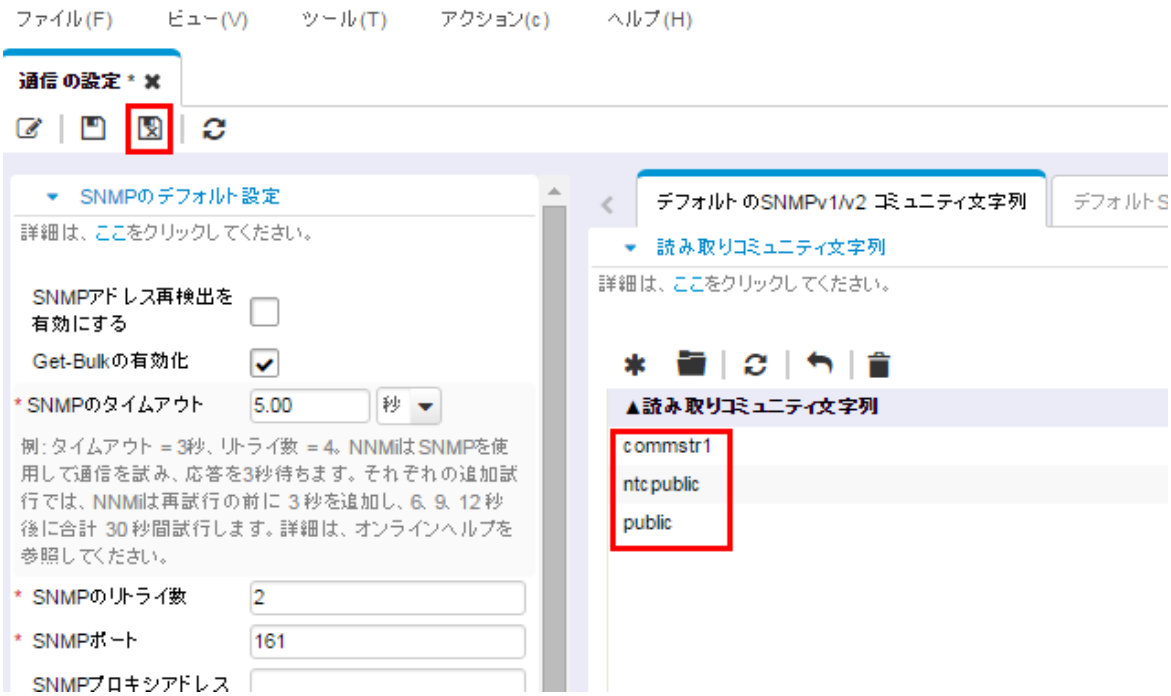
ヒント: 追加の変更を行う場合は、その他の [**通信**] 設定オプションを調べます。

---

5 コミュニティ文字列の設定が完了したら、[**通信の設定**] フォームの [**保存して閉じる**] をクリックして変更内容を保存します。

SNMP 設定はこれで完了です。

図 9: 通信の設定: 保存して閉じる



検出の設定

NNMi では、検出の方法としてリストベースと自動の 2 つの方法がサポートされています。それぞれの方法にメリットがあります。

リストベース検出では、ノード名または IP アドレスのリストを入力として使用し、そのリストに含まれているノードのみを検出します。NNMi は、このリストに含まれていないノードや IP アドレスを検出しません。この方法では、NNMi で検出および管理するノードを制御できます。リストの各ノードは、シードと呼ばれます。

注: NNMi は、各シードの IP アドレスが自動検出の範囲外にあったとしてもロードします。

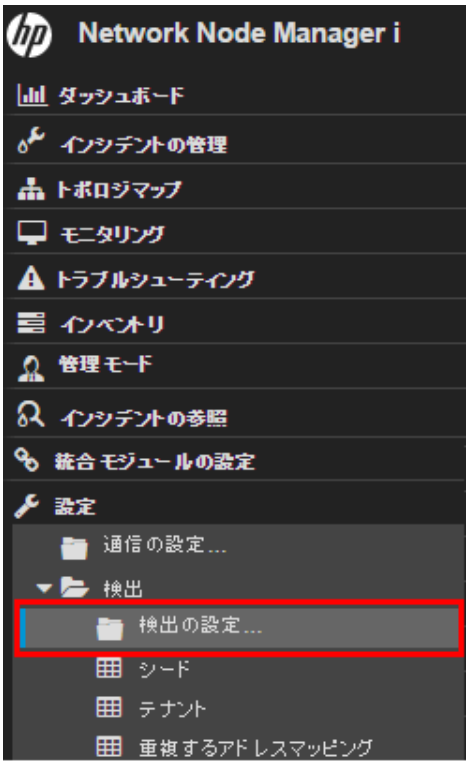
ヒント: シードをデバイスの IP アドレスとしてロードする場合、優先管理アドレス (通常、Cisco ギアのあるループバックアドレス) をシードとして指定することをお勧めします。

自動検出は、ユーザー指定の基準に基づいてネットワーク上のノードを検出します。検出するノードをアドレス範囲、SNMP 値 (システムオブジェクト ID)、デバイスタイプなどのメソッドによって制限するように NNMi を設定できます。単一のシードノードで自動検出を設定できます。ただし、追加で利用可能な Ping スイープ機能を有効にした場合、このノードも不要です。

以下の例では、アドレス範囲に基づいた自動検出について説明します。さらに、この例では 2 つのシードノードをロードする方法も示します。

1. ワークスペースのナビゲーションパネルで [**設定**] ワークスペースを選択し、[**検出**] フォルダーを展開して、[**検出の設定**] をクリックします。

図 10: 検出の設定



2. [**自動検出ルール**] タブをクリックし、✱ アイコンをクリックして新しいルールを作成します。

図 11: 検出の設定: 自動検出ルール

3. [**基本**] セクションに入力します。

ヒント: NNMi は [**順序**] 属性値を使用して複数の自動検出ルールに優先順位を設定します。この例では、1 つの自動検出ルールのみが使用されています。

図 12: 自動検出ルール: [順序] 属性

4. ✱ アイコンをクリックし、このルールの IP 範囲の入力画面を開きます。

5. [**IP 範囲**] テキストボックスに、検出する IP 範囲を入力します。包括的なルール (ルールに含める) と排他的なルール (ルールにより無視された) の両方を入力できます。排他的なルールは、包括的なルールよりも優先されます。

図 13: IP の自動検出範囲

6. このフォームおよび [**自動検出ルール**] フォームの [**保存して閉じる**] をクリックし、変更内容を保存します。

この例では、Ping スイープ機能を使用しません。

ヒント: 自分の環境で Ping スイープ機能を使用することを選択すると、NNMi は各自動検出ルールについて最大でクラス B ネットワーク (たとえば 10.2.*.*) 全域でスイープします。

以下の点に注意してください。

- デフォルトでは、NNMi は定義した IP アドレス範囲内のルーターとスイッチのみを検出します。スイッチとルーター以外のノードを検出するには、他のデバイスを含むシステム オブジェクト ID 範囲を追加します。
- ルーターのようにノードに複数のアドレスがある場合、IP アドレス範囲内にあるのは 1 つのアドレスのみである必要があります。このアドレスは、ループバック アドレスである必要はありません。ループバックアドレス以外のアドレスを入力した場合、NNMi は最初に予想した以上にノードを検出することがあります。

これで自動検出ルールを定義できました。各ルールはきわめて複雑になる可能性があるため、ほとんどの場合、必要な自動検出ルールは 1 つのみです。

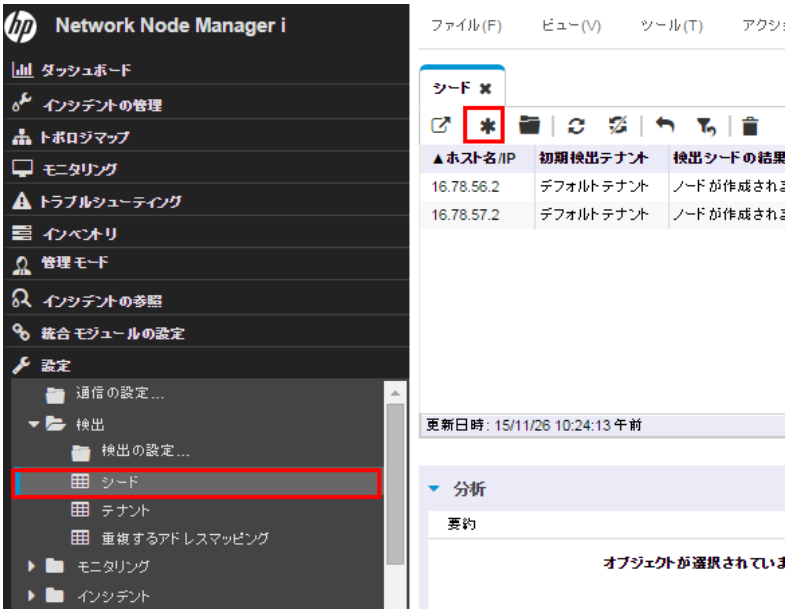
次の例では、シードノードを追加する方法が説明されています。

ヒント: ルーターにはNNMi が検出するアドレスがたくさんあるため、ルーターはスイッチではなくシードとして追加することをお勧めします。

---

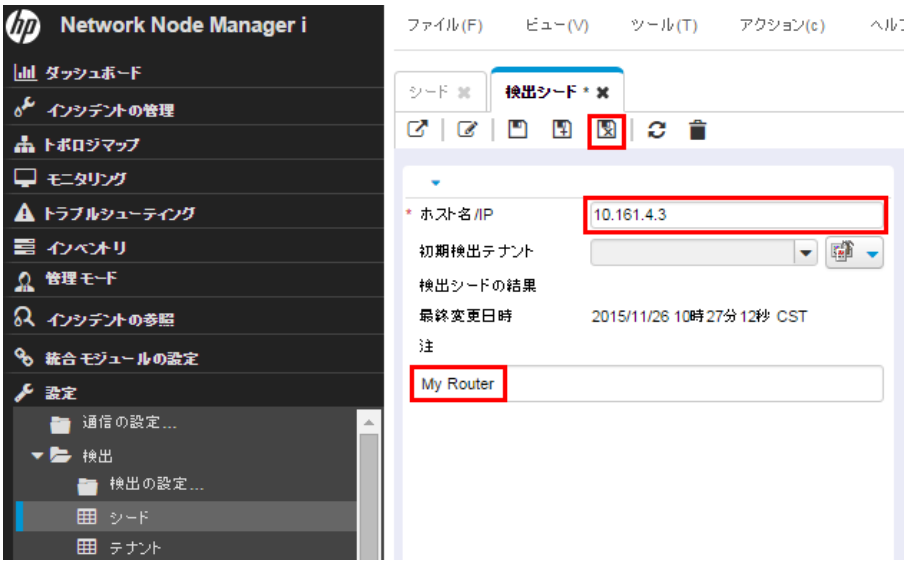
1. ワークスペースのナビゲーションパネルで [**設定**] ワークスペースを選択し、[**検出**] フォルダーを展開して、[シード] をクリックします。
2. ✱ アイコンをクリックして新しいシードを作成します。

図 14: ディスカバリ: シード



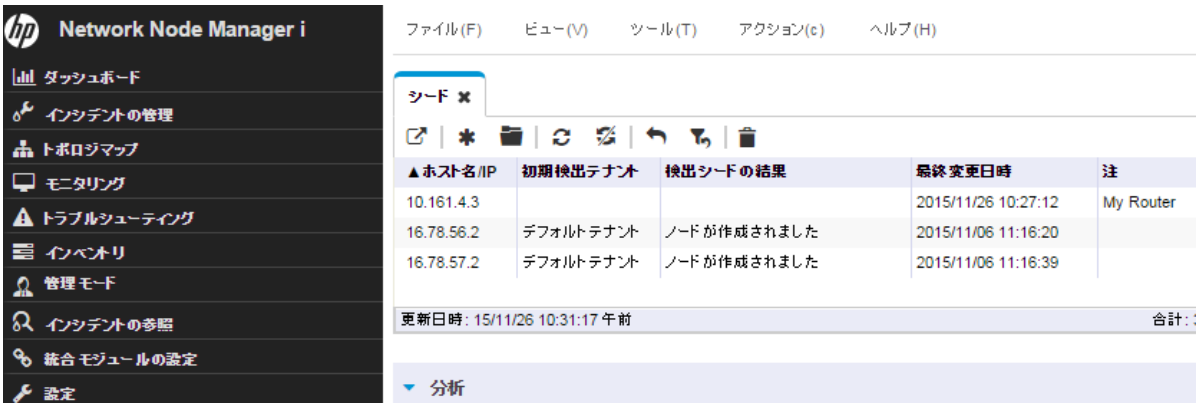
3. [**検出シード**] フォームでホスト名またはIP アドレスを、および必要に応じて [**メモ**] を入力し、[**保存して閉じる**] をクリックします。

図 15: シード: 検出シード



ヒント: [シード] テーブルの [**検出シードの結果**] 列を確認し、各シードの検出ステータスを判断します。NNMi がノードの検出を開始すると、NNMi は進行状況を [進行中] と表示します。検出が完了すると、[**検出シードの結果**] エントリが [ノードが作成されました] に変わります。

図 16: シード: 検出シードの結果



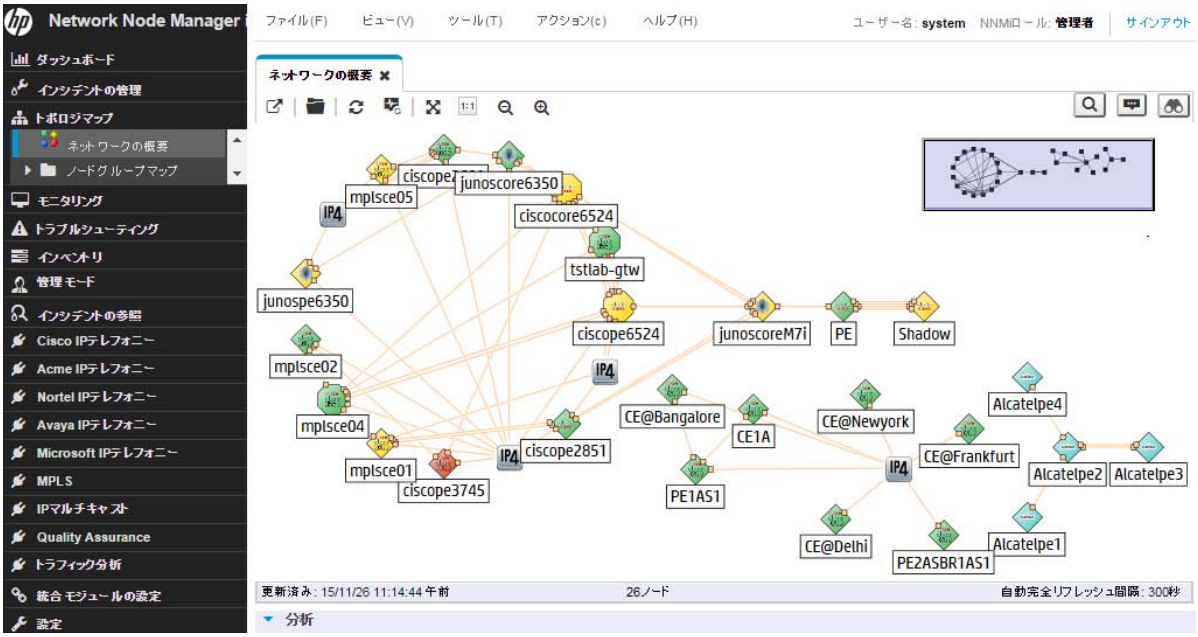
ヒント: nnmloadseeds.ovpl スクリプトを使用してファイルからすべてのシードをロードすることもできます。このスクリプトでは、多数のシード ノードをロードできます。自動検出ルールではなくリストベース検出を使用する場合、nnmloadseeds.ovpl スクリプトを使用してすべてのノードをロードできます。詳細については、nnmloadseeds.ovpl のリファレンスページ、または Linux のマンページを参照してください。

自動検出メソッドを使用する場合、自動検出は自動検出ルールで指定したアドレス範囲内のアドレスを持つその他のスイッチおよびルーターの検出を開始します。NNMi では、最初はステータスが表示されない状態でノードが表示されます。最終的に、検出された各ノードのステータスが表示されます。

[**ネットワークの概要**] マップは限られた数のノードおよび接続を表示するため、小規模な環境で検出の進行状況を表示するのに役立ちます。

ヒント: [**ネットワークの概要**] マップの [リフレッシュ] をクリックし、初期ノードを表示します。

図 17: トポロジマップ: ネットワークの概要



ハイパーバイザーと仮想マシンの検出の設定

NNMi では、ハイパーバイザーでホストされている仮想マシン (VM) と、それらの VM およびハイパーバイザーにおける L2 接続を一緒に検出できます。

以下の例は、1 つのハイパーバイザーと、そのハイパーバイザーでホストされている VM の検出を設定する方法を示しています。

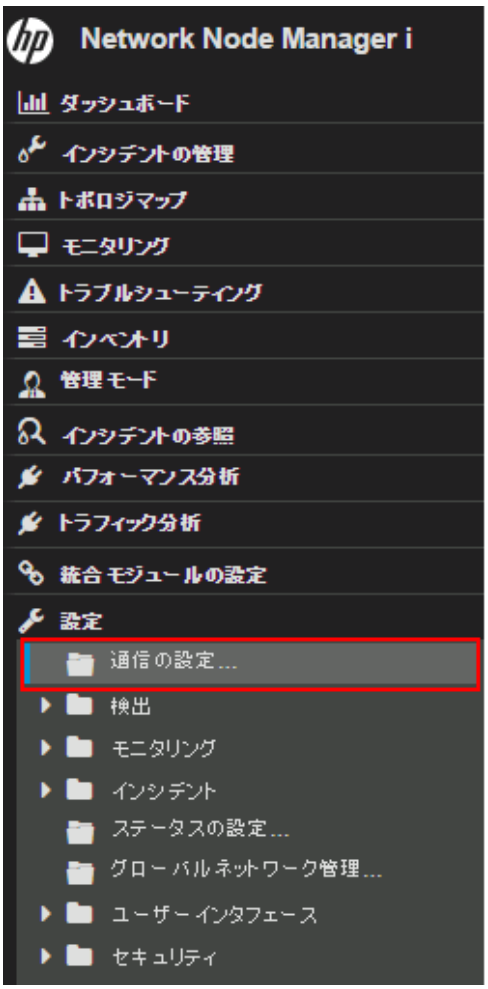
注: ハイパーバイザーサーバーから SSL 証明書のコピーを取得する必要があります。この証明書の取得方法については、『HP Network Node Manager i Software デプロイメントリファレンス』を参照してください。

注: この例は、このドキュメントの「通信の設定」の説明に従って NNMi 通信設定がすでに完了していることも前提にしています。

---

1. ワークスペースのナビゲーションパネルで [**設定**] ワークスペースを選択してから [**通信の設定**] をクリックします。

図 18: 通信の設定

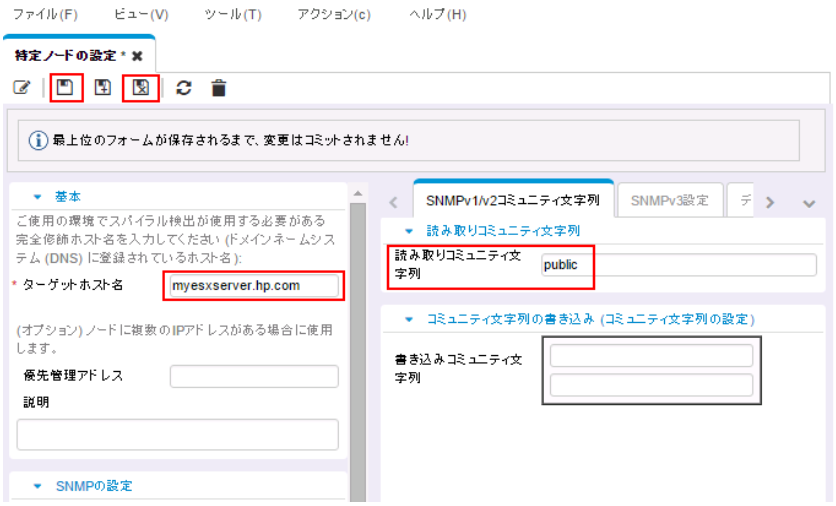


2. [**特定ノードの設定**] タブをクリックして ✱ アイコンをクリックし、新しい設定を作成します。

図 19: 通信の設定: [特定ノードの設定] タブ

3. [**ターゲットホスト名**] フィールドにハイパーバイザーの FQDN、[**読み取りコミュニティ文字列**] フィールドにハイパーバイザーの SNMP 読み取りコミュニティ文字列を入力し、[**保存**] をクリックします。その他の設定は、デフォルト値が使用されるように未設定のままにしておいてください。

