HP Network Node Manager i Software

NNMi を導入するためのステップバイステップ ガイド

NNMi 9.1x パッチ 1

このドキュメントでは、小規模なテスト ネットワークに新しい NNMi 9.10 インストールを導入する方法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 i Software 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。

最新の『HP Network Node Manager i Software デプロイメント リファレンス』については、http://h20230.www2.hp.com/selfsolve/manuals を参照してください。

目次

基本手順: 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。
- サーバーがすべてのシステム前提条件 (http://h20230.www2.hp.com/selfsolve/manuals にある『HP Network Node Manager i Software システムとデバイス対応マトリックス』に記載されているパッチ前提条件やカーネル パラメータなど) を満たしている。

注意: NNMi インストール スクリプトでは、サーバーがシステム前提条件を満たしているかどうかはチェックされません。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。

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. 監視の設定
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。

1. セキュリティ グループおよびマルチテナント
2. 他の HP 製品 (HP Operations Manager (HP OM) や HP Universal Configuration Management Database (HP UCMDB) など) やサードパーティ製品との統合
3. 高可用性またはアプリケーション フェイルオーバー
4. リモート Oracle データベースの使用
5. NNM iSPI (NNM iSPI for Performance や NNM iSPI for MPLS など)

ライセンスの適用

インスタントオン ライセンスを使用したり、HP からより大規模な一時ライセンスを取得したりできます。

NNMi ライセンス構造に関する詳細について HP 営業担当または Hewlett-Packard 正規販売店に問い合わせて、企業向けインストールにライセンス層を追加する方法について調べます。追加のライセンス キーを取得するには、HP ライセンス キー配信サービス (https://webware.hp.com/welcome.asp) に移動します。

注: インスタントオン ライセンスでは、NNMi で 250 ノードを使用できます。

コマンド ラインを使用してライセンスを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コマンドの例を示します。

```
nnmlicense.ovpl NNM -f ./mylicense.key
```

元の設定のバックアップ

変更する前に元の NNMi の設定をバックアップします。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が作成されています。
2. **nnmconfigexport.ovpl** コマンドを **-c** および **-f** オプションを使用して実行します。**-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コマンドの例を示します。