図 20: 特定ノードの設定の作成



4. [**デバイスの資格証明**] タブをクリックして ✱ アイコンをクリックし、新しい資格証明を作成します。

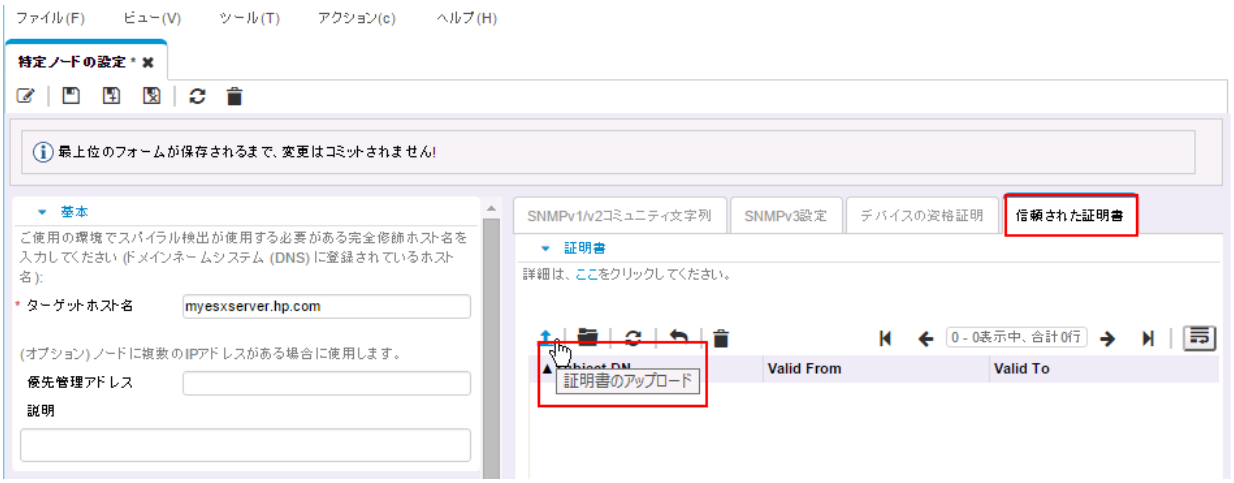
図 21: 特定ノードの設定 – [デバイスの資格証明] タブ

5. [**タイプ**] ボックスで VMware を選択し、ハイパーバイザーに対する資格証明を入力し、[**保存して閉じる**] アイコン をクリックします。

図 22: 特定ノードの設定 – 新しいデバイス資格証明

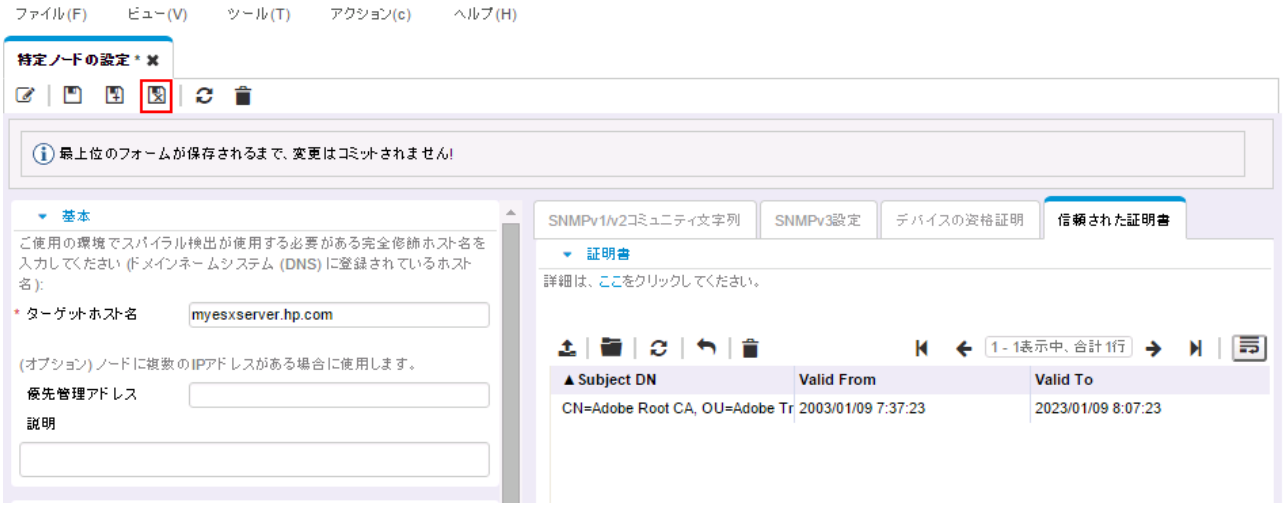
6. ハイパーバイザーの SSL 証明書をインポートするには、[**信頼された証明書**] タブをクリックし、[**証明書のアップロード**] をクリックします。

図 23: 特定ノードの設定 – [信頼された証明書] タブ



7. [**保存して閉じる**] アイコン をクリックします。

図 24: 特定ノードの設定 – ハイパーバイザーの証明書の保存



8. [特定**ノードの設定**] の設定が完了したら、[**通信の設定**] フォームの [**保存して閉じる**] アイコン をクリックして変更内容を保存します。以上でハイパーバイザーの設定は完了です。同じ手順を繰り返してハイパーバイザーをさらに追加できます。

図 25: 通信の設定: 保存して閉じる

ヒント: ハイパーバイザーと VM の検出の設定は、nnmcommunication.ovpl スクリプトを使用しても実行できます。設定をすべて行うには、以下の方法で nnmcommunication.ovpl コマンドを 3 回繰り返します。

nnmcommunication.ovpl -createNodeSettings -name <*FQDN*> -icmpEnabled true -snmpEnabled true -snmpGetBulk true -snmpCommunity <*read string*>

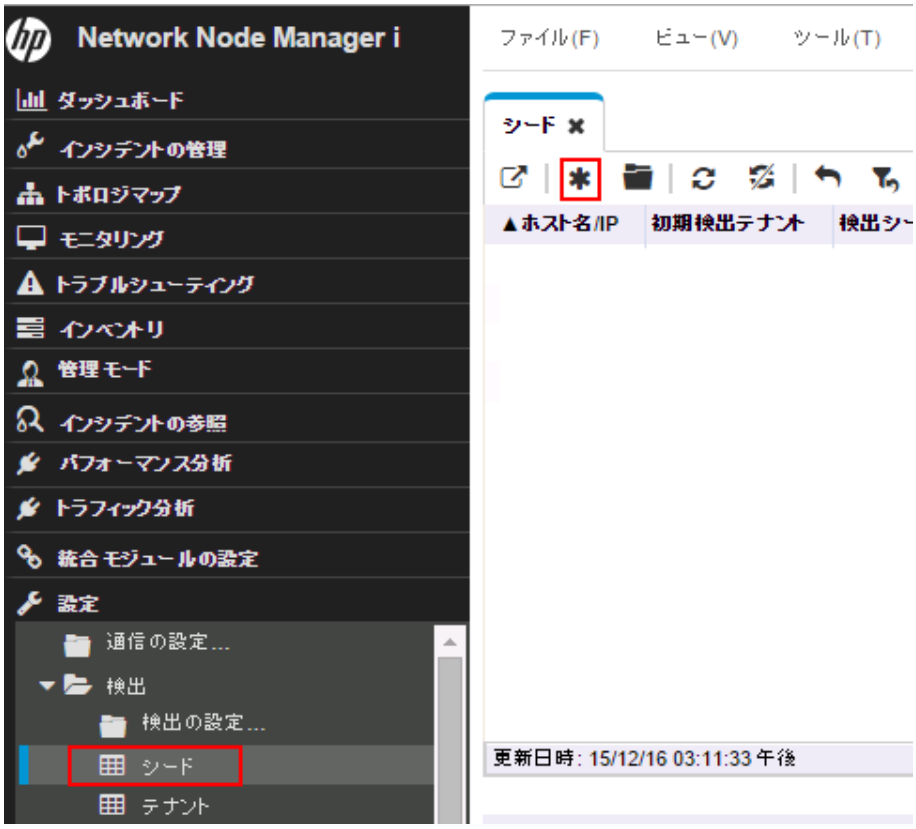
nnmcommunication.ovpl -addCredential -nodeSetting <*FQDN*> -type VMWARE -username <*user name*> -password <*password*>

nnmcommunication.ovpl -addCertificate -nodeSetting <*FQDN*> -cert <*certificate*>

---

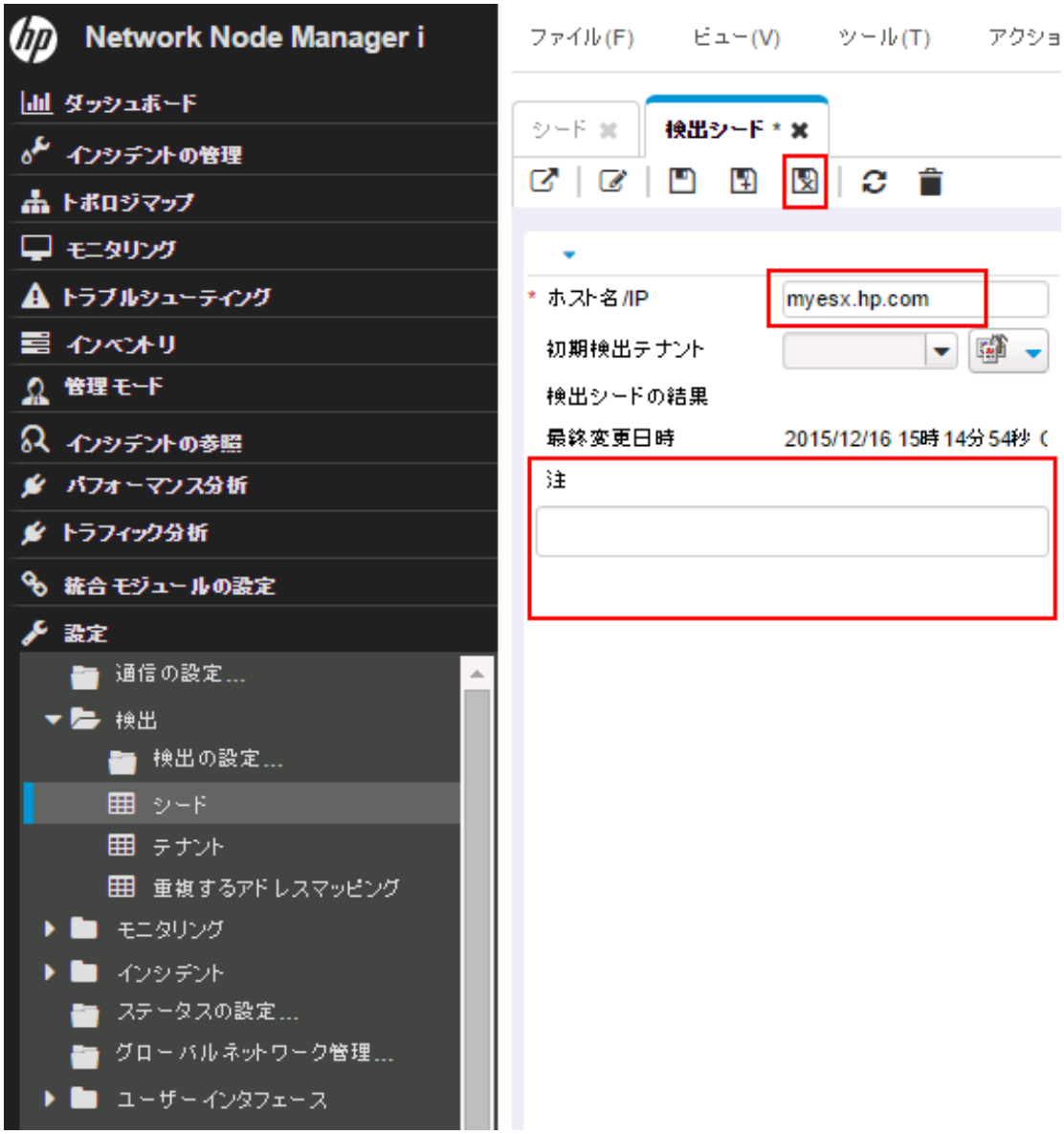
9. ハイパーバイザーをシードとしてロードし、その後で NNMi にこれを検出させます。ワークスペースのナビゲーションパネルで [**設定**] ワークスペースを選択し、[**検出**] フォルダーを展開して、[**シード**] をクリックします。✱ アイコンをクリックして新しいシードを作成します。

図 26: 検出 – 新しいシードの作成



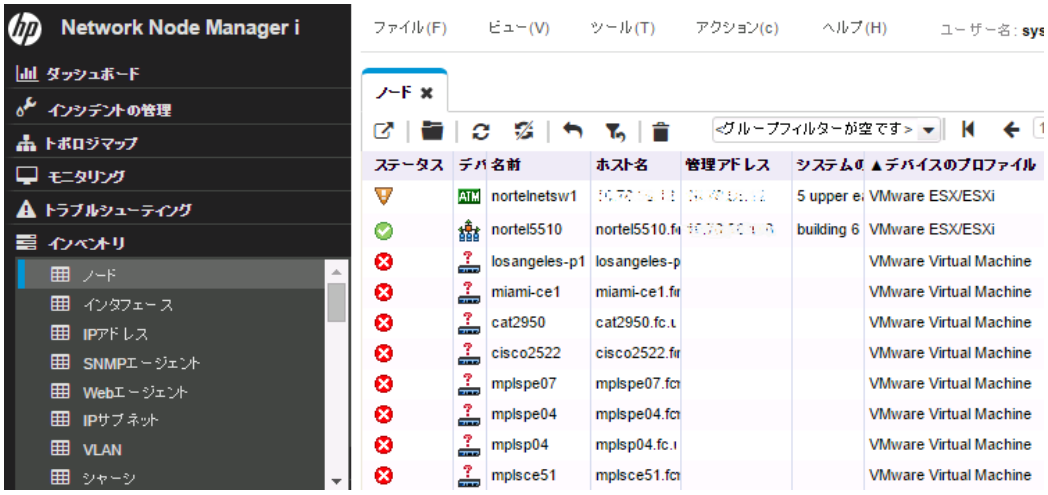
10. [**検出シード**] フォームで、ハイパーバイザーのホスト名または IP アドレスを指定し、必要に応じてメモを入力して、[**保存して閉じる**] アイコン をクリックします。

図 27: 検出 – シードとしてのハイパーバイザーの追加



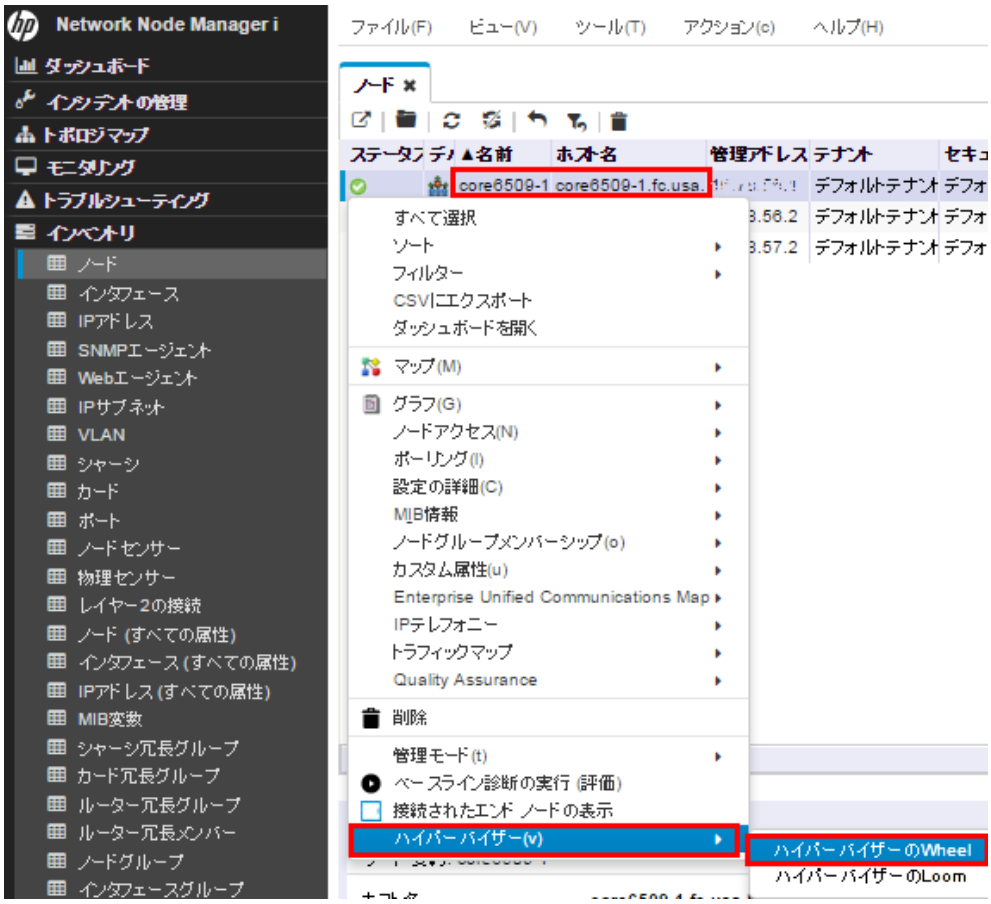
11. 結果を確認します。NNMiが検出を完了するまで数分待ちます。ワークスペースのナビゲーションパネルで[**インベントリ**]ワークスペースを選択して、[**ノード**]を選択します。ハイパーバイザーと、サーバー上でホストされているすべてのVMが[ノード]テーブルビューに表示されます。

図 28: ハイパーバイザーとその VM を表示したノードリスト



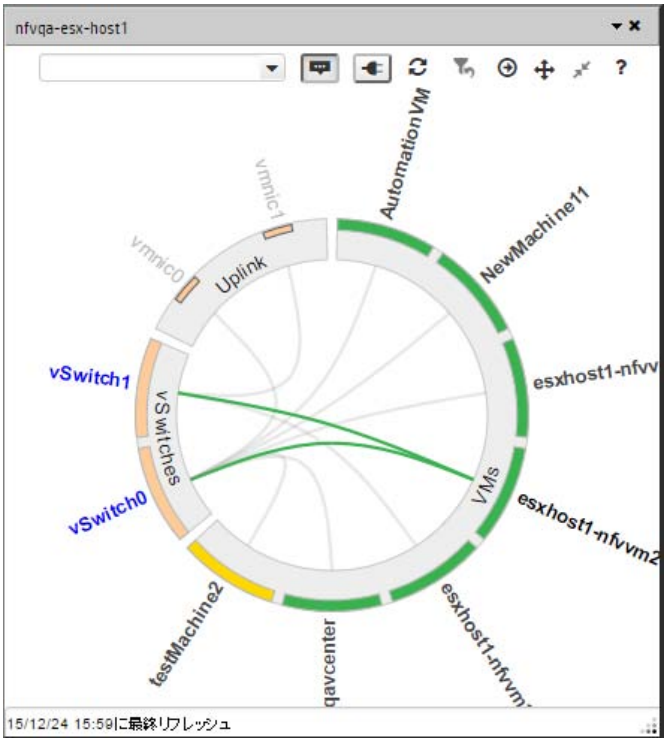
12. ハイパーバイザーとその VM 内の vSwitch、vNIC、および L2 接続を表示します。
13. テーブルビューで、ハイパーバイザー名を右クリックして [**ハイパーバイザー**] をクリックし、[**ハイパーバイザーの Wheel**] をクリックします。

図 29: [ハイパーバイザーの Wheel] メニュー項目



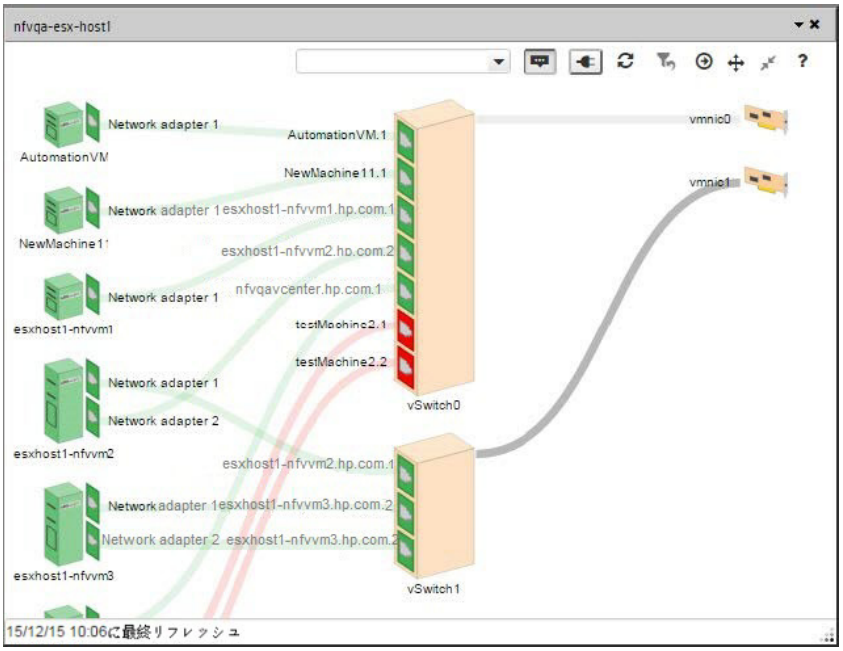
14. ハイパーバイザーの Wheel 図には、仮想スイッチと L2 接続が示されます。

図 30: 仮想スイッチと L2 接続が示されたハイパーバイザーの Wheel 図



[ハイパーバイザーの Loom] メニュー項目を選択してハイパーバイザーの Loom 図を表示することもできます。

図 31: 仮想スイッチと L2 接続が示されたハイパーバイザーの Loom 図



モニタリングの設定

NNMi のモニタリングには柔軟性があり、設定が簡単です。NNMi では、ICMP (ping) ポーリングではなく SNMP ポーリングがデフォルトで使用されます。この場合の例外は非 SNMP ノードであるということで、NNMi はこれらのノードを ICMP を使用してポーリングします。ICMP ポーリングは、必要に応じてより広範囲で有効にすることができます。

デフォルトで NNMi は、接続されているインタフェースをポーリングします。NNMi の接続インタフェースは、NNMi トポロジで接続されているインタフェースです。ケーブルで接続されたインタフェースへのマッピングが常に含まれているわけではありません。

以下のシナリオについて考えます。

- 48 ポート搭載のアクセススイッチが、デスクトップコンピューターと 1 つのアップリンクポートに接続されている。
- NNMi はアップリンクノードを検出したが、デスクトップコンピューターは検出していない。

この場合、デスクトップコンピューターへの接続が認識されないため、そのアップリンクポートのみが NNMi に接続済みとみなされます。一般的に、これが適切な動作になります。通常、夜間にコンピューターがオフになるたびに NNMi から通知される必要はありません。

以下の例において、c2900xl-1 スイッチは、アップリンク (Fa0/2) が 1 つのアクセススイッチです。**図 33: [ノード] フォーム: インタフェースのリスト**に示すように、1 つのインタフェースのみが監視されます。

図 32: マップビュー: 1 つのインタフェースをモニタリング

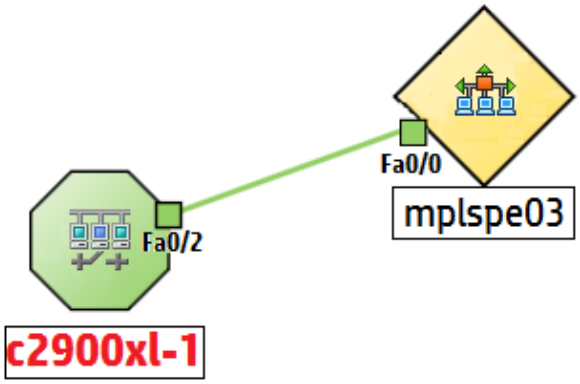
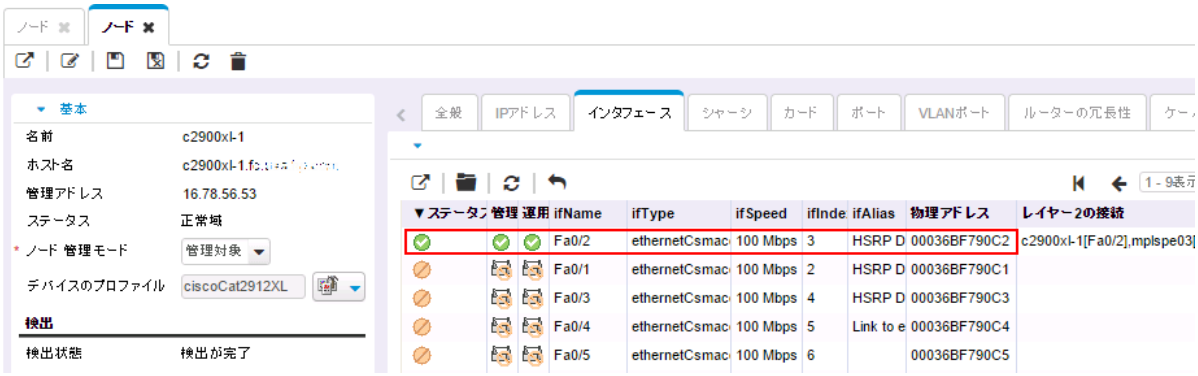


図 33: [ノード] フォーム: インタフェースのリスト



2 番目のデフォルトの動作がルーターに適用されます。ルーターの場合、IP アドレスをホストする大部分のインタフェースが NNMi によって監視されます。NNMi では、管理者が IP アドレスを設定するのに時間がかかったインタフェースが監視すべきインタフェースであることが想定されています。NNMi では、これらのインタフェースを接続インタフェースまたは未接続インタフェースとしてモデリングします。この例では、ルーターに WAN クラウドに接続されたインタフェースがあります。NNMi は、クラウドへの接続を検出してモデル化しない可能性がありますが、デフォルトでルーターインタフェースを監視します。

このデフォルト動作を変更する場合、以下の点に注意してください。

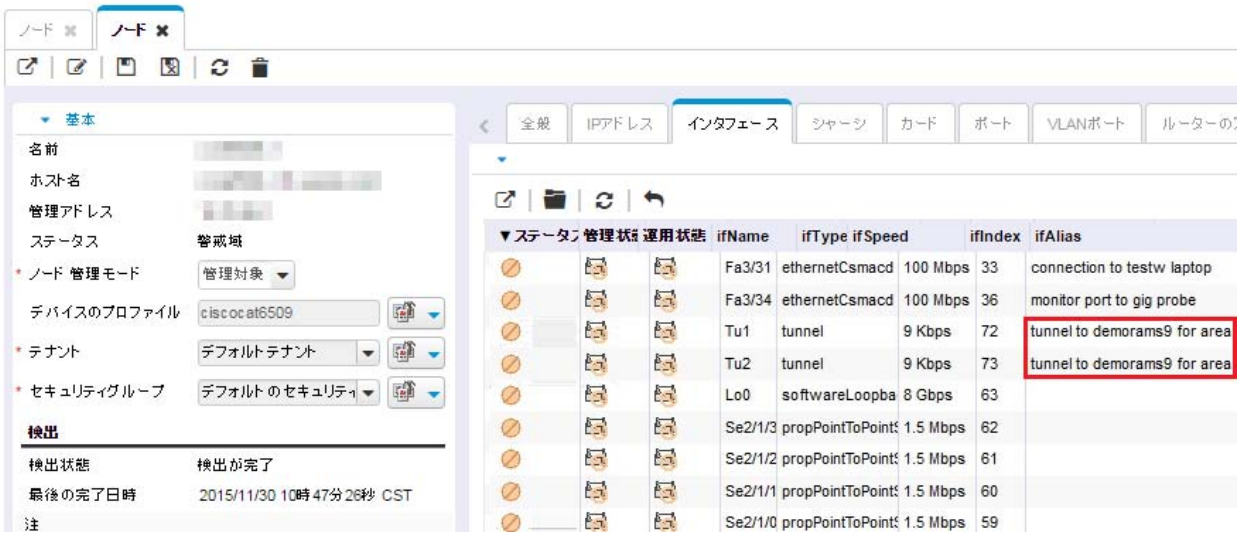
- NNMi により、大量の設定をモニタリングすることができます。
- NNMi は、フィルタリングを使用して個々のノード、インタフェース、およびアドレスにモニタリングを適用することによってこの処理を実行します。これらのフィルターは、ユーザーインタフェースで利用可能なフィルターと同じです。
- このドキュメントでは、ノードとインタフェースに重点が置かれていますが、NNMi ではファンや HSRP グループなどのエンティティも監視対象となります。

以下のシナリオについて考えます。

- ノードのサブセットでのインタフェースには、トンネルで開始する IfAlias があります。
- これらのインタフェースの速度が 9Kbs になった場合に NNMi で監視する必要があると判断する。

NNMi を使用してフィルターを作成し、これらの基準に適合するインタフェースを識別することができます。このフィルターを作成したら、モニタリング設定をこれらのインタフェースに適用します。

図 34: [ノード] フォーム: モニタリング設定の適用



ESXi サーバーと VMware のモニタリング設定

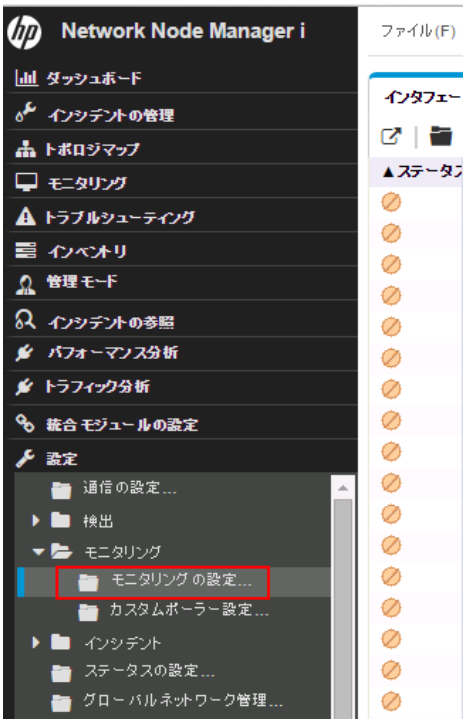
ハイパーバイザー上でホストされている仮想マシン (VM) を NNMi が監視できるようにするには、追加のモニタリングの設定が必要です。以下の手順では、これらの手順について説明します。

1. 2 つのノードグループを作成します。1 つはすべての VM (仮想マシンと呼ばれる) 用、もう 1 つはすべてのハイパーバイザー (VMware ESX ホストと呼ばれる) 用です。

図 35: 設定: ノードグループ

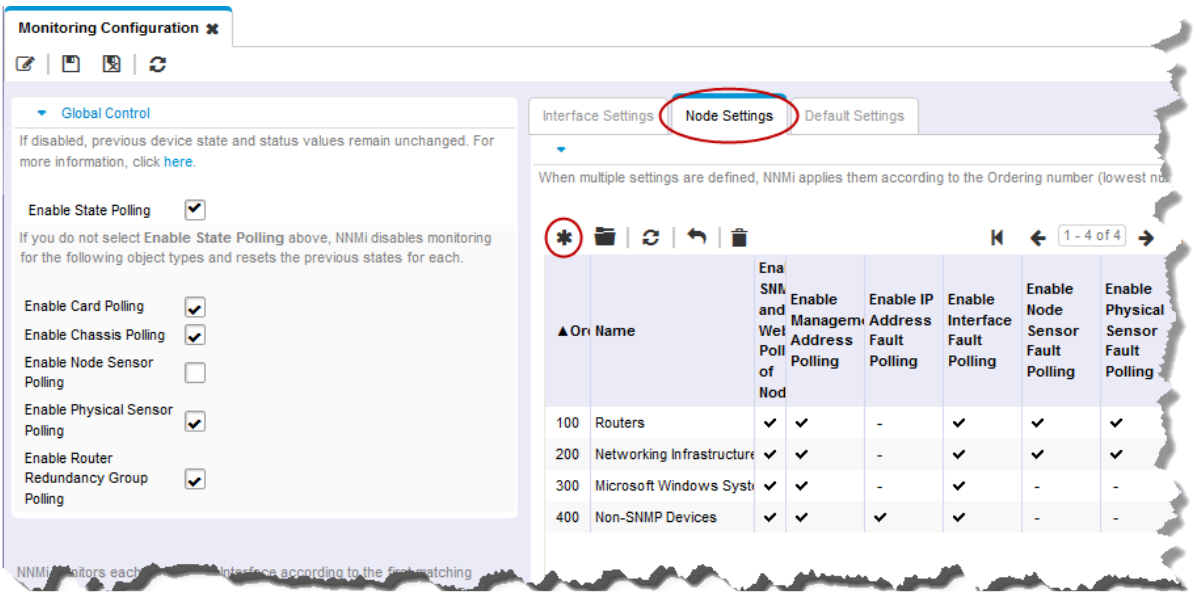
2. ワークスペースのナビゲーションパネルで [**設定**] ワークスペースを選択して、**[モニタリング] > [モニタリングの設定]** をクリックします。

図 36: モニタリングの設定



3. [**ノードの設定**] タブをクリックして ✱ アイコンをクリックし、新しい設定を作成します。

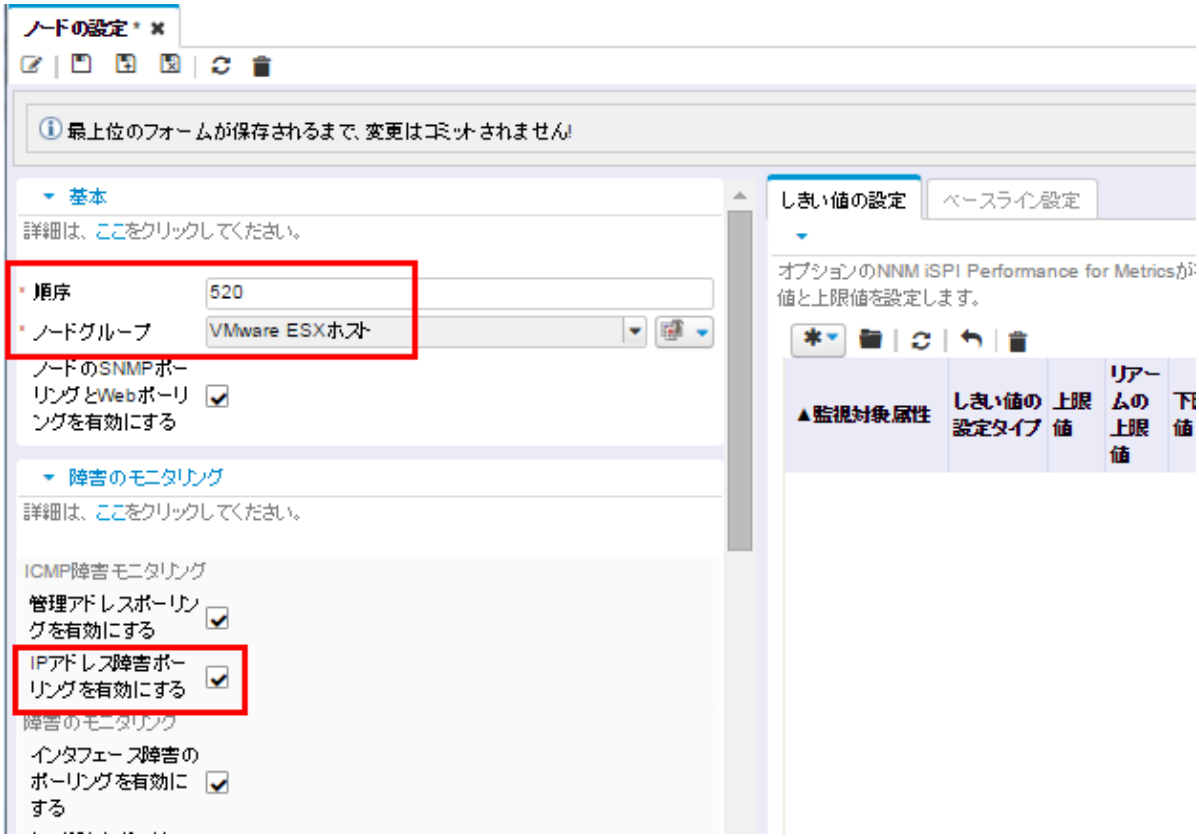
図 37: モニタリングの設定



4. デフォルト設定を保持し、次の設定を追加します。

- [**順序**] の値には、500 より大きな値、たとえば 520 を設定します。
- [**ノードグループ**] 用にハイパーバイザーグループ、たとえば「VMware ESX ホスト」を選択します。
- [**IP アドレス障害ポーリングを有効にする**] チェックボックスをオンにします。
- [**インタフェースパフォーマンスのポーリングを有効にする**] チェックボックスをオンにします。
- [**未接続インタフェースのポーリング**] チェックボックスをオンにします。
- [**IP アドレスをホストするインタフェースのポーリング**] チェックボックスをオンにします。

図 38: モニタリングの設定: [ノードの設定]



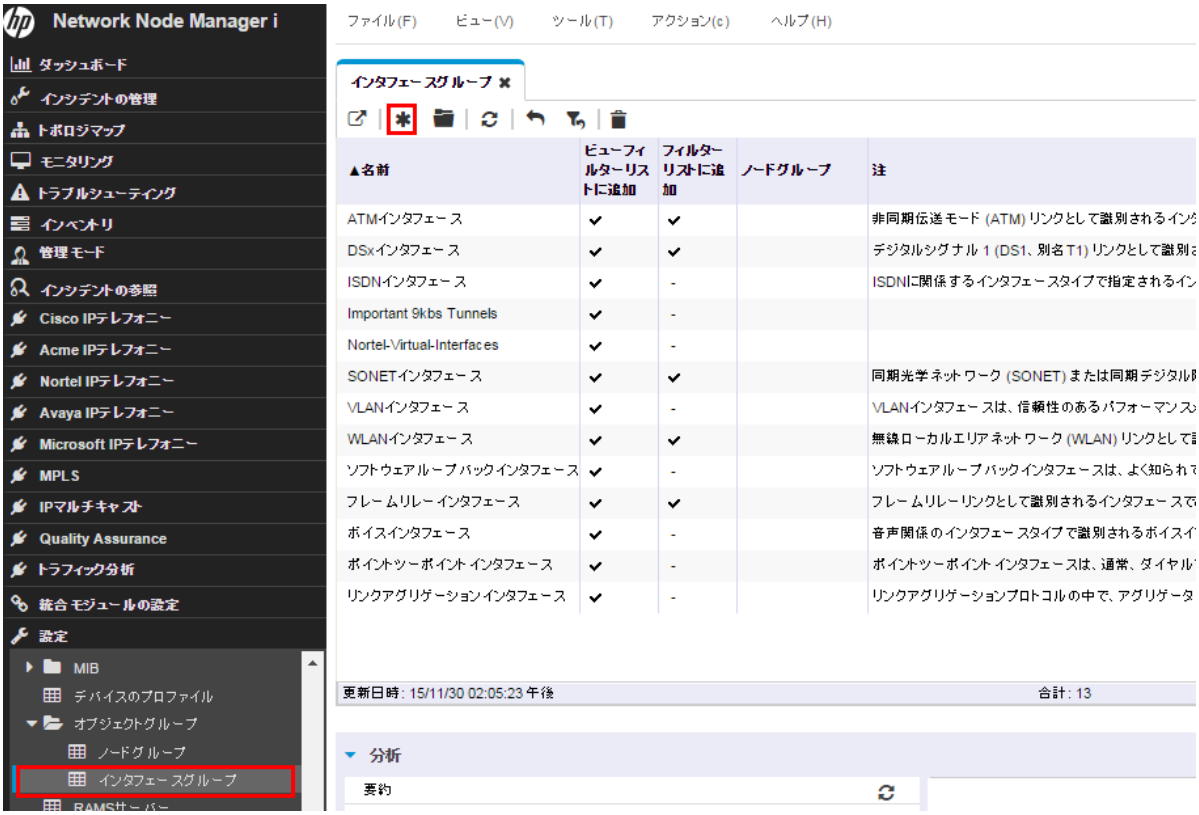
5. [**保存して閉じる**] アイコン をクリックします。
6. 手順 4a で異なる順序番号を指定しながら、仮想マシンノードグループに対して手順 2 ~ 5 を繰り返します。

監視対象インタフェースグループの作成

NNMi により、ノードおよびインタフェースのグループを作成できます。インタフェースグループを作成するには、以下の手順を実行します。

1. ワークスペースのナビゲーションパネルで [**設定**] ワークスペースを選択してから [インタフェースグループ] をクリックします。

図 39: 設定: インタフェースグループ



2. ✱ アイコンをクリックして新しいインタフェースグループを作成します。
3. [**名前**] テキストボックスに「Important 9kbs Tunnels」と入力するか、その他の分かりやすい名前を入力します。