   ```
   nnmconfigexport.ovpl -c all -f /var/tmp/origconfig/
   ```

   nnmconfigexport.ovpl スクリプトを実行したら、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。
   ```

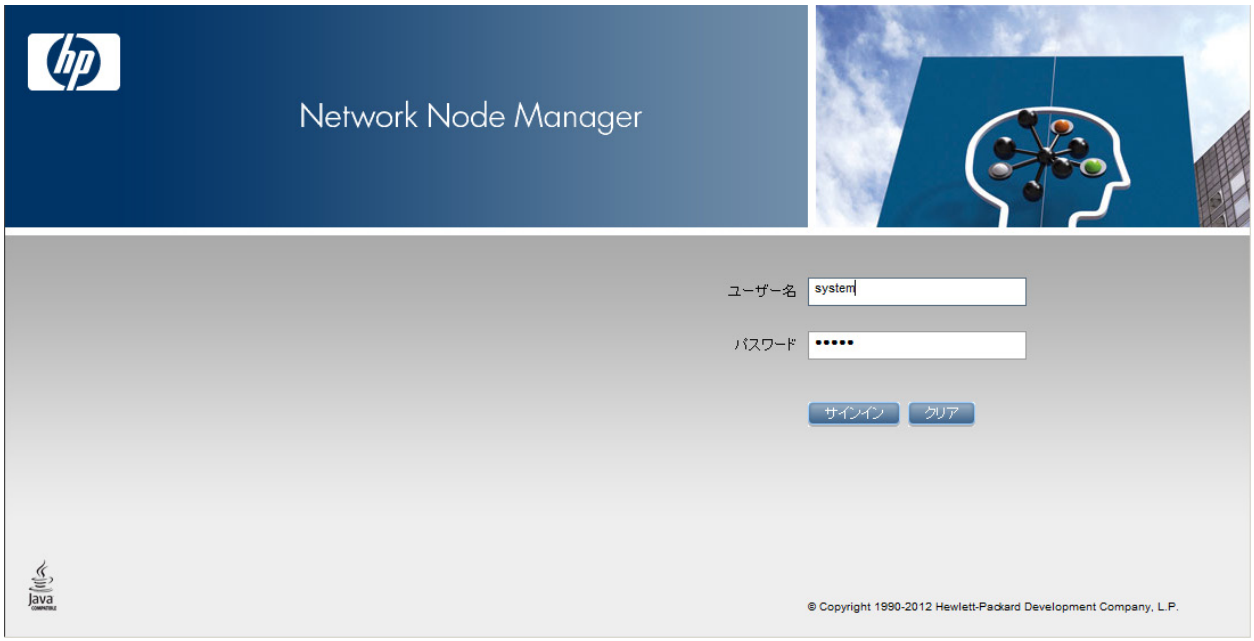
NNMi へのサインインとユーザーの作成

最初のサインイン

Internet Explorer や Mozilla Firefox などのブラウザを使用して、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 のサインイン画面



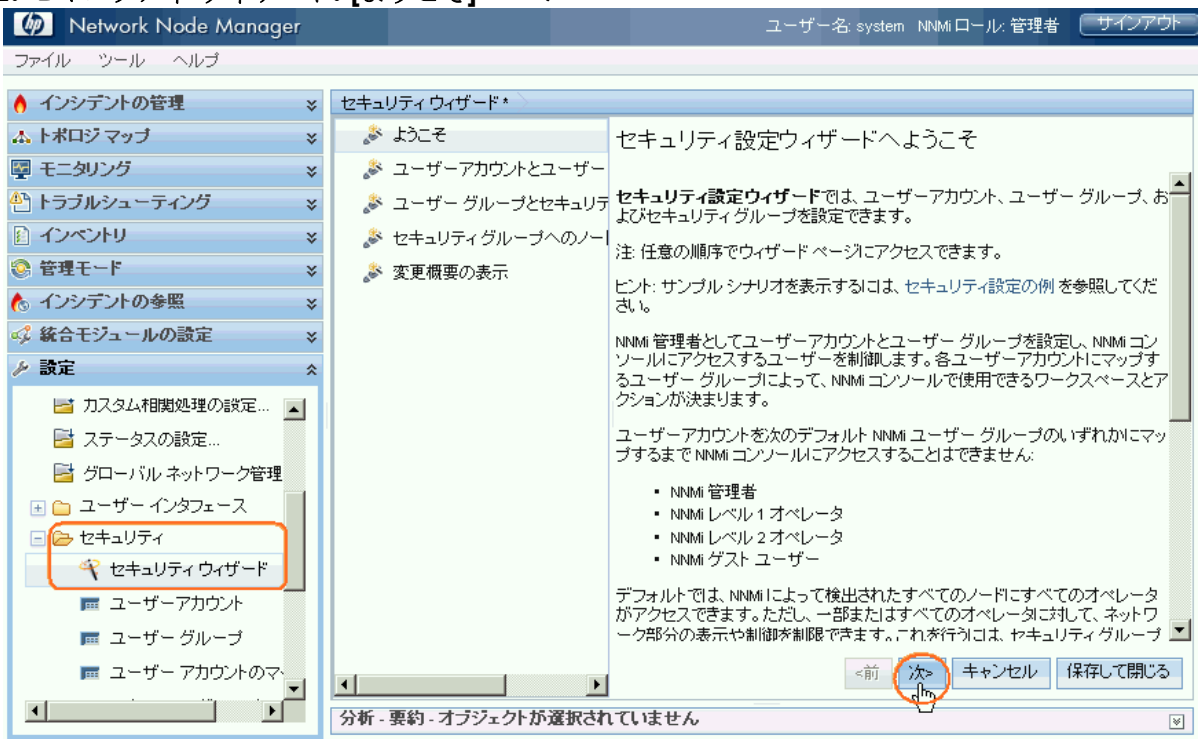
ユーザー アカウントとロールの作成

通常、ユーザー名に `system` を使用しないでください。以下の手順に従って、通常の作業で使用する管理者アカウントを作成して使用してください。

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]** フォルダを展開します。
3. **[セキュリティ ウィザード]** をクリックし、**[次へ]** をクリックします。

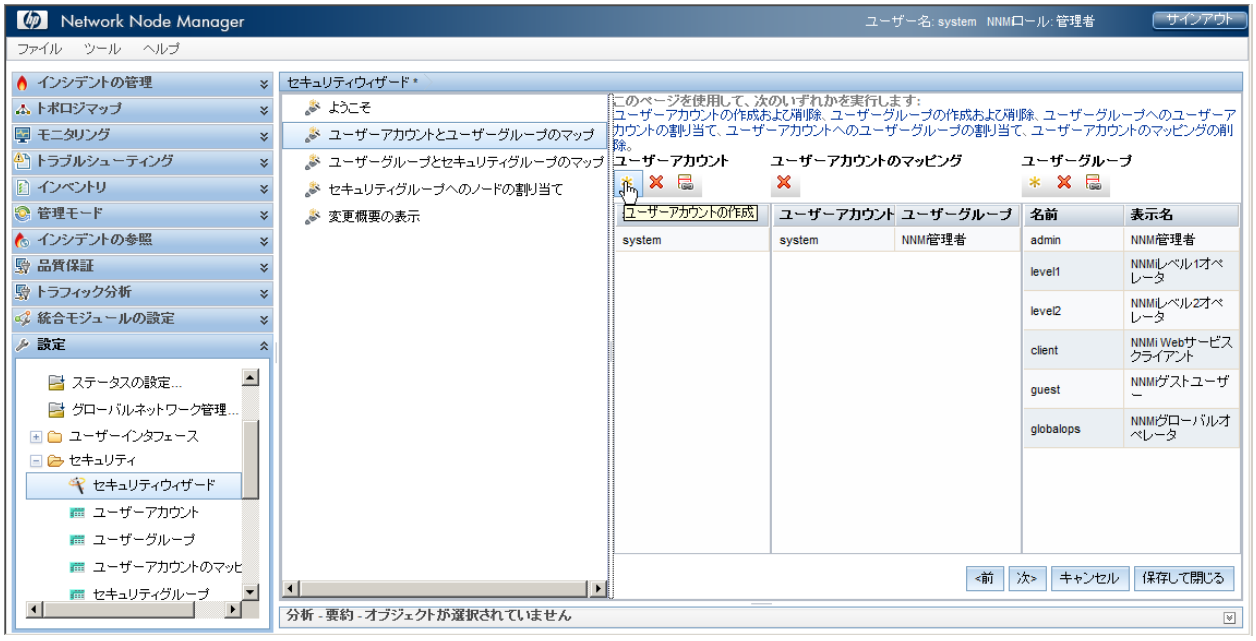
セキュリティ ウィザードの [ようこそ] ページが表示されます。

図 2: セキュリティ ウィザード: [ようこそ] ページ



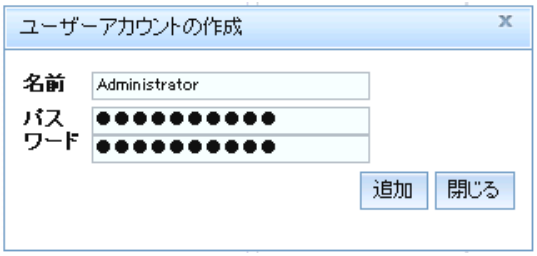
4. **[ユーザー アカウント]** に移動し、 * アイコンをクリックします。

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て **[追加]** をクリックし、**[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

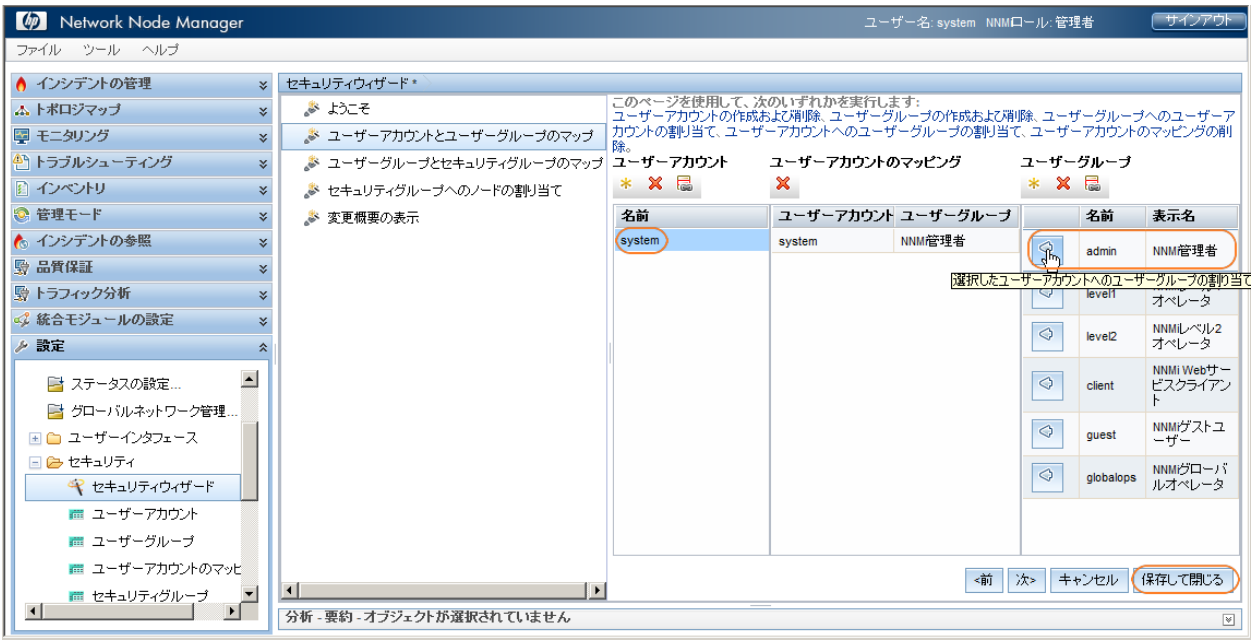


6. **[ユーザー アカウント]** 列で新しいアカウント名をクリックします。次に、適切なユーザー グループの横にある アイコンをクリックし、ユーザー アカウント マッピングを作成します。

7. **[保存して閉じる]** をクリックします。次に、**[OK] > [OK]** をクリックして変更を適用します。