ヒント: よくあることですが、このインタフェースグループを特定のノードグループに制限しないでください。

---

4. [**追加のフィルター**] タブをクリックして、フィルターのロジックの定義で使用する [**フィルターエディター**] にアクセスします。

フィルター式は、属性、演算子、および値を 1 つずつ選択することによって定義します。変数照合では、like 演算子をアスタリスクと一緒に使用することができます。

この例では、2 つの属性で AND 条件を使用します。

ヒント: ロジックの定義中に問題が発生した場合は、保存せずにそのフォームを閉じ、最後に保存した値に戻してください。その後、フォームを再び開いて再開します。

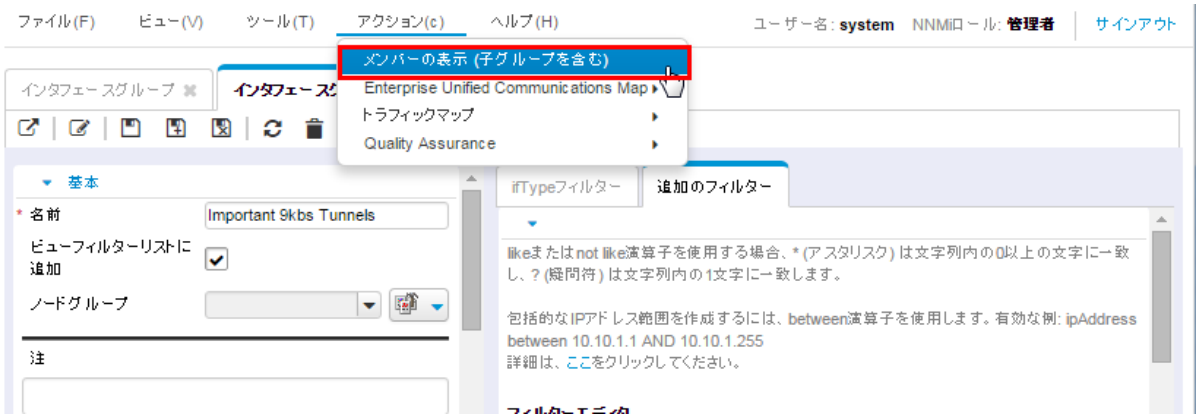
注: IfType フィルターを定義する ([**IfType フィルター**] タブ) と、その IfType フィルターは必ず [**追加のフィルター**] タブでのフィルターと論理 AND 演算されます。

図 40: インタフェースグループ: 保存

5. フィルターを指定した後は、そのフィルターを保存します。ただし、まだ閉じないでください。
6. **[アクション] > [メンバーの表示 (子グループを含む)]** ニュー項目を使用して、フィルターが期待どおり機能するかどうか検証します。

NNMi には、フィルター基準を通過するすべての項目が表示されます。

図 41: アクション: インタフェースグループのメンバーの表示



7. 結果を確認します。この例では、フィルターがネットワークの多数のインタフェースに一致しています。NNMi では、これらの一部が常に監視されます。

図 42: インタフェース: インタフェースグループのフィルター結果

インタフェースグループへの監視の適用

作成したフィルターによって定義されるインタフェースを監視するには、モニタリングをこのインタフェースグループに適用します。ノードグループとインタフェースグループの両方に監視を適用できます。

注: NNMi では、インタフェース設定のほうがノード設定より優先度が高いとみなされます。

---

1. ワークスペースのナビゲーションパネルで [**設定**] ワークスペースを選択して、[**モニタリングの設定**] をクリックします。

図 43: モニタリングの設定

2. [**インタフェースの設定**] タブをクリックします。

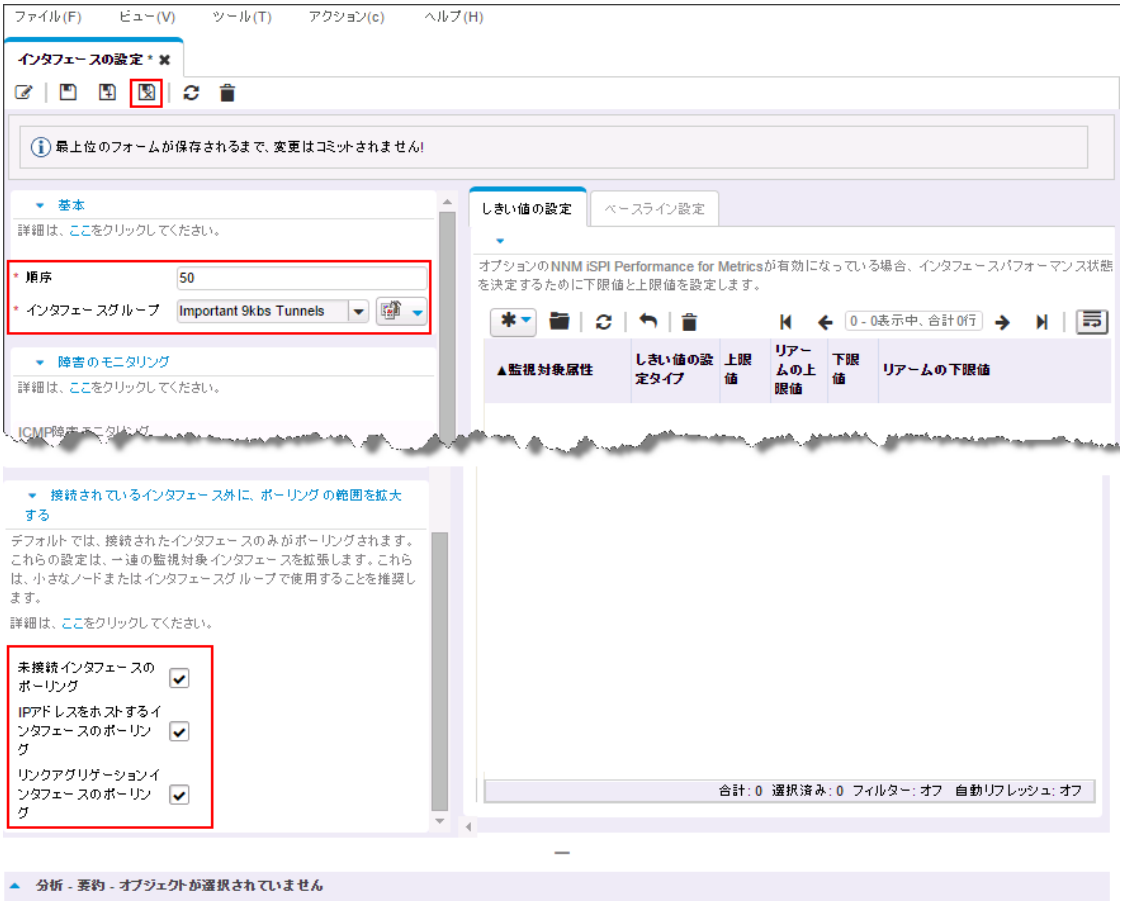
ヒント: 現在の [順序] の値をすべて書き留めてください。それらの値により、インタフェースが複数のグループに属する場合の優先度が定義されます。

この例での最高優先度は 100 です。

図 44: モニタリングの設定:[インタフェースの設定] タブ

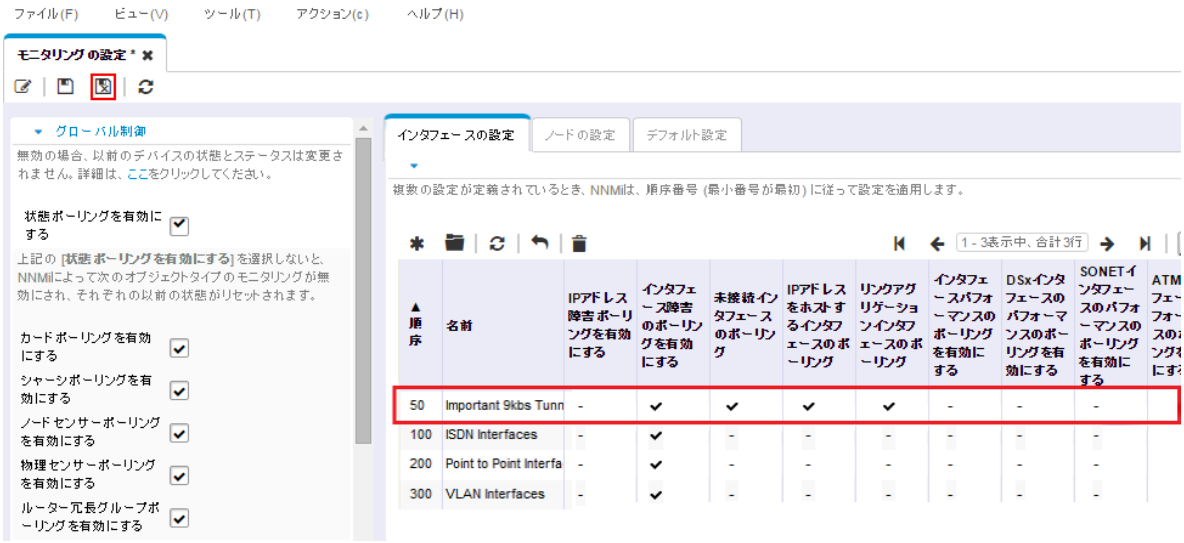
3. ✱ アイコンをクリックします。
4. この設定を、その他の設定よりも優先度が高くなるように設定する [**順序**] 値を入力します。これにより、これらのインタフェースがポーリングされるようになります。NNMi では、数値が低いほど優先度が高くなります。将来的な設定を考慮した [**順序**] 値を選択することもできます。たとえば、この数値を 1 にすると、設定可能な最高優先度が設定され、将来的なエントリ数が制限されます。この例の場合は、「50」と入力します。
5. モニタリング領域を拡大します。接続されているかどうかに関係なくこれらのインタフェースを監視するには、フォームの [**接続されているインタフェース外に、ポーリングの範囲を拡大する**] エリアですべてのチェックボックスをオンにします。
6. [**クイック検索**] 機能を使用して、新規作成したインタフェースグループを選択します。次に、 [**保存して閉じる**] をクリックします。

図 45: インタフェースの設定: 保存して閉じる



7. 最上位レベルの [**モニタリングの設定**] フォームで [**保存して閉じる**] をクリックして、変更を保存します。

図 46: モニタリングの設定: 保存して閉じる



これで、このインタフェースグループに適用されるモニタリングの設定が完了しました。NNMi は、SNMP を使用して [**Important 9kbs Tunnels**] フィルターに適合するインタフェースをすべて監視します。

監視設定のテスト

新しいモニタリング設定は、多くの異なる方法でテストできます。たとえば、以下の手順を実行します。

1. ワークスペースのナビゲーションパネルで [インベントリ] ワークスペースを選択してから [インタフェース] をクリックします。
2. ドロップダウンメニューを使用して、新規のインタフェースグループである [Important 9kbs Tunnels] を選択します。

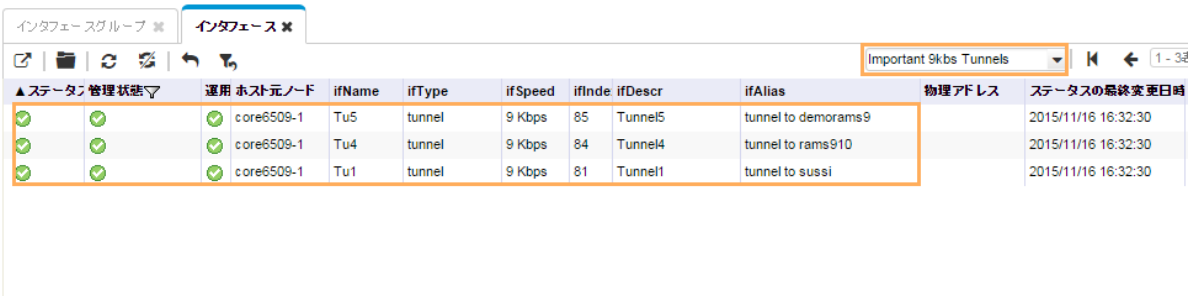
これによりテーブルをフィルターし、このインタフェースグループのインタフェースのみが表示されるようにします。

ヒント: インタフェースの中には、[管理状態] が [未ポーリング] になっているものがあります。監視設定の変更が反映されるまで数分かかる場合があります。インタフェースを手動で強制的にポーリングするには、これらのインタフェースをホストしているいずれかのノードでステータス ポーリング コマンドを実行します。すべてのコマンドがステータスの取得を開始するのを確認してください。

ノードでステータス ポーリングを実行するには、以下の手順を実行します。

1. ワークスペースのナビゲーションパネルで [**インベントリ**] ワークスペースを選択して、[**ノード**] をクリックします。
2. ポーリングするノードを選択し、**[アクション] > [ポーリング] > [ステータスのポーリング]** コマンドを使用してステータスのポーリングを開始します。

図 47: インタフェース: [Important 9kbs Tunnels] フィルター

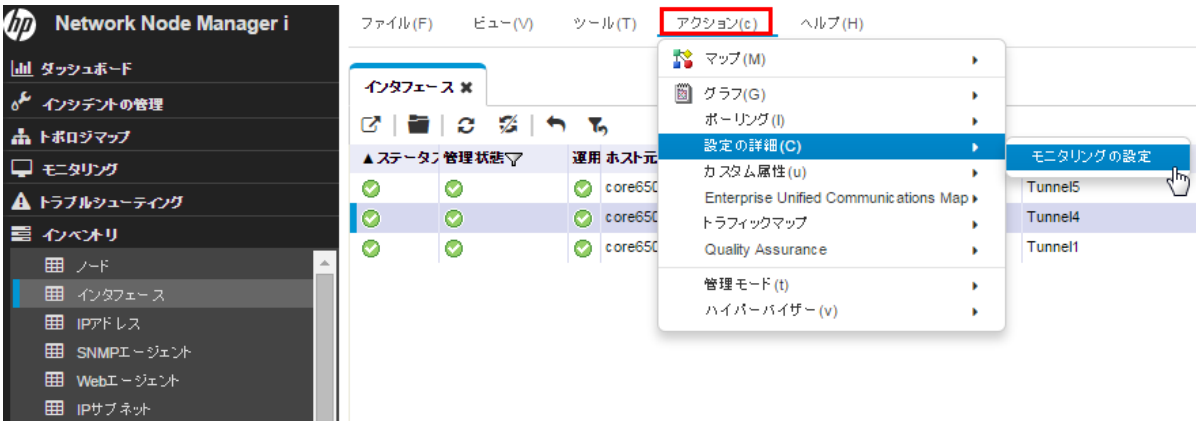


上の図で強調表示されているインタフェースの 1 つを開き、そのモニタリングの設定で正常に機能することを確認します。

インタフェースの監視設定を確認するには、以下の手順を実行します。

1. インタフェースをダブルクリックします。
2. **[アクション] > [設定の詳細] > [モニタリングの設定]** をクリックして、選択したインタフェースのモニタリングの設定を表示します。

図 48: アクション: モニタリングの設定

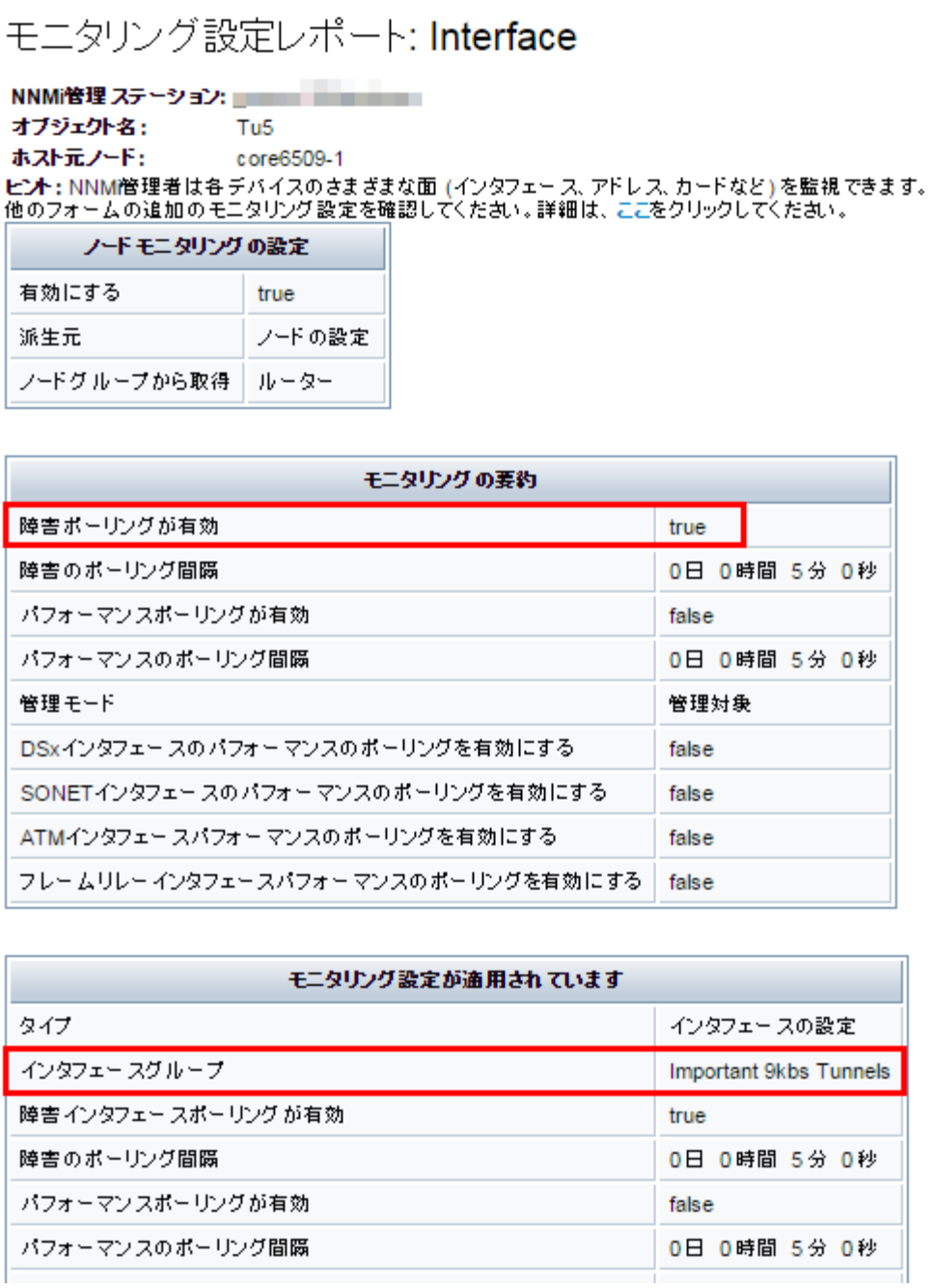


このレポートの例では、監視設定が正常に動作していることがわかります。

まず、NNMi が **Important 9kbs Tunnels** グループのモニタリング設定をこのインタフェースに適用したことを確認できます。これは、監視設定がこのインタフェースに適切に関連付けられていることを示しています。

2 番目に、NNMi で [障害ポーリングが有効] が true に設定されていることを確認できます。これは、新しいモニタリング設定が Important 9kbs Tunnels インタフェースグループに正常に適用されていることを示します。

図 49: モニタリング設定レポート: インタフェース



モニタリング設定レポート: Interface

NNMi管理 ステーション: [redacted]
オブジェクト名: Tu5
ホスト元ノード: core6509-1
ヒント: NNMi管理者は各デバイスのさまざまな面 (インタフェース、アドレス、カードなど) を監視できます。
他のフォームの追加のモニタリング設定を確認してください。詳細は、ここをクリックしてください。

ノード モニタリング の設定	
有効にする	true
派生元	ノード の設定
ノード グループ から取得	ルーター

モニタリング の要約	
障害 ポーリング が有効	true
障害 の ポーリング 間隔	0日 0時間 5分 0秒
パフォーマンス ポーリング が有効	false
パフォーマンス の ポーリング 間隔	0日 0時間 5分 0秒
管理 モード	管理対象
DSxインタフェース の パフォーマンス の ポーリング を有効にする	false
SONETインタフェース の パフォーマンス の ポーリング を有効にする	false
ATMインタフェース パフォーマンス の ポーリング を有効にする	false
フレーム リレー インタフェース パフォーマンス の ポーリング を有効にする	false

モニタリング設定が適用されています	
タイプ	インタフェース の設定
インタフェース グループ	Important 9kbs Tunnels
障害 インタフェース ポーリング が有効	true
障害 の ポーリング 間隔	0日 0時間 5分 0秒
パフォーマンス ポーリング が有効	false
パフォーマンス の ポーリング 間隔	0日 0時間 5分 0秒