ヒント: ユーザー アカウント マッピングは、以前のバージョンの NNMi の「ロール」という概念に置き換わるものです。

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 グループの割り当て



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

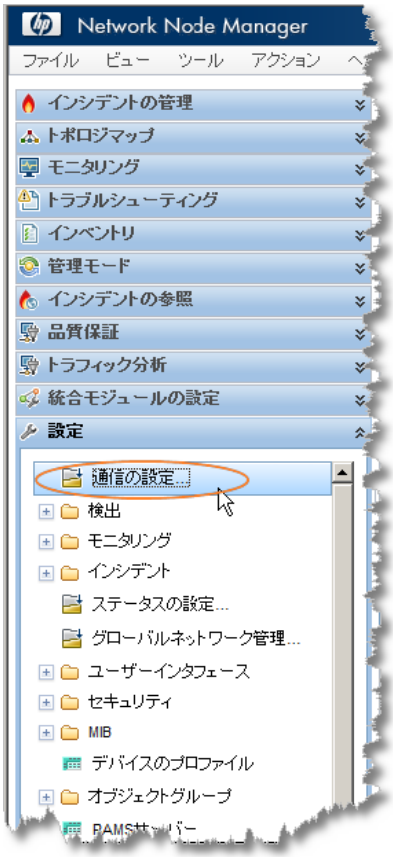
NNMi では、デフォルトで *SNMP コミュニティ文字列の検出*が実行されます。この例では、このデフォルトの方法の使い方が説明されています。

ヒント: 以前のバージョンの NNMi とは異なり、優先順位を付けた SNMP コミュニティ文字列のリストを設定する必要はありません。

NNMi では、デフォルトですべてのコミュニティ文字列の候補が順番に試行されます。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、より複雑な解決方法を実装することもできますが、通常はこの方法で十分です。

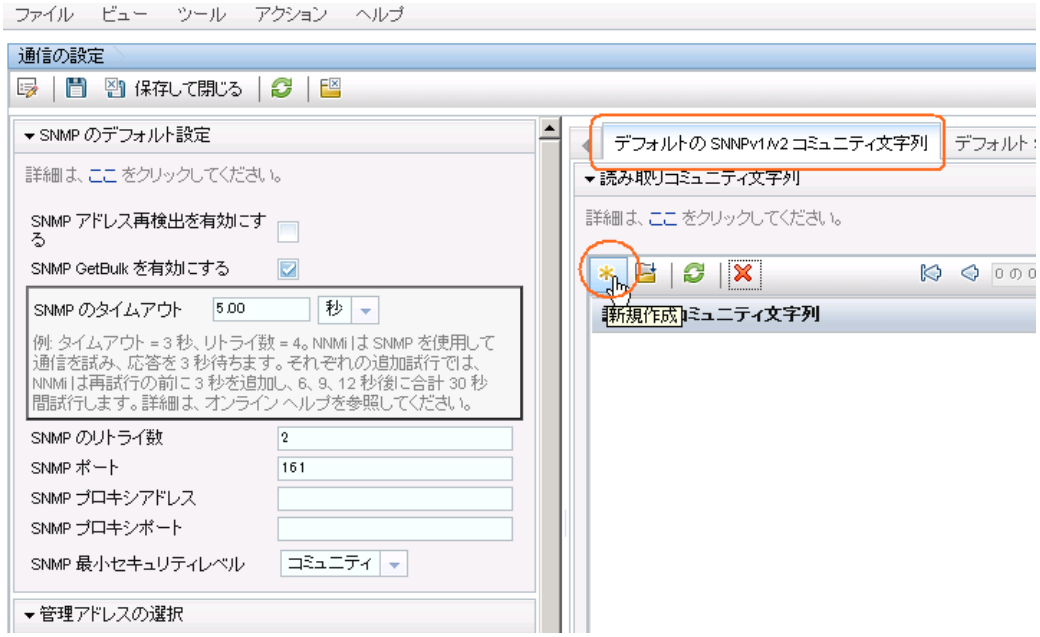
1. ワークスペースのナビゲーション パネルで **[設定]** ワークスペースを選択し、**[通信の設定]** をクリックします。

図 6: 通信の設定



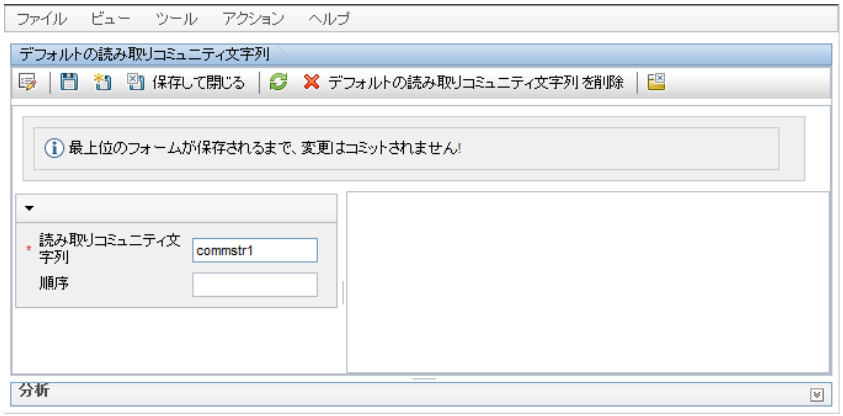
2. **[デフォルトの SNNPv1/v2 コミュニティ文字列]** タブをクリックします。次に、* アイコンをクリックし、新しいコミュニティ文字列を作成します。

図 7: 通信の設定: [デフォルトの SNNPv1/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



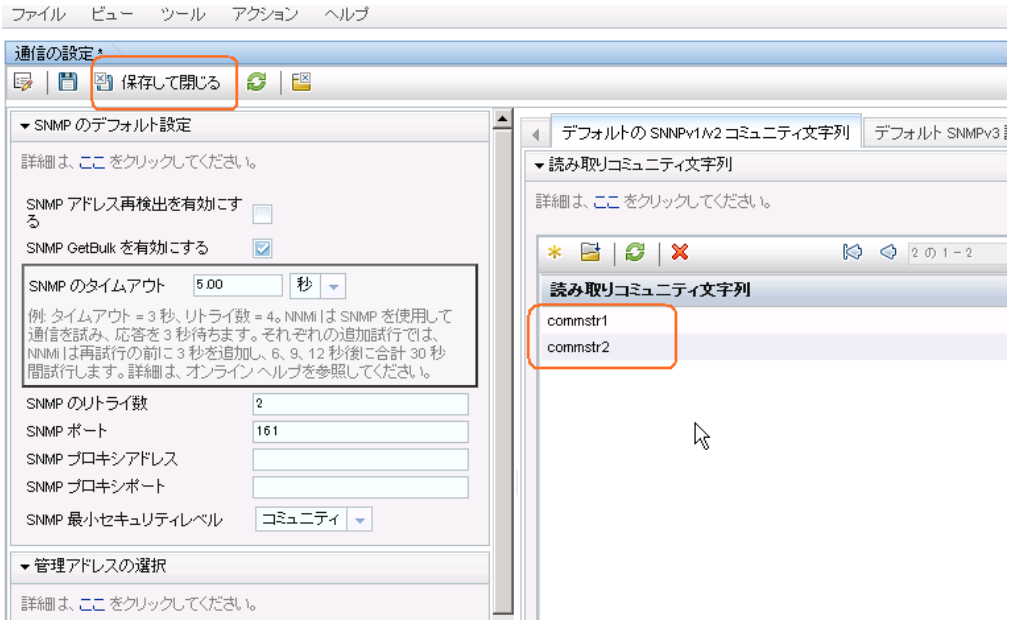
4. すべてのコミュニティ文字列に対して前の手順を繰り返します。

ヒント: 追加の変更を行う場合は、他の通信設定オプションを探してください。

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

SNMP の設定は完了しました。

図 9: 通信の設定: 保存して閉じる



検出の設定