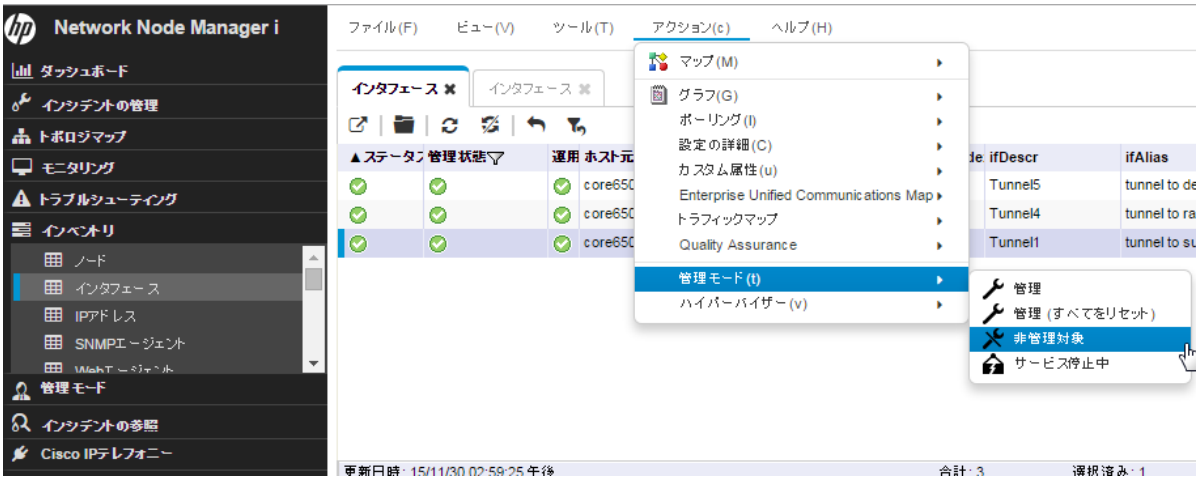
モニタリングの例外

インタフェースまたはノードは、手動で強制的に監視対象から除外することができます。

[インタフェース] フォームで、**[アクション] > [管理モード] > [非管理対象]** をクリックして、そのインタフェースを管理除外に切り替えます。

このインタフェースは、監視設定に関係なく NNMi で監視されなくなります。

図 50: アクション: 管理モード: 非管理対象



NNMi では現在、NNM と同じ方法ではインタフェースを強制的に監視対象から除外していません。現行では、インタフェースの対象除外には単なる否定的な上書きが行われています。

NNMi でインタフェースを強制的に監視するには、「Forcing an Interface to be Polled」(softwaresupport.hp.com) を参照してください。

インシデント、トラップ、および自動アクションの設定

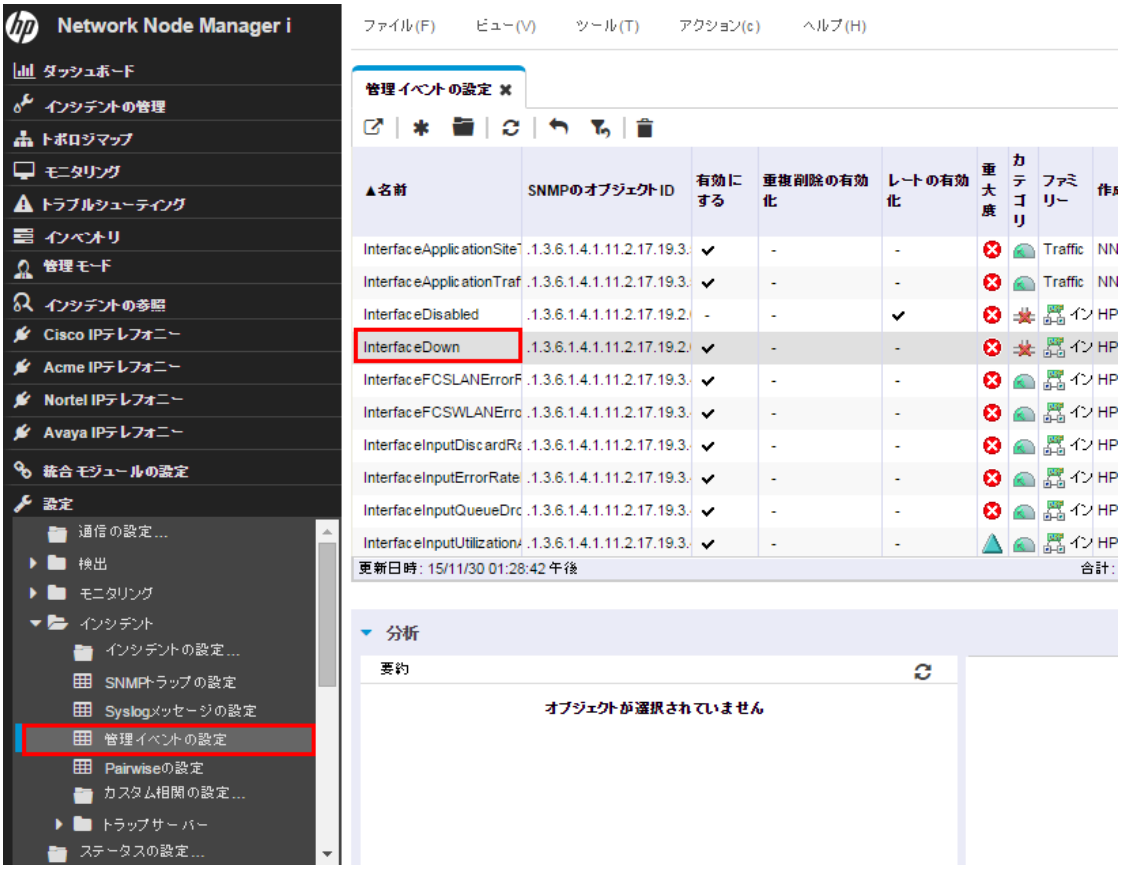
インシデントの設定

NNMi を使用して、インシデントの特定の側面を変更することができます。一部の例には、インシデントの有効化、メッセージのフォーマット、重複削除の有効化、レート相関の有効化などが含まれます。

この例では、InterfaceDown (インタフェース停止中) インシデントを拡張してメッセージにインタフェースエイリアスを含める方法を説明します。

1. ワークスペースのナビゲーションパネルで [**設定**]ワークスペースを選択してから [**インシデント**] > [**管理イベントの設定**] をクリックします。
2. [InterfaceDown] インシデント設定をダブルクリックします。

図 51: 設定: 管理イベントの設定



3. 次に進む前に、NNMi ヘルプで「インシデントメッセージを設定するための有効なパラメーター」を参照し、メッセージ形式に追加できる利用可能な引数を確認してください。この例では、以下に示すように、引数$ifAlias をインシデントメッセージに追加します。

図 52: 管理イベントの設定: メッセージの形式

4. [**クイック検索**] を使用して、[**作成者**] を [**カスタマー**] に変更します。
5. 最後に、このフォームと [**管理イベントの設定**] フォームで [**保存して閉じる**] をクリックします。

以下の [**重要な未解決インシデント**] の表示例に示されるように、すべての「InterfaceDown」インシデントに$ifAlias パラメーターが表示されます。

注: インタフェースにエイリアスが存在しない場合、NNMi では、エイリアスが null として表示されます。

図 53: 重要な未解決インシデント

トラップの設定

ヒント: NNMi でのトラップの処理方法の詳細については、softwaresupport.hp.com で入手できる『Step-by-Step Guide to Incident Management』を参照してください。

注: NNMi インシデントブラウザーでトラップを受信するには、トラップ定義を含む MIB を NNMi にロードする必要があります。

この例では、依存関係を満たすために 3 つの MIB をロードする必要があります。まず、ruggedcom.mib ファイルをロードし、続いて rcsysinfo.mib ファイルをロードします。次に、ruggedcomtraps.mib ファイルからトラップをロードできます。nnmloadmib.ovpl コマンドを使用して MIB を NNMi にロードします。

注: NNMi コンソールを使用して MIB をロードすることもできます。

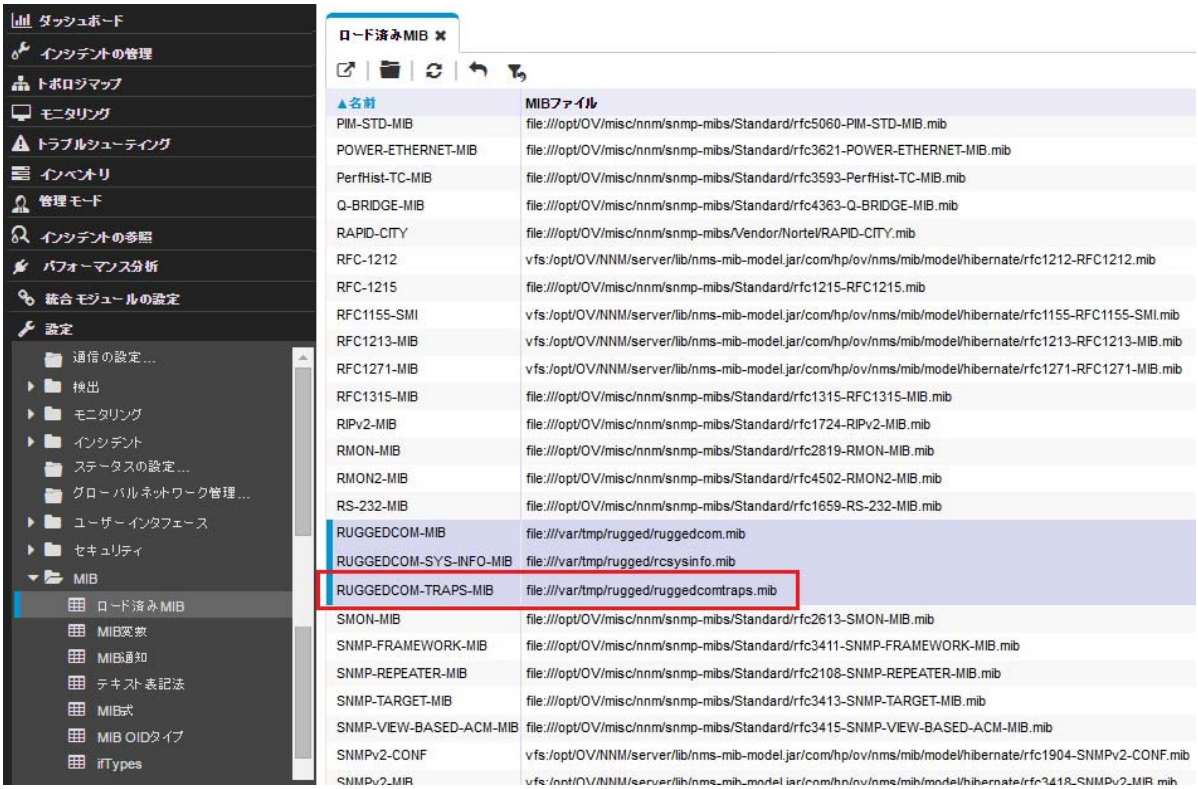
コマンド ラインを使用して MIB をロードするには、以下の手順を実行します。

1. nnmloadmib.ovpl -load ./ruggedcom.mib コマンドを実行します。これにより、ruggedcom.mib の定義がロードされます。
2. nnmloadmib.ovpl -load ./rcsysinfo.mib コマンドを実行します。これにより、**rcsysinfo.mib** の定義がロードされます。
3. nnmloadmib.ovpl -load ./ruggedcomtraps.mib コマンドを実行します。これにより、ruggedcomtraps.mib ファイルがロードされます。

次に、MIB がロードされていることを確認します。

1. ワークスペースのナビゲーションパネルで [**設定**] ワークスペースを選択して、**[MIB] > [ロード済み MIB]** をクリックします。
2. 新規にロードされた Rugged Com MIB が表示されることを確認します。
3. トラップモジュール (「RUGGEDCOM-TRAPS-MIB」) を書き留めます。次のコマンドでこれが必要になります。

図 54: 設定: ロード済み MIB



4. nnmincidentcfg.ovpl -loadTraps RUGGEDCOM-TRAPS-MIB コマンドを実行して、このモジュールからトラップをロードします。以下のような出力が表示されます。

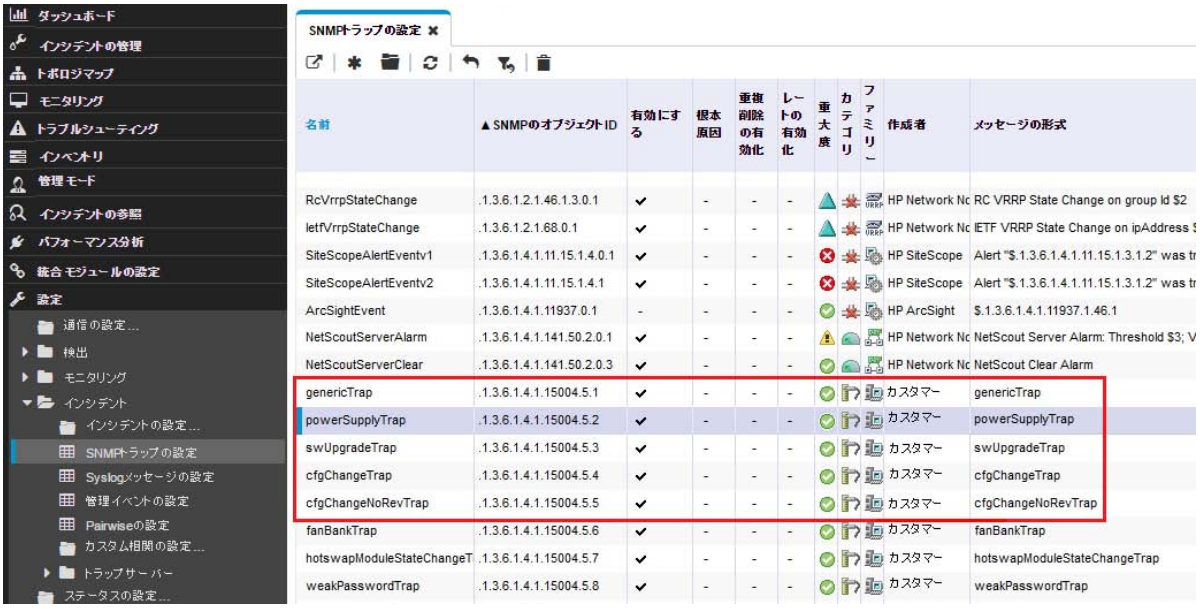
   MIB モジュールからの SNMP トラップがロードされました: RUGGEDCOM-TRAPS-MIB
   トラップ数: 5
   次のトラップがインシデントの設定に追加されました:
   cfgChangeNoRevTrap - .1.3.6.1.4.1.15004.5.5
   cfgChangeTrap - .1.3.6.1.4.1.15004.5.4
   powerSupplyTrap - .1.3.6.1.4.1.15004.5.2
   swUpgradeTrap - .1.3.6.1.4.1.15004.5.3
   genericTrap - .1.3.6.1.4.1.15004.5.1

これで NNMi に 4 つの新しいトラップが定義されました。これらを表示するには、以下の手順を実行します。

1. ワークスペースのナビゲーションパネルで [**設定**] ワークスペースを選択して、**[インシデント] > [SNMP トラップの設定]** をクリックします。
2. **[SNMP のオブジェクト ID]** でトラップをソートします。

トラップは、すべて有効としてロードされます。受信する特定のトラップを除いてすべて無効にできます。この時点で設定を変更できます。

図 55: 設定: SNMP トラップの設定



自動アクションの設定

インシデントに対する自動アクションを設定できます。トラップのレートや容量を予測することは難しいため、一般的にこれを行うのは SNMP トラップではなく管理イベントの場合だけです。NNMi の自動アクションは、実行可能コマンド、コマンド ライン スクリプトまたは Python スクリプトになります。Python スクリプトは、NNMi の Java 仮想マシン (JVM) 内で高速に実行されます。NNMi では Python で Java インタープリターを使用するため、NNMi はこれらのスクリプトを Jython として参照します。

NNMi でのアクションは、インシデントのライフサイクル状態の変化に基づいています。インタフェースが停止中になったときともう一度動作中に戻ったときにそれぞれアクションを実行するように NNMi を設定できます。これには、「InterfaceDown」インシデントで両方のアクションを設定しますが、1 つのアクションを [登録済み] に設定されたライフサイクル状態に関連付け、もう 1 つのアクションを [解決済み] に設定されたライフサイクル状態に関連付けます。通常、NNMi は、関連付けられた動作中インシデントを生成しません。

注: NNMi は、インシデントの生成時に [登録済み] 状態をそのインシデントに割り当てます。

「ノード停止中」インシデントを受信したときに Perl スクリプトを実行するように NNMi を設定するには、以下の手順を実行します。

1. スクリプトを actions ディレクトリに配置します。

注: セキュリティ上の理由により、このディレクトリにアクセスするには root または管理者権限が必要です。

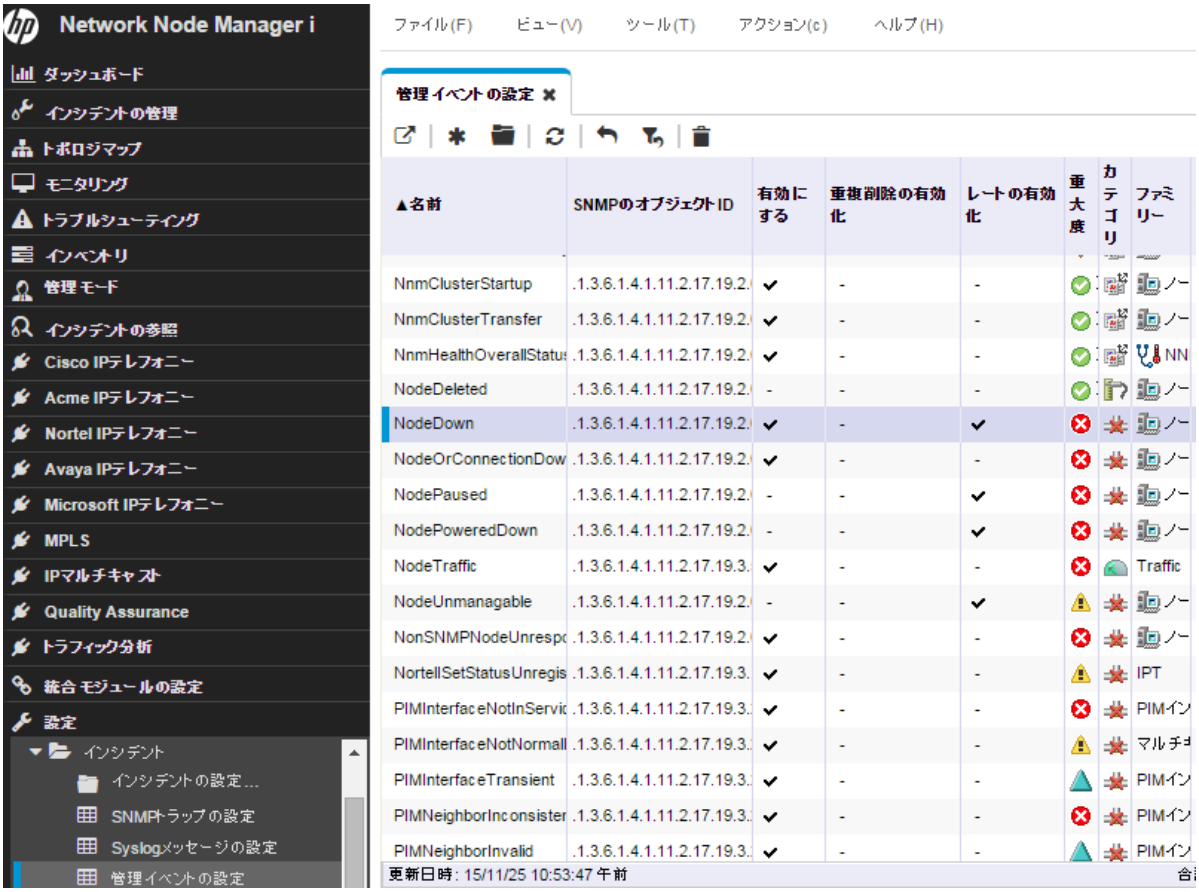
この例では、actions ディレクトリが以下の場所に存在すると想定しています。

- Windows の場合: %NnmDataDir%\shared\nnm\actions
- Linux の場合: $NnmDataDir/shared/nnm/actions

actions ディレクトリは、NNMi のインストール方法に応じて、異なる場所に存在する可能性があります。この例では、スクリプトが writelog.ovpl と命名されています。このスクリプトを actions ディレクトリにコピーします。スクリプトが実行可能であることを確認します。

2. このスクリプトをこのインシデントのアクションに関連付けるには、以下の手順を実行します。
   a. ワークスペースのナビゲーションパネルで [**設定**] ワークスペースを選択します。
   b. **[インシデント] > [管理イベントの設定]** をクリックします。
   c. [NodeDown] インシデントをダブルクリックします。

図 56: 管理イベントの設定: 「NodeDown」 インシデント



3 [**作成者**] を [**カスタマー**] に変更し、[**アクション**] タブをクリックしてから ✱ アイコンをクリックします。

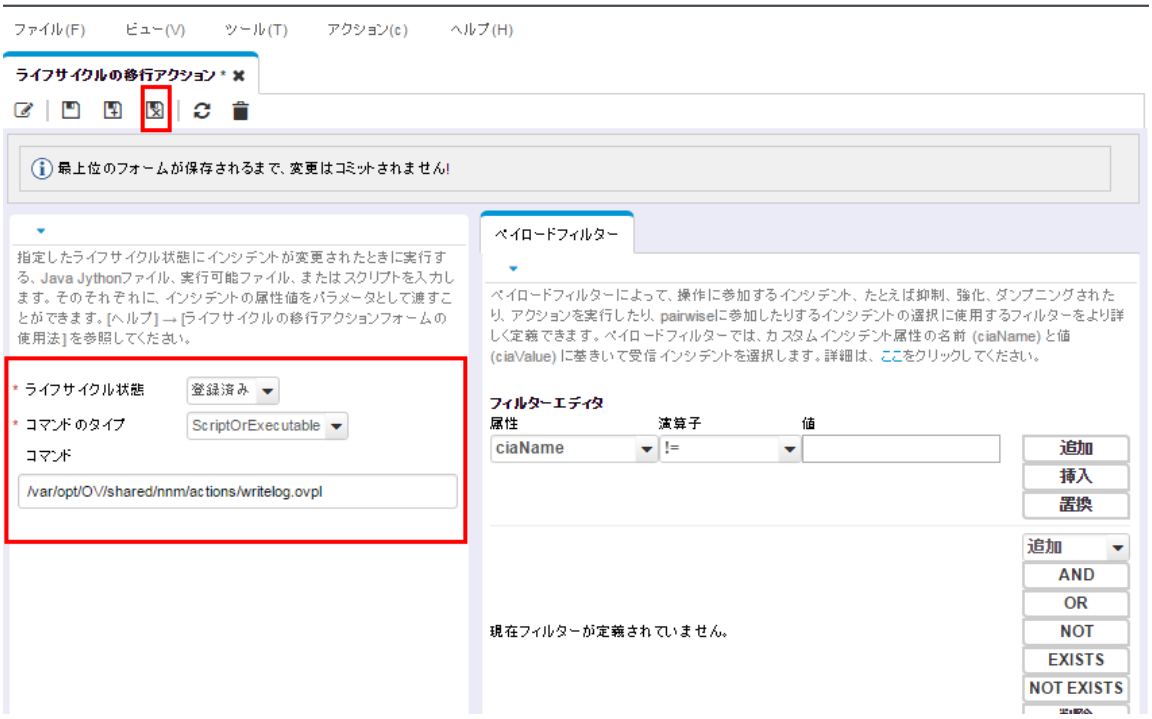
図 57: 管理イベントの設定: [アクション] タブ

4 適切な [**ライフサイクル状態**] (この例では [**登録済み**]) を選択します。

5 [**コマンドのタイプ**] を [ScriptOrExecutable] に設定します。

6 実行可能ファイルへの完全なパスが含まれたコマンドの名前を入力して、 [**保存して閉じる**] をクリックします。

図 58: ライフサイクルの移行アクション



6. [**有効にする**] チェックボックスをオンにしてアクションを有効にします。

図 59: 管理イベントの設定: [アクション] タブ: アクションを有効化

次に、アクションをテストする必要があります。テストを行うための最も簡単な方法は、前に発生した「NodeDown」インシデントを探すことです。

1. ワークスペースのナビゲーションパネルで [**インシデントの参照**] ワークスペースを選択して、[**解決済みの重要なインシデント**] をクリックします。

図 60: インシデントの参照: [解決済みの重要なインシデント] ビュー

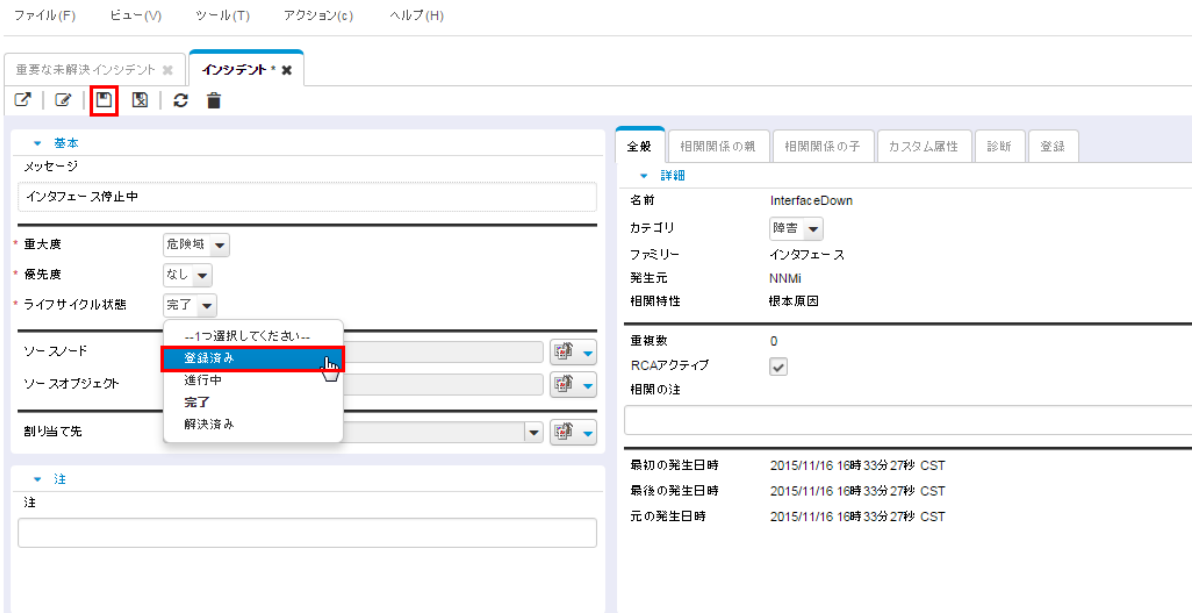
2. NNMi で解決された「NodeDown」インシデントのフォームをダブルクリックして開きます。

   この例において、「解決済み」はそのインタフェースがバックアップされることを意味します。障害がなくなると NNMi によって自動的にインシデントが解決済みにされます([**ライフサイクル状態**] を [登録済み] に設定することにより、インシデントを再び開くことができます。このアクションを実行すると、NNMi は、アクションの実行中にそのインシデントが初めて開いたかのように動作します)。

3. [**ライフサイクル状態**] を [登録済み] に設定します。

   これにより、このフォームを保存した後 (ライフサイクル状態の変更の保存) にアクションが実行されます。変更を保存せずにライフサイクル状態を変更すると、NNMi はアクションを実行しません。

図 61: [インシデント] フォーム: [登録済み] ライフサイクル状態



4. ライフサイクル状態を変更するごとに、[**保存**] をクリックします。

変更を保存したら、アクションの結果を確認します。この場合、このスクリプトに関連付けられているログ ファイルを調べます。テストが終了したら、[**ライフサイクル状態**] を [解決済み] に設定し、インシデントを保存して元の状態に戻します。

NNMi コンソールの設定

概要

NNMi 管理者は、ノードグループを定義してデバイスの論理グループを作成します。それらのノードグループは、さまざまな方法で使用されます。このセクションでは、それらのグループを使用してマップを作成する方法を説明します。

NNMi 管理者がノードグループを作成する場合:

- ノードグループのマップへのリンクは、自動的に [トポロジマップ] > [すべてのノードグループ] フォルダーの下にアルファベット順に表示されます。

  [すべてのノードグループ] フォルダーは NNMi 管理者に対してのみ表示されます。

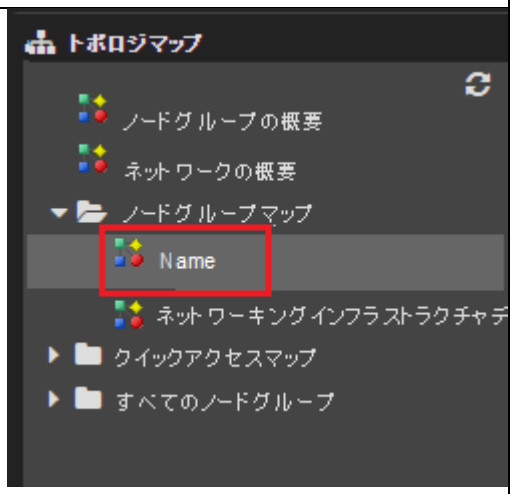
- [ノードグループマップ] アイコン は灰色で表示されます。

NNMi 管理者がノードグループマップを開き、[マップを保存] アイコンをクリックすると、以下のように動作します。

- ノードグループのマップへのリンクは、自動的に [トポロジマップ] > [ノードグループマップ] フォルダーの下にアルファベット順に表示されます。

  [ノードグループマップ] フォルダーはすべての NNMi ユーザーに対して表示されます。

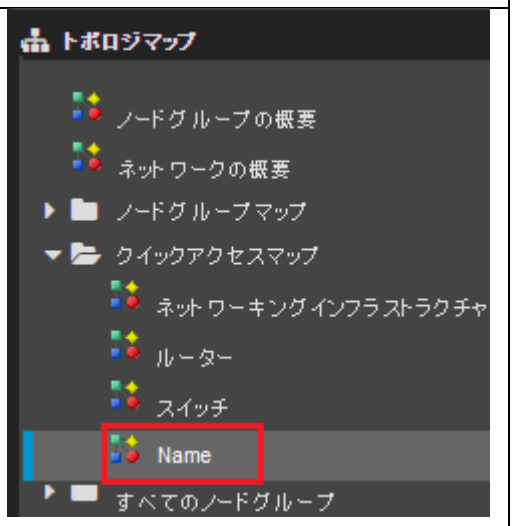
- ノードグループマップのアイコンが複数色の表示 に変わります。



NNMi 管理者が [トポロジマップ順序] 番号をノードグループのマップに割り当てる ([設定] > [ユーザーインタフェース] > [ノードグループマップの設定]) と、以下のように動作します。

- ノードグループのマップへのリンクが、[トポロジマップ] > [クイックアクセスマップ] フォルダーの下に自動的に割り当て順に表示されます。

  [クイックアクセスマップ] フォルダーはすべての NNMi ユーザーに対して表示されます。



NNMi ユーザーが NNMi を開くたびに新規ノードグループマップが毎回表示されるようにする場合、NNMi 管理者は、[設定] > [ユーザーインタフェース] > [ユーザーインタフェースの設定] >[初期ビュー] の設定を使用します。

ノードグループの設定

診断機能を強化するには、ノードグループに含まれているノードを表示するノードグループマップを作成します。

ノードグループの設定の詳細については、softwaresupport.hp.com で入手できる『HP Network Node Manager i Software デプロイメントリファレンス』の「ノードグループの使用」を参照してください。

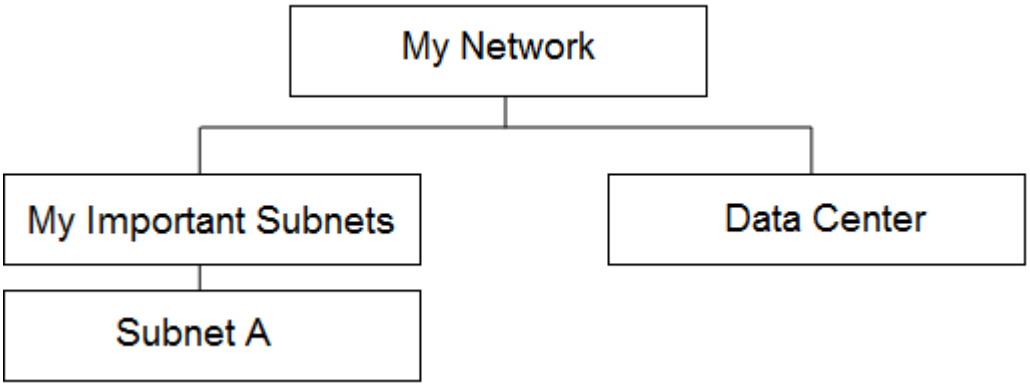
この例では、少ない数の異なるサブネットのノードグループを作成します。

ヒント: これらのノードグループでは、ノード上のアドレスではなく管理アドレスを参照するように設定することができます。また、名前に基づいてこれらのノードグループにノードを含めます。

注: 同じノードを複数のノードグループに含めることができます。

以下の図に、ノードグループの階層の例を示します。

図 62: グループの階層



Subnet A = 192.125.*.* の管理アドレス

Data Center = 「data_center」 で始まるシステム名を持つノード

以下の点に注意してください。

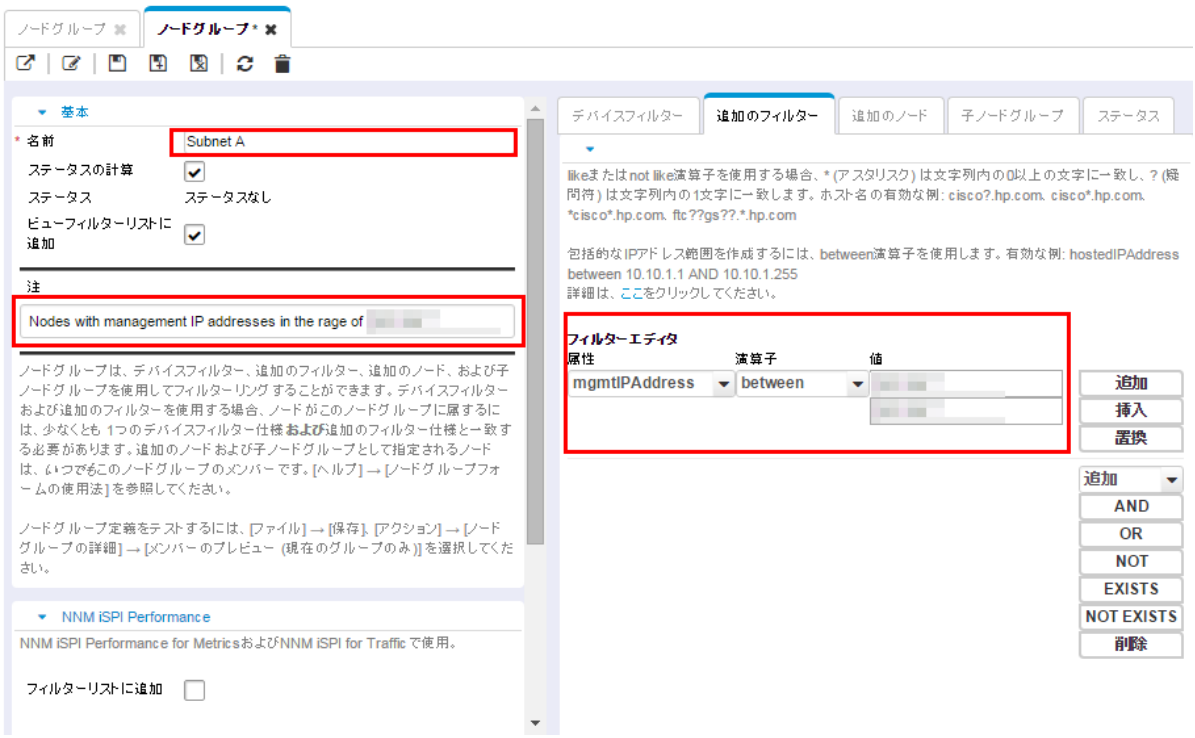
- Subnet A ノードグループと Data Center ノードグループにのみノードが取り込まれます。My Important Subnets ノードグループは階層の構造を表しており、子ノードグループのみが設定されています。
- 下から階層を作成していくことが最も簡単です。

1. [**設定**] ワークスペース > [**オブジェクトグループ**] > [**ノードグループ**] をクリックします。
   [**ノードグループ**] フォームで ✱ アイコンをクリックします。

   以下の例に示すようにして、Subnet A ノードグループを作成します。

ヒント: IP アドレス範囲の固有の式に注目してください。

図 63: ノードグループ: 基本



2. 次に、Data Center ノードグループを作成します。

図 64: ノードグループ: [追加のフィルター] タブ

3. 次に、「My Important Subnets」という名前のノードグループを作成します。

1 [**ノードグループ**] フォームで ✱ アイコンをクリックします。

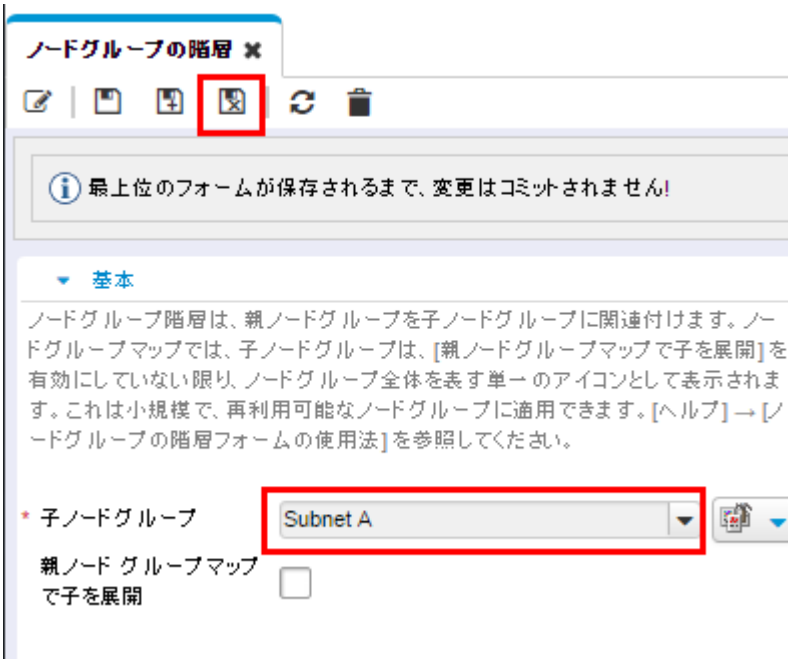
2 [**名前**] テキストボックスに「**My Important Subnets**」と入力します。

3 [**子ノードグループ**] タブをクリックし、✱ アイコンをクリックします。

図 65: ノードグループ: [子ノードグループ] タブ

4  をクリックし、[**クイック検索**] をクリックします。「**Subnet A**」子ノードグループをクリックして、[**OK**] をクリックします。

図 66: ノードグループの階層: 子ノードグループ名の割り当て



5. [保存して閉じる] をクリックします。これで、「My Important Subnets」ノードグループに「Subnet A」という子ノードグループが作成されました。

図 67: [子ノードグループ] タブ: 保存して閉じる

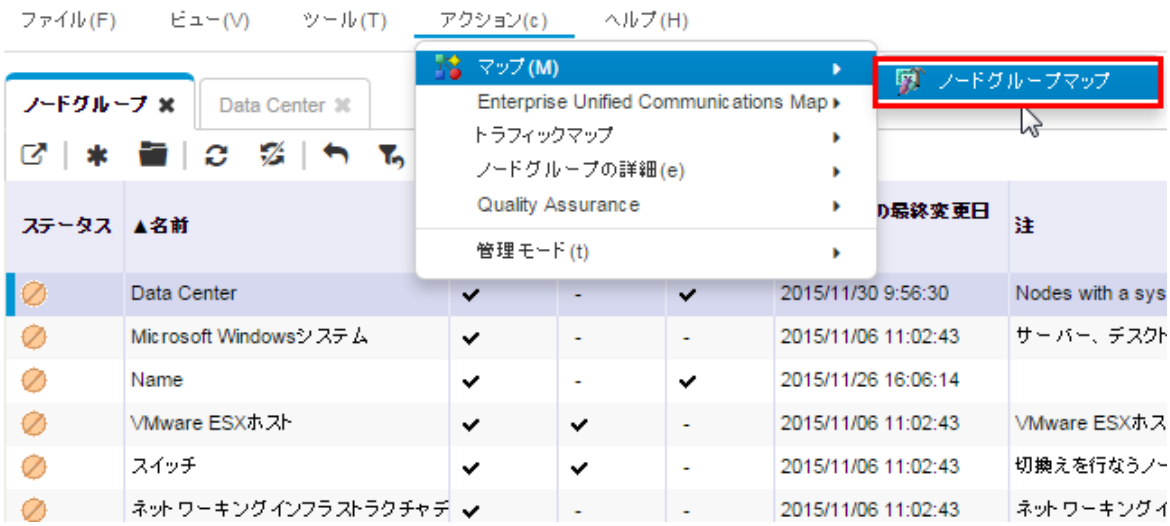
最後に、「My Network」という名前のノードグループを作成します。これには、「Data Center」および「My Important Subnets」という子ノードが含まれます。