NNMi では、*リストベースと自動*の 2 つの検出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、ノードの名前またはアドレスのリストが入力として使用され、そのリストに含まれるノードのみが検出されます。NNMi では、このリストに含まれていないノードの名前またはアドレスは検出されません。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 では、IP アドレスが自動検出の範囲外でも各シードがロードされます。

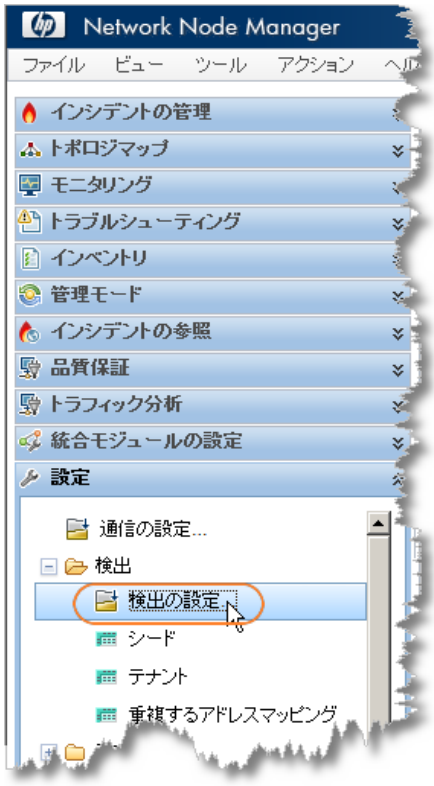
ヒント: デバイスの IP アドレスとしてシードをロードする場合、優先される管理アドレス (通常は、Cisco ギアを使用したループバック アドレス) をシードとして指定することをお勧めします。

自動検出では、ユーザー指定の条件に基づいてネットワーク上のノードが検出されます。アドレス範囲、SNMP の値 (システム オブジェクト ID など)、デバイス タイプ、およびその他の方法に基づいて、検出されるノードを制限するように NNMi を設定できます。1 つのシード ノードを使用して自動検出を設定できます。ただし、オプションの *ping スイープ*機能を有効にすれば、このノードも必要ありません。

以下の例では、アドレス範囲に基づいた自動検出が説明されています。また、この例では、いくつかのシード ノードをロードする方法も示されています。

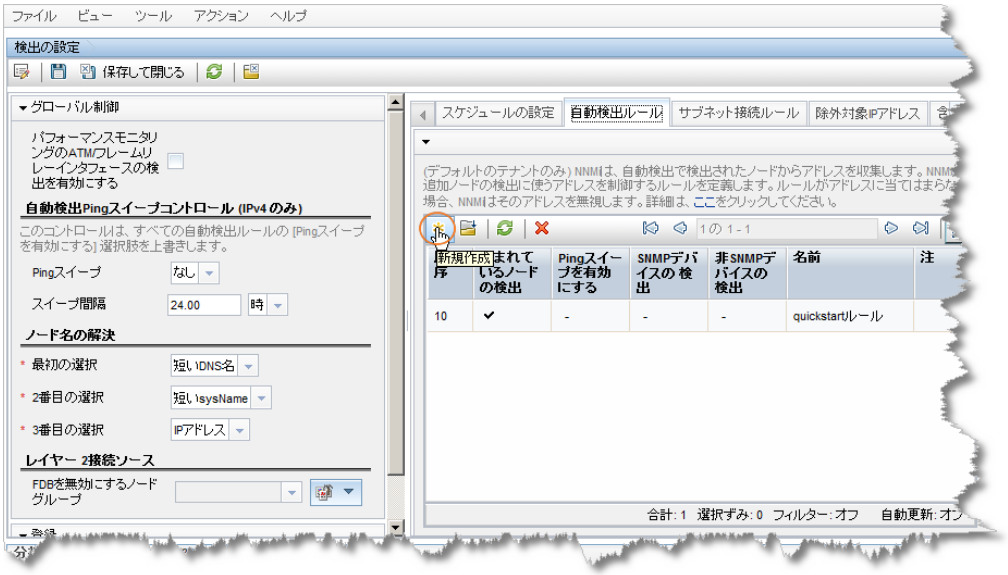
1. ワークスペースのナビゲーション パネルで **[設定]** ワークスペースを選択し、**[検出]** フォルダを展開します。次に、**[検出の設定]** をクリックします。

図 10: 検出の設定



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

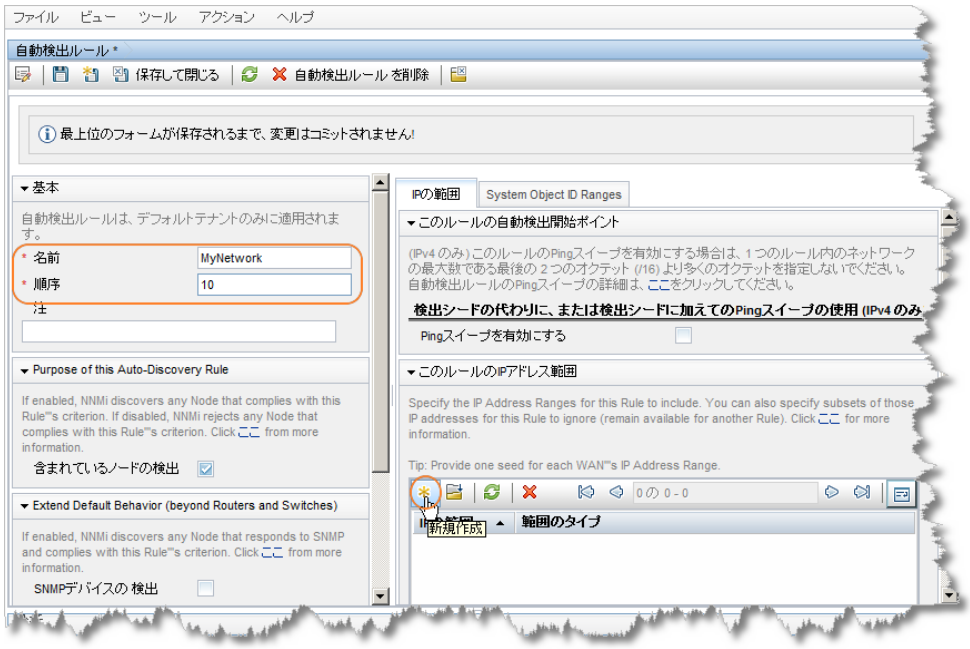
図 11: 検出の設定: 自動検出ルール



3. [基本] セクションを入力します。

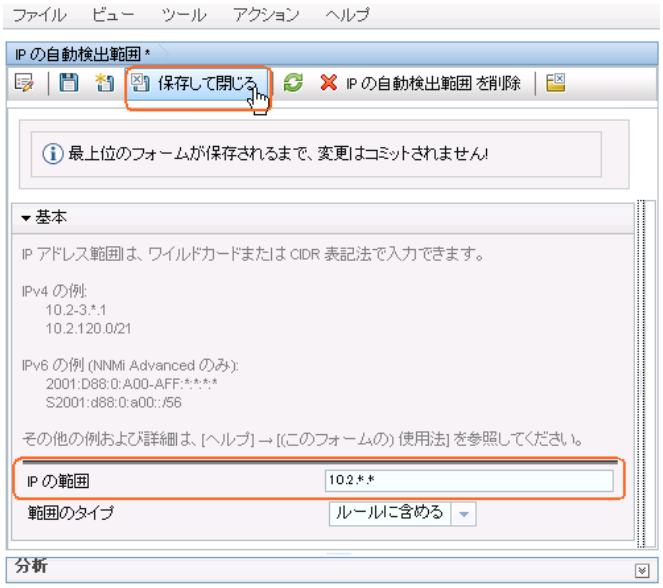
ヒント: NNMi では、**[順序]** 属性の値を使用して、複数の自動検出ルールに優先順位を付けます。この例では、1 つの自動検出ルールのみが使用されています。

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 の範囲]** テキスト ボックスに検出する IP 範囲を入力します。包含ルール ([ルールに含める]) と除外ルール ([ルールにより無視された]) の両方を入力できます。包含ルールよりも除外ルールの方が優先されます。

図 13: IP の自動検出範囲



6. このフォームと [自動検出ルール] フォームで **[保存して閉じる]** をクリックし、変更を保存します。

この例では、ping スイープ機能は使用されていません。

ヒント: 環境内で ping スイープ機能を使用すると、各自動検出ルールでクラス B ネットワーク (10.2.*.* など) の最大数が NNMi によってスイープされます。

以下の項に注意してください。

- デフォルトでは、定義された IP アドレス範囲内のルーターとスイッチのみが NNMi によって検出されます。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。
- ノードに複数のアドレスがある場合 (ルーターなど)、いずれかのアドレスのみが IP 範囲に含まれるようにする必要があります。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すると、最初に想定していたよりも多くのノードが NNMi によって検出される可能性があります。

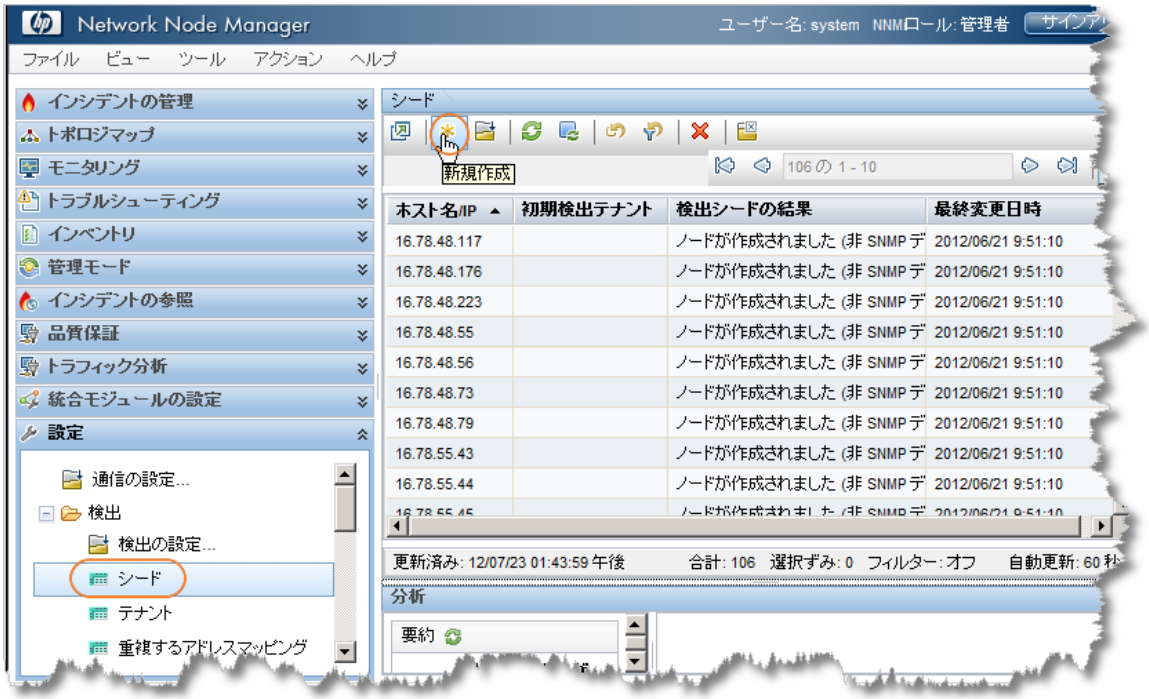
これで 1 つの自動検出ルールが定義されました。各ルールは極めて複雑になる場合があるため、通常は 1 つの自動検出ルールで十分です。

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: ルーターの場合、NNMi 検出に多数のアドレス セットを使用できるため、スイッチではなくルーターをシードとして追加することをお勧めします。

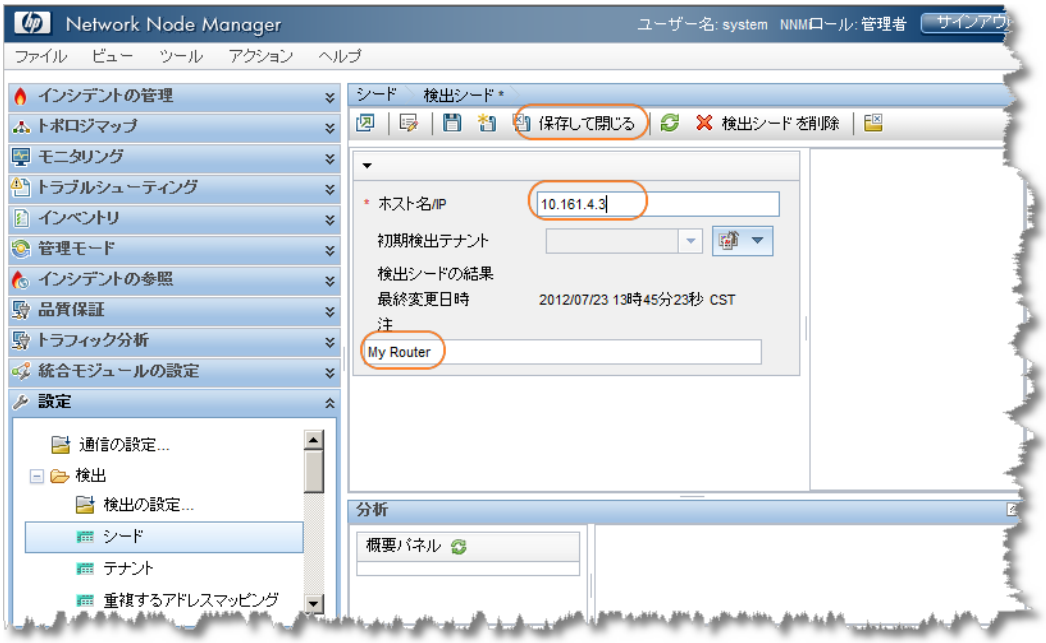
1. ワークスペースのナビゲーション パネルで **[設定]** ワークスペースを選択し、**[検出]** フォルダを展開します。次に、**[シード]** を選択します。
2. アイコンをクリックして、新しいシードを作成します。

図 14: 検出: シード



3. **[検出シード]** フォームで、目的のホスト名または IP アドレスおよび任意のノードを入力し、**[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] 列を調べて、各シードの検出ステータスを判別します。NNMi によってノードの検出が開始されると、NNMi に進行状況が [進行中] として表示されます。検出が完了すると、[検出シードの結果] のエントリが [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