ヒント: 各ノードグループを保存したら、**[アクション] > [ノードグループの詳細] > [メンバーのプレビュー (現在のグループのみ)]** をクリックして、忘れずにメンバーシップのテストを行ってください。

ノードグループの設定のテストが完了したら、ノードグループごとにマップの初期インスタンスを作成します。

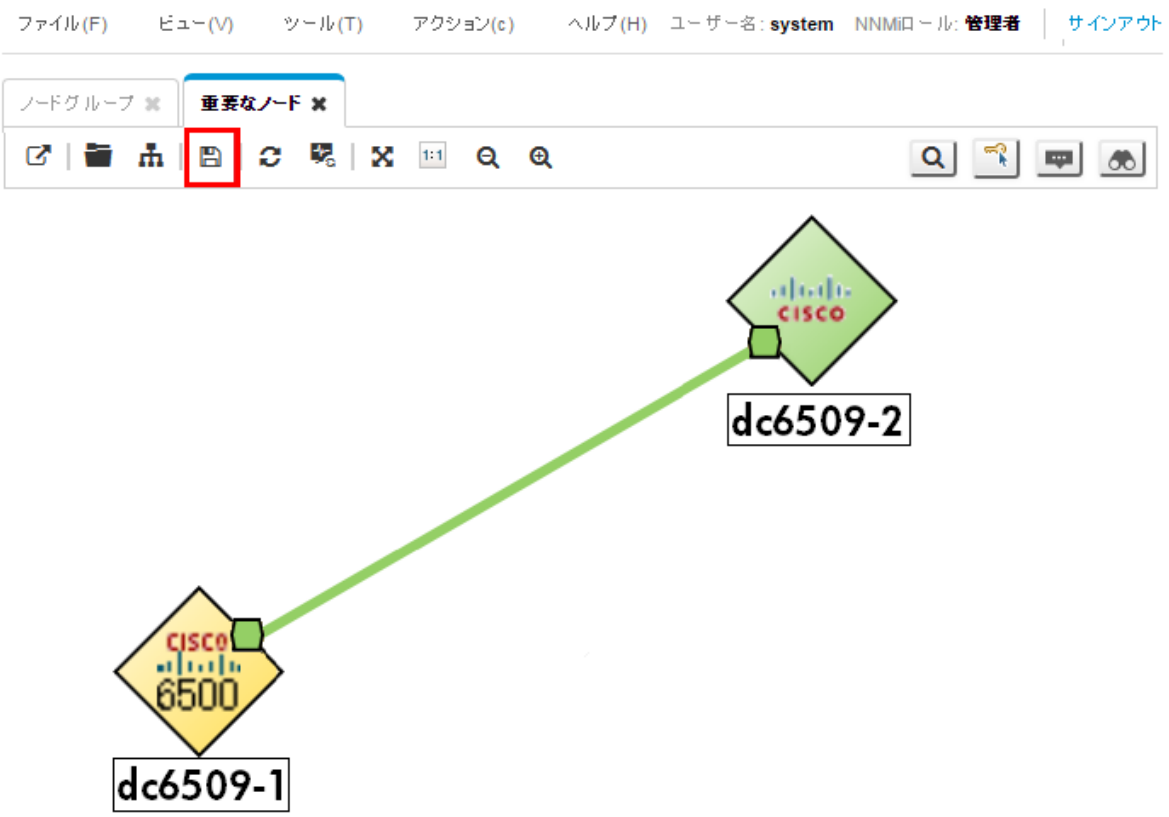
1. **[アクション] > [マップ] > [ノードグループマップ]** をクリックしてマップを開きます。

図 68: アクション: マップ: [ノードグループマップ] の選択



2. オプション: **アイコンを移動させ、** [マップを保存] をクリックすることができます (これにより、マップの全ユーザーのコピーが変更されます)。

図 69: トポロジマップ: すべてのノードグループ: ノードグループマップ: マップを保存



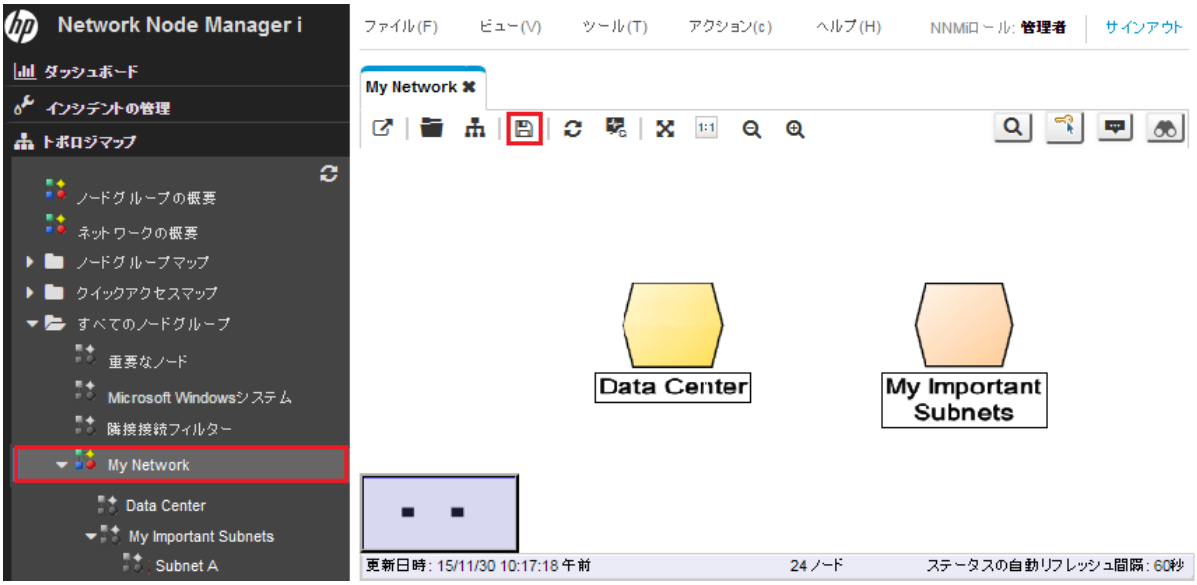
変更を保存すると、ノードグループマップが作成されたことを通知するメッセージが NNMi に表示されます。

階層全体でこの同じプロセスを繰り返します。ステータスがノードグループ全体に伝達するまでには、しばらく時間がかかる場合があります。

ノードグループマップの設定

これで、その内部を移動可能なマップ階層が作成されました。ワークスペースのナビゲーションパネルで[**トポロジマップ**]ワークスペースを選択します。新しく作成したノードグループマップが表示されていない場合、ブラウザーをリフレッシュするか、NNMi をサインアウトしてからもう一度サインインしてください。

図 70: [My Network] トポロジマップ



[ノードグループマップの設定]オプションにより、ノードグループの位置を指定し、背景グラフィックを追加して接続オプションを変更することができます。

マップに背景グラフィックを配置するには、以下の手順を実行します。

1. ワークスペースのナビゲーションパネルで[**トポロジマップ**]ワークスペースを選択して[**すべてのノードグループ**]フォルダーを展開し、[My Network]をクリックしてマップを表示します。

   [**マップを保存**]をクリックします(これにより、マップが[ノードグループマップの設定]に追加されます)。

2. ワークスペースのナビゲーションパネルで[**設定**]ワークスペースを選択し、[**ユーザーインタフェース**]フォルダーを展開して[**ノードグループマップの設定**]をクリックします。

現在の[**トポロジマップ順序**]の値を書き留めます。現在使用されている最低値は 10 です。

図 71: 設定: ノードグループマップの設定

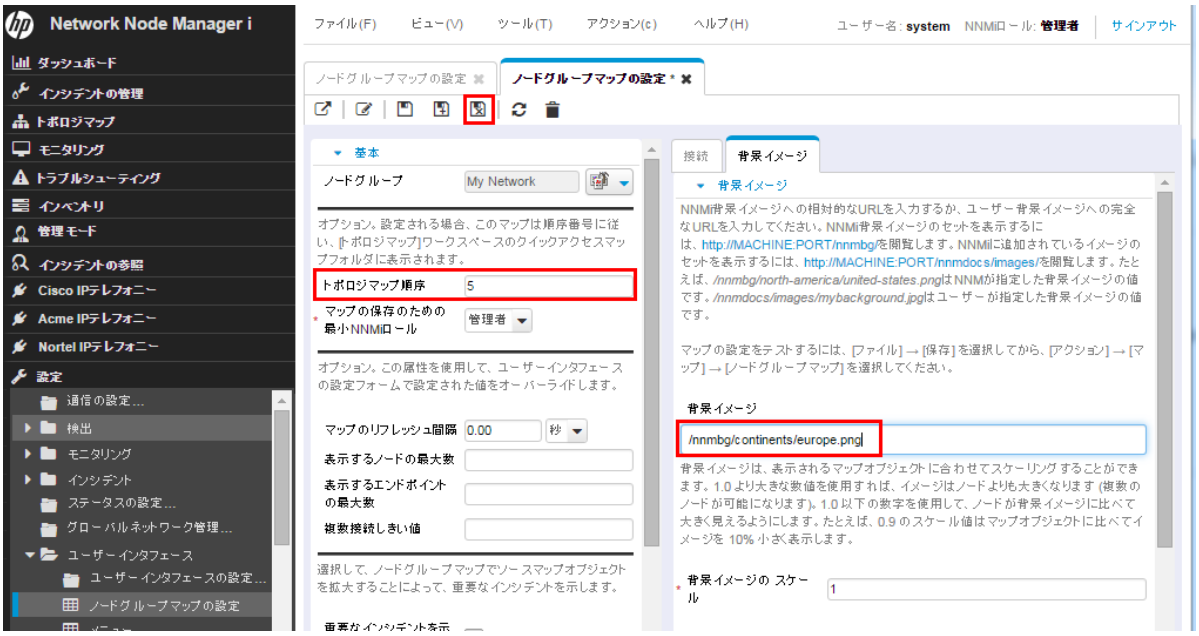
3. [My Network] をダブルクリックします。
4. 背景イメージを追加します。

ヒント: パスの先頭に http://<machine name>を含めるのではなく、/nnmbg/continents/europe.png などのローカルパスを使用してください。これにより、アプリケーションフェイルオーバーが正常に機能するようになります。

---

5. [**トポロジマップ順序**] の値を 5 に変更し、この値が前の例で使用した最低値より小さくなるようにします。
6. [**保存して閉じる**] をクリックします。

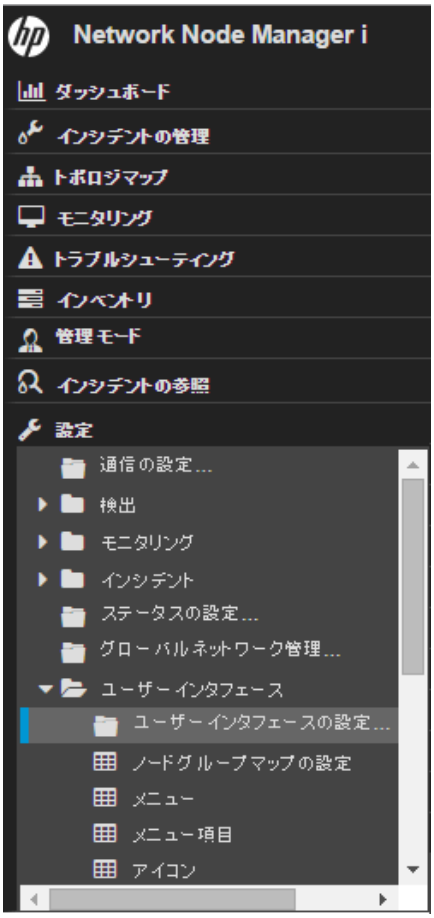
図 72: ノードグループマップの設定の保存



My Network マップを初期ビューに指定するには、以下の手順を実行します。

1. [**ユーザーインタフェースの設定**] をクリックします。

図 73: 設定: ユーザーインタフェースの設定



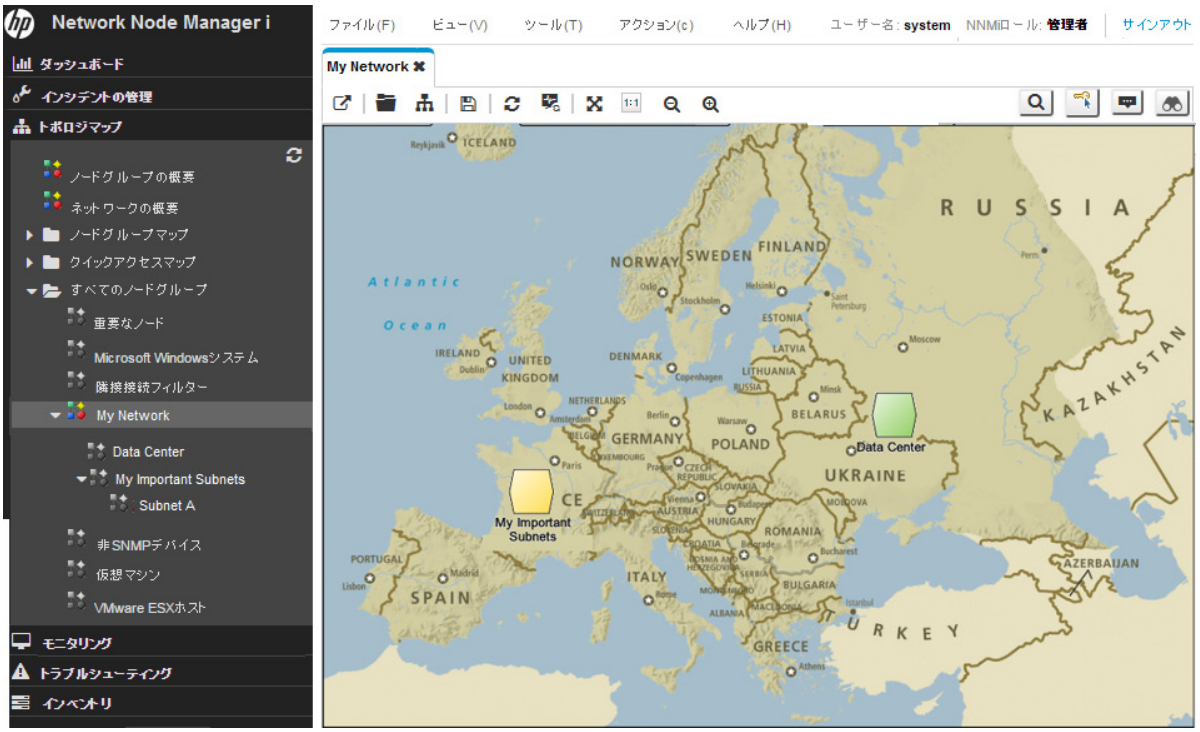
2. [**初期ビュー**] の選択を [**クイックアクセスマップフォルダの最初のノードグループ**] に変更します。[**トポロジマップ順序**] 属性値を 5 に設定しているため、これは My Network マップとなります。

   [**保存して閉じる**] をクリックします。

図 74: ユーザーインタフェースの設定の保存

9 NNMiからサインアウトとしてもう一度サインインすると、初期ビューがMy Networkマップになります。

図 75: My Network マップ



NNMi の保守

NNMiデータのバックアップおよび復元

NNMi には、データの保護に役立つバックアップスクリプトおよび復元スクリプトが用意されています。

バックアップスクリプトは nnmbackup.ovpl です。オンラインまたはオフラインのいずれかでこのスクリプトを使用してください。オンラインオプションでは、NNMi を停止せずにスクリプトを実行できます。このスクリプトを実行すると、毎回同じターゲットディレクトリを指定できるように日時スタンプが含まれたファイル名でバックアップが作成されます。このバックアップには、NNMi 環境の復元に必要なすべての情報が含まれます。

以下に、バックアップスクリプトを使用したコマンドの例を示します。

nnmbackup.ovpl -type online -scope all -force -archive -target /var/tmp/mybackups

以前のコマンドでは、nnm-bak-20110504145143.tar に似た名前のファイルが作成されました。

関連付けられている復元スクリプトは nnmrestore.ovpl です。このコマンドには、nnmbackup.ovpl スクリプトで作成されたバックアップファイルまたはディレクトリが必要です。このスクリプトを実行するには、ovstop -c コマンドを使用して NNMi を停止する必要があります。

nnmrestore.ovpl スクリプトの使用例を以下に示します。

nnmrestore.ovpl -force -source /var/tmp/mybackups/nnm-bak-20110504145143.tar

ソースディレクトリには、バックアップからのファイルのすべて、または単一の tar ファイルが格納されている必要があります。ソースが tar ファイルの場合は、スクリプトにより、現在の作業ディレクトリの一時フォルダーに tar ファイルが抽出されます。このスクリプトにより、復元が完了した後に一時フォルダーを削除します。

注意: NNMi パッチのバージョンをまたいでバックアップを復元したり、NNMi の以前のパッチレベルからのバックアップを復元したりしないでください。

たとえば、以下の場合、パッチ 4 を実行している NNMi 管理サーバーのバックアップをパッチ 5 コードに復元しないでください。これを行うと、NNMi に致命的なエラーが発生します。

- パッチ 4 が NNMi 管理サーバーで実行されている。
- バックアップの実行後、パッチ 5 にアップグレードする。

ヒント: ディレクトリの命名規則を使用して、バックアップで実行するパッチのバージョンを追跡してください。たとえば、バックアップディレクトリを patch4 と命名します。

NNMi の設定のエクスポートとインポート

NNMi の設定は、実行する必要がある重要なタスクの 1 つです。設定は nnmbackup.ovpl および nnmbackupembdb.ovpl スクリプトの一部としてバックアップされますが、NNMi に含まれる nnmconfigexport.ovpl と nnmconfigexport.ovpl スクリプトを使用することを検討してください。これらのスクリプトでは、NNMi 設定の復元を柔軟に行うことができます。これらのスクリプトにより、以下の処理を実行できます。

- 現在の NNMi 設定のスナップショットを作成する
- 設定を小部分に分割する
- 最新のスナップショットに戻す必要がある場合に、NNMi 設定の一部のみ復元する

たとえば、複数のノードグループを作成する場合、重大なミスが発生しても元に戻せるように、エクスポートスクリプトを使用してこれまでの重要なポイントで設定のスナップショットを作成します。

エクスポートスクリプトは nnmconfigexport.ovpl です。nnmconfigexport.ovpl スクリプトを使用して、検出、ノードグループ、インシデントを含むその他の多くの設定エリアを指定します。NNMi には、設定情報をすべてエクスポートするオプションも用意されています。

詳細については、nnmconfigexport.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。

nnmconfigexport.ovpl スクリプトの使用例を以下に示します。

nnmconfigexport.ovpl -c nodegroup -f /tmp

この例の場合、NNMi に以下のメッセージが表示されます。

/tmp/nodegroup.xml を正常にエクスポートしました。

エクスポートされた各設定は NNMi コンソールの 1 つの設定領域に対応しています。

注: nnmconfigexport.ovpl スクリプトはファイルで日付やタイムスタンプを生成しません。このコマンドを自動化する場合、ディレクトリ名に日時スタンプを含めてください。

設定を復元するには、nnmconfigimport.ovpl スクリプトを使用します。

ヒント: ファイルの内容から判別可能なため、設定エリアを指定する必要はありません。

---

nnmconfigexport.ovpl スクリプトの使用例を以下に示します。

nnmconfigimport.ovpl -f /tmp/nodegroup.xml

nnmbackup.ovpl および nnmbackupembdb.ovpl スクリプトの場合と同様に、パッチのバージョンをまたいでこれらのスクリプトを使用しないでください。設定ファイルは NNMi によって検証され、現在のバージョンの NNMi で無効な場合はインポート中に拒否されます。

注意: nnmconfigimport.ovpl スクリプトは、フォーマットが正しい場合、現在の設定を上書きします。

注: NNMi は、他の NNMi 管理サーバーからの設定のインポートをサポートしません。そのため、ある NNMi 管理サーバーで設定エクスポートを作成し、別のサーバーにインポートすることはできません。サーバー間ではフルバックアップ (nnmbackup.ovpl) のみを転送できます。

データベースのトラップのトリム

すべてのNNMiフィルターを通過したトラップは、最終的にNNMiデータベースに保存されます。トラップは、大容量になる可能性があり、NNMi のパフォーマンスに影響を与える場合があります。

ヒント: nnmtrimincidents.ovpl スクリプトを使用して、NNMi データベースからのトラップを定期的にトリムしてください。これらのトラフィックは必要に応じてアーカイブできます。