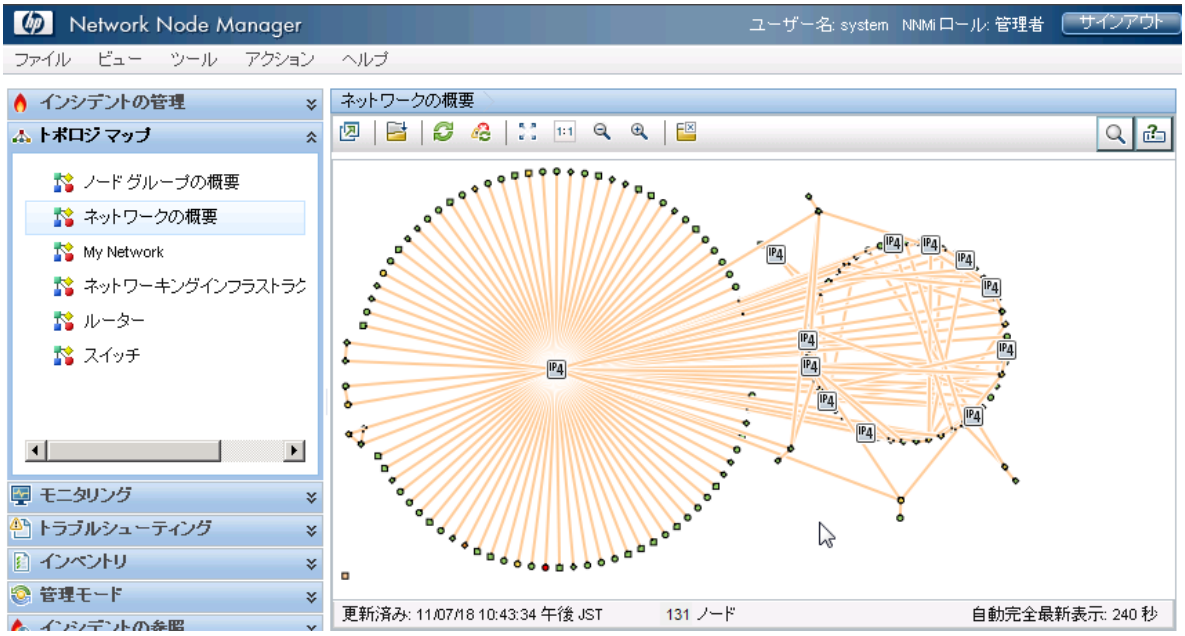
ヒント: `nnmloadseeds.ovpl` スクリプトを使用してファイルからシードのリストをロードすることもできます。このスクリプトでは、多数のシード ノードをロードできます。自動検出ルールではなくリストベース検出を使用する場合、`nnmloadseeds.ovpl` スクリプトを使用してすべてのノードをロードできます。詳細については、`nnmloadseeds.ovpl` のリファレンス ページまたは UNIX のマンページを参照してください。

自動検出の方法を使用する場合、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他のスイッチやルーターの検出が自動検出によって開始されます。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、小規模な環境で検出の進行状況を表示する場合に便利です。これは、**[ネットワークの概要]** マップに表示されるノードおよび接続が制限されているためです。

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

図 17: トポロジ マップ: ネットワークの概要



監視の設定

NNMi の監視は、柔軟性があり簡単に設定できます。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。非 SNMP ノードの場合はこの限りではありません。これらのノードは ICMP を使用してポーリングされます。必要に応じて、ICMP ポーリングの範囲を拡張できます。

NNMi では、デフォルトで *接続*インタフェースがポーリングされます。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 個のポートを備えたアクセス スイッチが、デスクトップ コンピュータと 1 つのアップリンク ポートに接続されている。
- NNMi でアップリンク ノードは検出されたが、デスクトップ コンピュータは検出されていない。

この場合、デスクトップ コンピュータに接続されていることが示されていないため、アップリンク ポートのみが NNMi に*接続されている*と見なされます。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。

以下の例の `c2900xl-1` スイッチは、1 つのアップリンク (`Fa0/2`) を備えたアクセス スイッチです。図 19: [ノード] フォーム: インタフェースのリストで示すように1 つのインタフェースのみが監視されます。

図 18: マップ ビュー: 監視されている 1 つのインタフェース

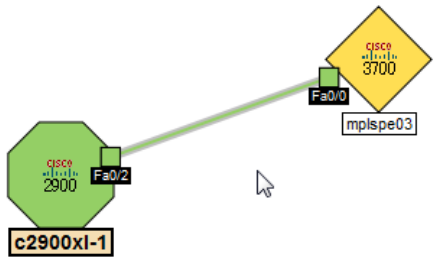
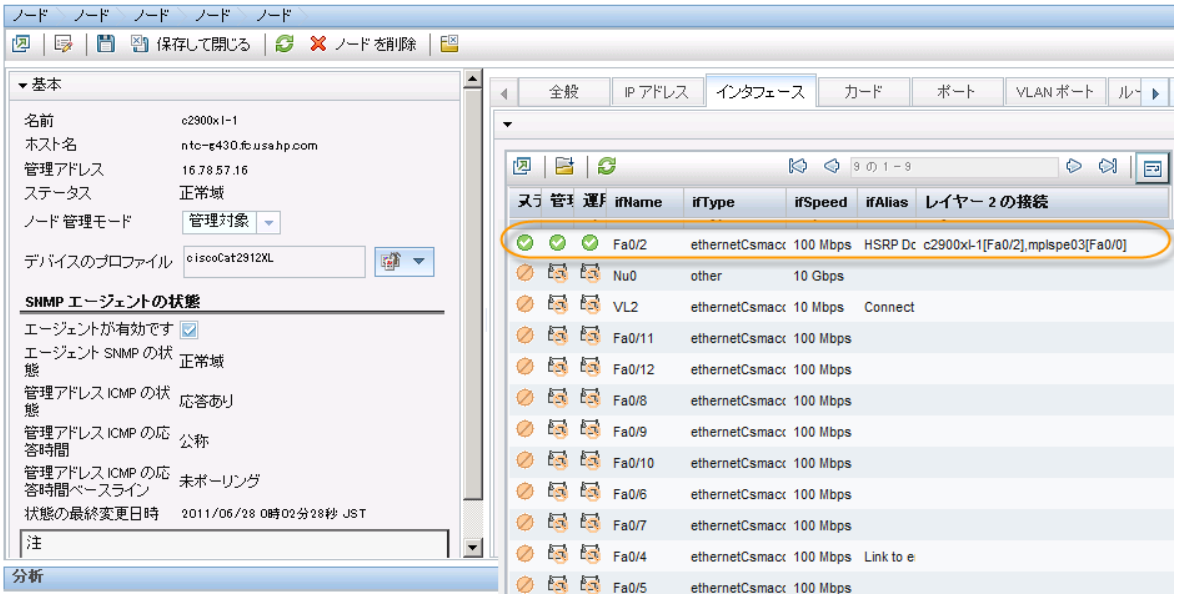


図 19: [ノード] フォーム: インタフェースのリスト



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。デフォルトでは、NNMi によってクラウドへの接続が検出およびモデリングされない可能性がありますが、ルーター インタフェースは監視されます。

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。

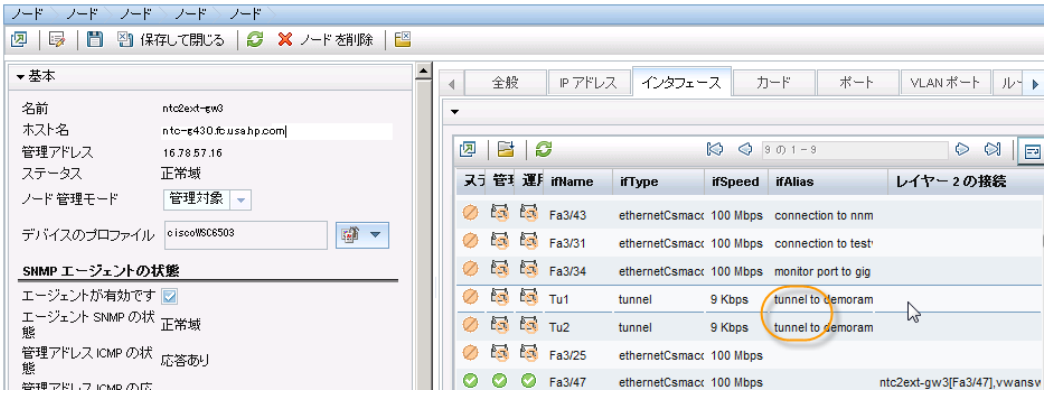
- NNMi では、大量の監視設定を変更できます。
- NNMi では、フィルタを使用して個々のノード、インタフェース、およびアドレスに監視を適用することでこれを行います。これらのフィルタは、ユーザー インタフェースで使用できるフィルタと同じです。
- このドキュメントでは、ノードとインタフェースに重点が置かれていますが、NNMi ではファンや HSRP グループなどのエンティティも監視対象となります。

以下のシナリオについて考えます。

- ノードのサブセットのインタフェースに `tunnel to` で始まる `IfAlias` がある。
- これらのインタフェースの速度が 9 Kbs 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を作成し、これらの条件を満たすインタフェースを特定できます。このフィルタを作成したら、監視設定をこれらのインタフェースに適用します。

図 20: [ノード] フォーム: 監視設定の適用

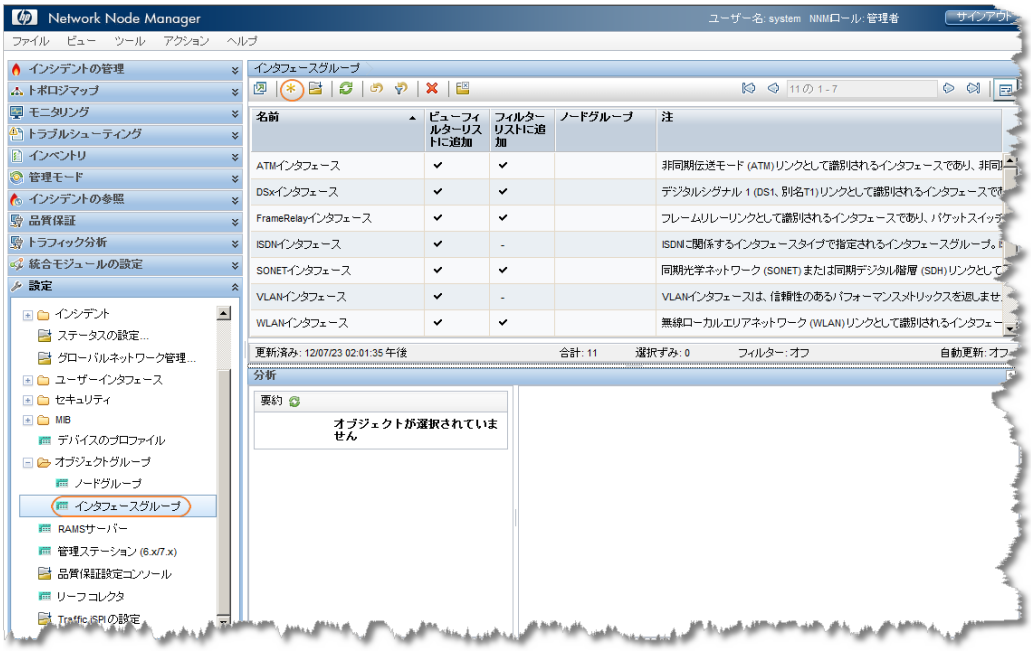


監視対象インタフェース グループの作成

NNMi では、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、**[インタフェース グループ]** をクリックします。