---

nnmtrimincidents.ovpl スクリプトの使用例を以下に示します。

nnmtrimincidents.ovpl -age 1 -incr weeks -origin SnmpTrap -trimOnly -quiet

この使用例では、1 週間以上過ぎた古いトラップをすべてトリムします。この使用法では、トラップはアーカイブされません。その他のオプションについては、nnmtrimincidents.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。

ヒント: cron ジョブの nnmtrimincidents.ovpl を使用して、古くなった不要なトラップインシデントを定期的にクリアしてください。

注: 最終的に NNMi は、NNMi データベース内のトラップ数が上限の 100,000 に到達すると、トラップのストレージを停止して強制的に NNMi データベースからトラップをトリムします。

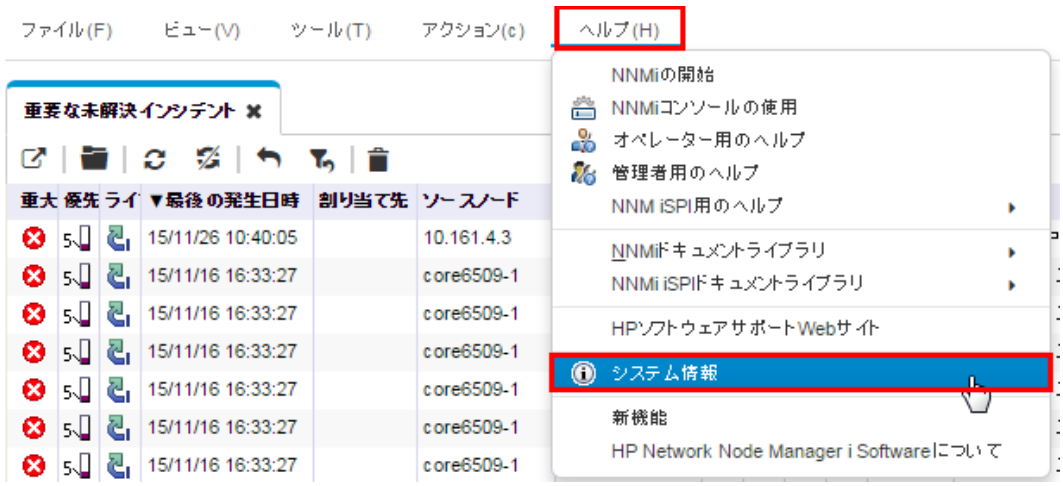
この NNMi データベースのリファレンスは、トラップデータストアとは異なります。詳細については、softwaresupport.hp.com で入手できる『Step- by-Step Guide to Incident Management』を参照してください。

NNMi ヘルスの確認

いくつかの異なるツールを使用して NNMi の一般的なヘルスを確認できます。

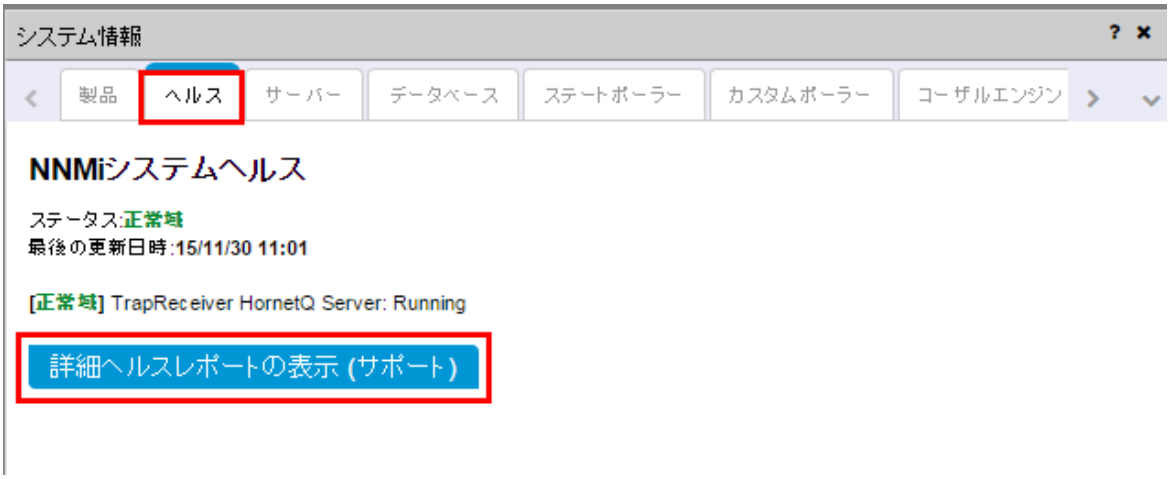
NNMi コンソールから、**[ヘルプ] > [システム情報]** をクリックし、重要な情報の一部をリストします。

図 76: ヘルプ: システム情報



NNMi のヘルスの最適な表示場所は、[**ヘルス**] タブです。NNMi でヘルスの問題が特定されると、ステータスが変わり、このレポートにそのステータスの理由が表示されます。

図 77: システム情報: [ヘルス] タブ



ベストプラクティス

考慮すべき追加の推奨事項を以下に示します。

- **NNMi の組み込みデータベース。**規模が大きい場合でも NNMi の組み込みデータベースを使用します。Postgres の拡張性の高さはテストで実証されています。ネットワークの規模が大きいことだけを理由に Oracle を検討する必要はありません。Postgres は信頼性が高く、NNMi に適したデータベースです。Postgres は NNMi に組み込まれており、NNMi には必要なツールが用意されています。
- **SNMP のタイムアウト設定。**SNMP のタイムアウト設定を調整する場合は注意が必要です。タイムアウト値はタイムアウトごとに増加するため、最初に意図した値を超えて急速に増加する可能性があります。
- **ノードステータス。**NNMi コンソールで、いずれかのトポロジマップをクリックします。表示結果を確認したら、いずれかのノードをダブルクリックしてノードフォームを開きます。[結果] タブをクリックし、データを確認して、現在のステータスがそのノードに設定されている理由を理解してください。

- **ノードグループマップの設定。**[ノードグループマップの設定] フォームの [終了ポイントフィルター] を使用して、ノードグループ間の接続数を減らします。高度に接続されたマップの表示は遅くなるため、NNMi では必要に応じてマップの接続が削除されます。
- **SNMP コミュニティ文字列。**SNMP コミュニティ文字列に@記号を使用しないでください。これは Cisco デバイスの予約文字で、予期しない NNMi の動作を引き起こします。

使用シナリオの例

このセクションでは、3 つの使用シナリオを示します。これらのシナリオ例では、NNMi のみを使用できると想定しています。

ヒント: NNMi は、HP Operations Manager (HP OM) などの他の製品に重要なインシデントを転送できます。

例外管理

NNMi は、ネットワーク障害に関連付けられた根本原因の問題を重要なインシデントとして識別します。

重要な未解決インシデントをすべて表示するには、以下の手順を実行します。

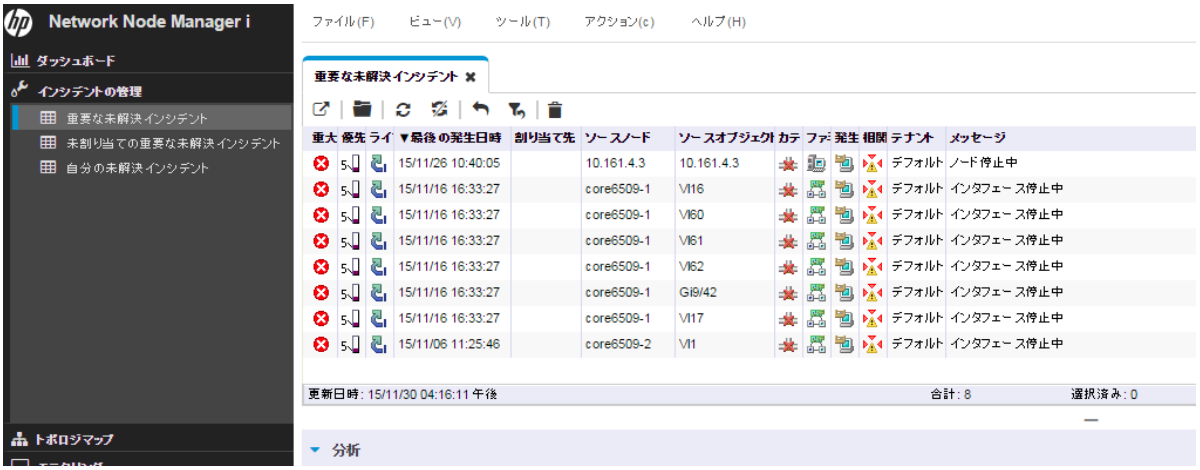
1. ワークスペースのナビゲーションパネルで**[インシデントの管理]** ワークスペースを選択します。
2. [**重要な未解決インシデント**] をクリックします。

NNMi は、ネットワークにおける重要な未解決インシデントをすべて表示し、リストを 30 秒ごとに更新します。重要なインシデントの詳細については、NNMi ヘルプの「オペレータ用のヘルプ」を参照してください。

ヒント: NNMi は、時間を基準に [重要な未解決インシデント] ビューをフィルターします。ドロップダウンメニューを使用して、適切な時間の値を選択します。

以下の例では、前日に発生した重要な未解決インシデントがすべて表示されています。この例では、過去 24 時間以内に 1 つのノードが停止したことが分かります。

図 78: 重要な未解決インシデント



[重要な未解決インシデント] ビューをモニタリングすることにより、ネットワーク問題の原因をピンポイントで突き止め、解決策を導き出すことができます。インシデントビューにはこれらの例外 (または停止) が示されるため、これは例外別の管理です。

例外別の管理手法には、以下の利点があります。

- 問題の根本原因をすばやく確認できます。
- 問題の発生元は、インタフェース、アドレス、ノード、その他の考えられるソースなどのソースオブジェクトとして容易に特定できます。

例外別の管理手法を使用する場合は、以下の点に注意してください。

- ノード停止中インシデントには根本原因のみが表示されますが、停止中のノードは他の多くのノードへの接続に影響する可能性があります。[**トポロジマップ**] ビューを確認して、停止の影響が及ぶ領域を認識してください(詳細については、以下の「マップベースの管理」セクションを参照してください)。
- ノード停止中インシデントのすべての重要性が等しくなることはありません。[**トポロジマップ**] ビューやノードグループ名などの別のツールを活用して、これらのインシデントの優先度を決めることができます。(詳細については、以下の「マップベースの管理」セクションを参照してください)。

マップベース管理

マップを作成してノードステータスの変化を監視することもネットワークを管理する 1 つの方法です。これらのマップは、地域やビルなどのさまざまな方法で調整できます。

[トポロジマップ] ワークスペースで使用できるすべてのマップはノードグループで調整できます。ノードグループマップについて以下の点に注意してください。

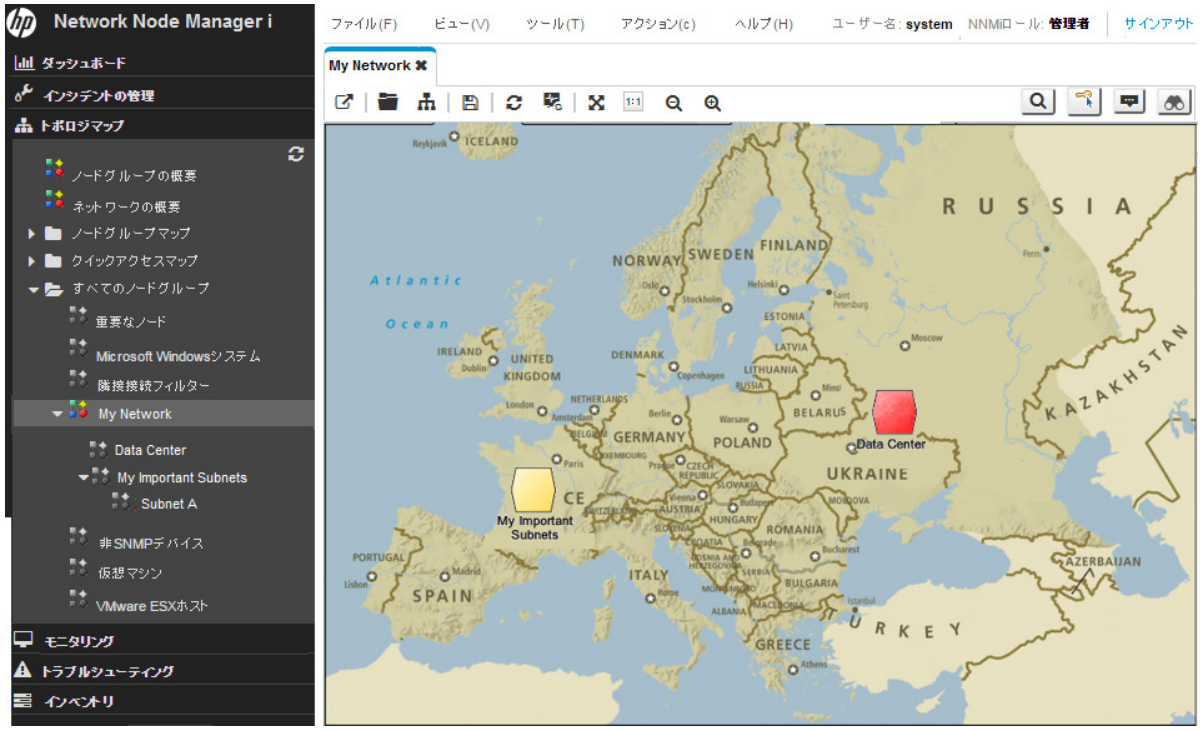
- ステータスは、子ノードグループのノードから親ノードグループマップまで伝達されます。
- NNMi では、デフォルトでノードグループの最もクリティカルなノードステータスが階層の上方向に伝達されます。これにより、高いレベルからノードステータスを監視できます。
- トップレベルのノードグループマップの色が緑から赤、黄、またはオレンジに変わった場合、問題のノードが見つかるまでノードグループマップに移動できます。問題のノードに達したら、前のセクションで説明されているようなアクションを実行し、問題のトラブルシューティングを行うことができます。
- トラブルシューティングの進行状況に関する情報を記録する場合、インシデントと同様にノードやインタフェースにも注記を付けることができます。

以下の画面キャプチャーは、修正が必要な問題を持つ My Network マップの例を示しています。この例では、[ノードグループ] アイコンをダブルクリックして障害ノードを探しています。

ヒント: NNMi 管理者は、初期サインインの後に NNMi に表示されるデフォルトマップを指定できます。

NNMi コンソールからノードグループマップに移動するには、[**トポロジマップ**] をクリックして、意図するマップの名前を選択します。

図 79: [My Network] トポロジマップ



マップベース管理手法には、以下の利点があります。

- 停止を簡単に調査できます。他のノードに影響がある場合でも、隣接するノードのステータスに基づいてすぐに明らかになります。
- 影響のある場所を簡単に特定できます。このアプローチでは、最初に行うべき作業の決定が容易になります。

マップベース管理手法を使用する場合は、以下の点に注意してください。

- 問題の発生元を見つけるには、ノードを開き、[結果] タブに移動して問題を特定します。
- ノードグループのノードがすでに停止している場合、NNMi では同じノードグループの他の 1 つ以上のノードが停止していることは示されません。

リストベース管理

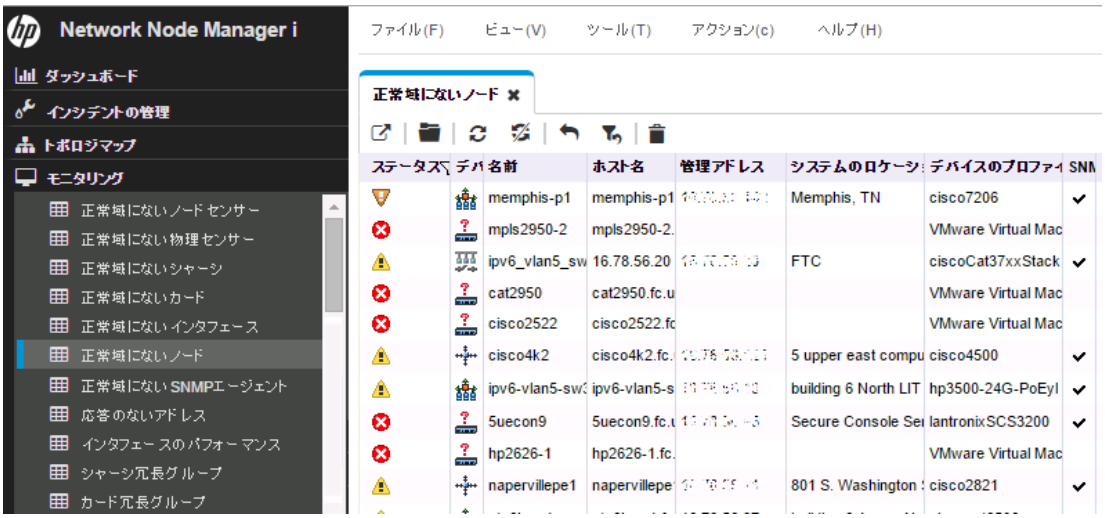
NNMi では、動的なリストでネットワークを管理できます。NNMi には、問題が発生しているノードまたはインタフェースを表示するテーブルが用意されており、動的に更新されます。このリストは、通常 15 秒ごとに NNMi によって更新されます。前のセクションで説明されているように、リストからツールを使用して問題を診断および修正できます。このリストは動的であるため、ノードまたはインタフェースが正常なステータスに戻ると、NNMi によってノードまたはインタフェースがこのリストから削除されます。

たとえば、ステータスが異常なノードをすべて表示するには、以下の手順を実行します。

1. ワークスペースのナビゲーションパネルで [モニタリング] ワークスペースを選択します。
2. [**正常域にないノード**] をクリックします。

以下の例に示すように、NNMi にはステータスが「正常域」以外のノードがすべて表示されます。

図 80: 正常域にないノード



リストベース管理手法には、以下の利点があります。

- 調査する必要のあるノードまたはインタフェースの数を把握できます。
- ネットワークのトラブルシューティングを行うのに、NNMi マップに移動する必要はありません。

リストベース管理を使用する場合、以下の点に注意してください。

- NNMi のステータスの履歴には最大 5 つのエントリが含まれます。
- NNMi では、停止中のノードの「陰に隠れている」ノードに [危険域] ステータスは割り当てられません。詳細については、NNMi ヘルプの「オペレータ用のヘルプ」を参照してください。
- リストベースビューでは、ノードの物理的な場所は示されません。

結論

このドキュメントでは、小規模なテストネットワークでの NNMi デプロイメントについて説明します。このドキュメントには、ライセンスのインストール、ユーザーの作成、通信の設定、検出、インシデント、トラップ、アクション、および NNMi コンソールに関する情報が含まれています。また、NNMi のメンテナンスタスクや NNMi ヘルスの監視方法についても説明しています。さらに、NNMi のベストプラクティスや考えられる使用シナリオについてもいくつか取り上げています。

フィードバックをお寄せください

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 宛て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: NNMi を導入するためのステップバイステップガイド

フィードバック:

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。ここに記載された情報は追加の保証をなすものではありません。HP ではここに記載されている技術的、または編集上の不正確さや脱漏については責任を負いません。

ここに記載する情報は、予告なしに変更されることがあります。

制限付き権利

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

著作権について

商標について

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

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

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

Google™は、Google Inc.の登録商標です。

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

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

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

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

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

sFlow は、InMon Corp.の登録商標です。

UNIX®は The Open Group の登録商標です。

Oracleテクノロジ - 権利制限について

DOD FAR Supplement によって届けられたプログラムは、「商業用コンピューターソフトウェア」であり、ドキュメントを含むプログラムの使用、複製、開示については Oracle の適切なライセンス契約に基づくライセンス制限に拠る必要があります。さらに、Federal Acquisition Regulations によって届けられたプログラムも「商業用コンピューターソフトウェア」であり、ドキュメントを含むプログラムの使用、複製、開示については FAR 52.227-19、商業用コンピューターソフトウェア制限についての権利 (6 月、1987) に拠る必要があります。Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Oracle のライセンスに関する全文は、NNMi 製品 DVD のライセンス契約のディレクトリを参照してください。

謝辞

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

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

サポート

以下の HP ソフトウェアサポート Web サイトを参照してください。

www.hp.com/go/hpsoftwaresupport

この Web サイトには、連絡先情報、および HP ソフトウェアが提供している製品、サービス、サポートに関する詳細が記載されています。

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

- 関心のあるナレッジドキュメントの検索
- サポート事例と改善要求の送信と追跡
- ソフトウェアパッチのダウンロード
- 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に関する情報のレビュー
- 他のソフトウェアーユーザーとの情報交換
- ソフトウェアートレーニングの調査と登録

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

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

アクセスレベルの詳細については、次の URL にアクセスしてください。

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