図 21: 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`** などのわ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、フィルタ ロジックを定義する **[フィルター エディタ]** にアクセスします。

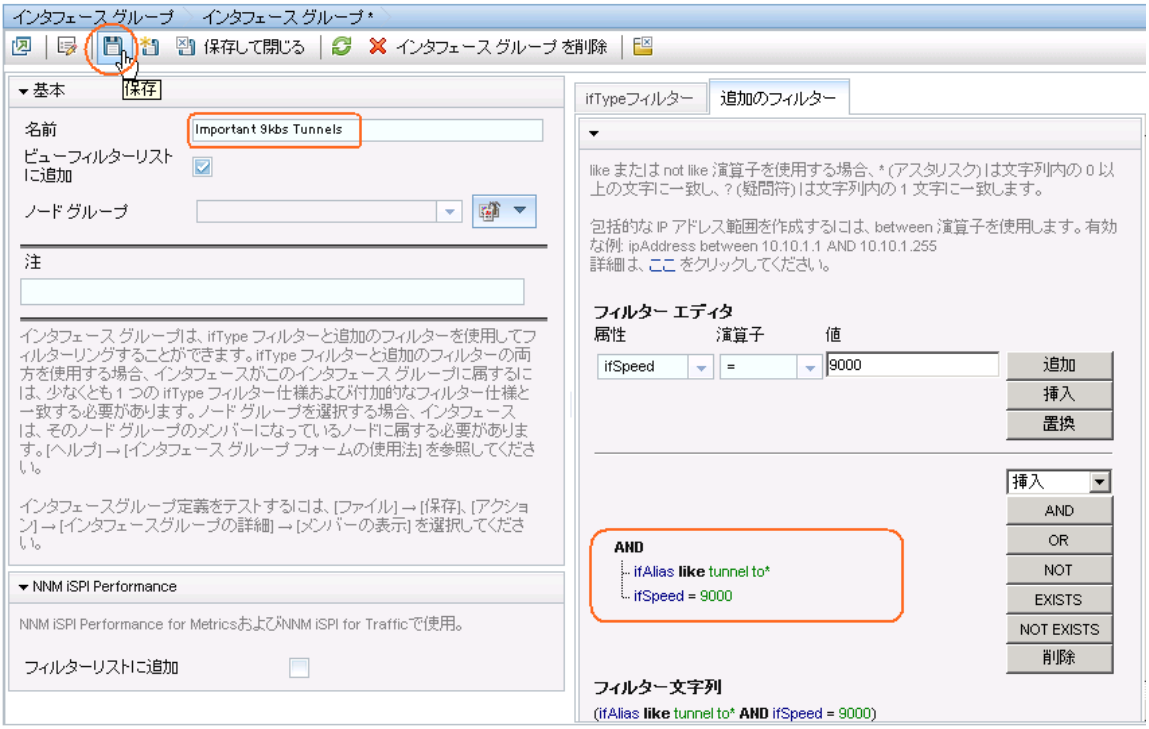
[属性]、[演算子] および [値] を選択してフィルタ式を定義します。`like` 演算子とアスタリスクを併用して変数を照合できます。

この例では、2 つの属性に対して AND 条件が使用されています。

ヒント: ロジックを定義しているときに問題が発生した場合、最後に保存した値に戻れるように保存しないでフォームを閉じます。その後、フォームをもう一度開いて再開します。

注: (**[IfType フィルター]** タブで) IfType フィルタを定義する場合、**[追加のフィルター]** タブのフィルタと常に論理 AND の関係になります。

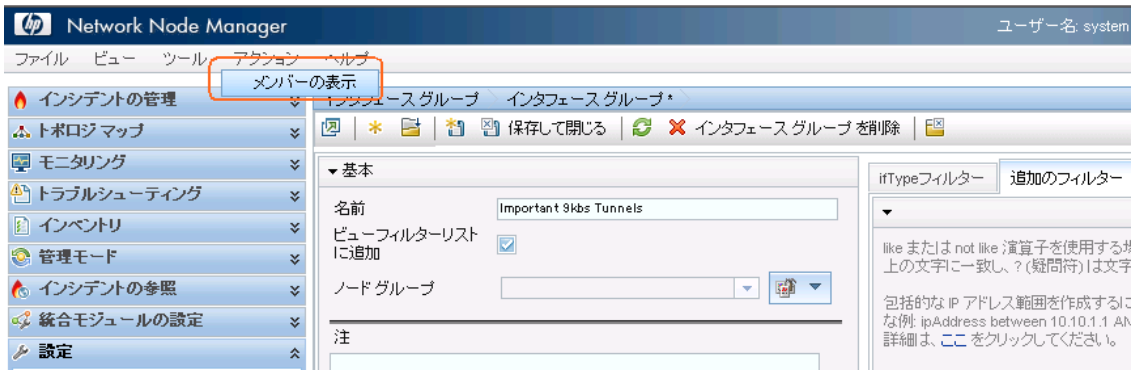
図 22: インタフェース グループ: 保存



5. フィルタを指定したらフィルタを保存しますが、閉じないでおきます。
6. **[アクション] > [メンバーの表示]** メニュー項目を使用して、フィルタが適切に動作することを確認します。

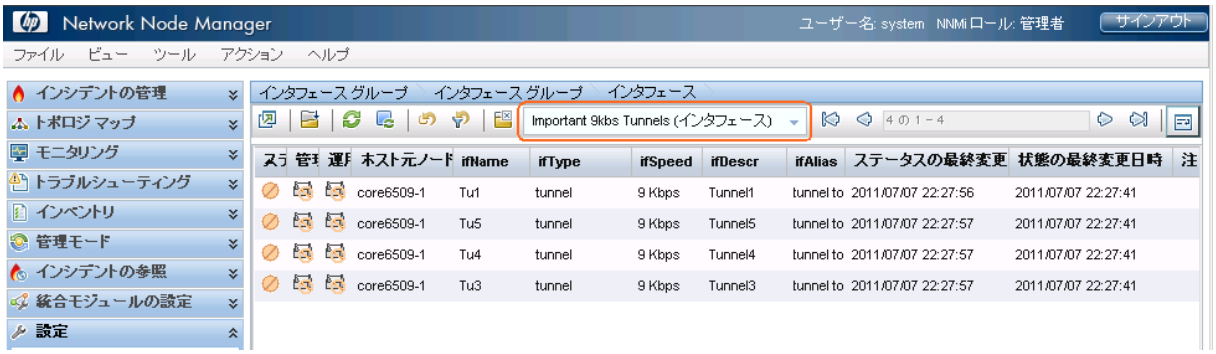
NNMi には、フィルタ条件を満たした項目がすべて表示されます。

図 23: アクション: インタフェース グループ 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 24: インタフェース: インタフェース グループのフィルタの結果



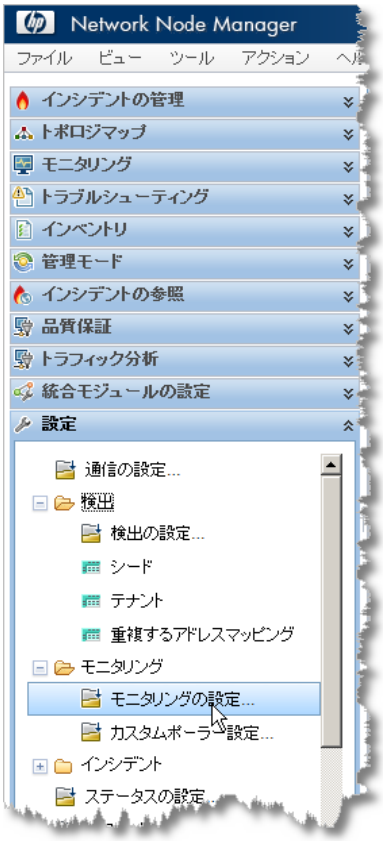
インタフェース グループへの監視の適用

作成したフィルタによって定義されたインタフェースを監視するには、このインタフェース グループに監視を適用します。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、ノード設定よりもインタフェース設定の方が優先されます。

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、**[監視の設定]** をクリックします。

図 25: モニタリングの設定

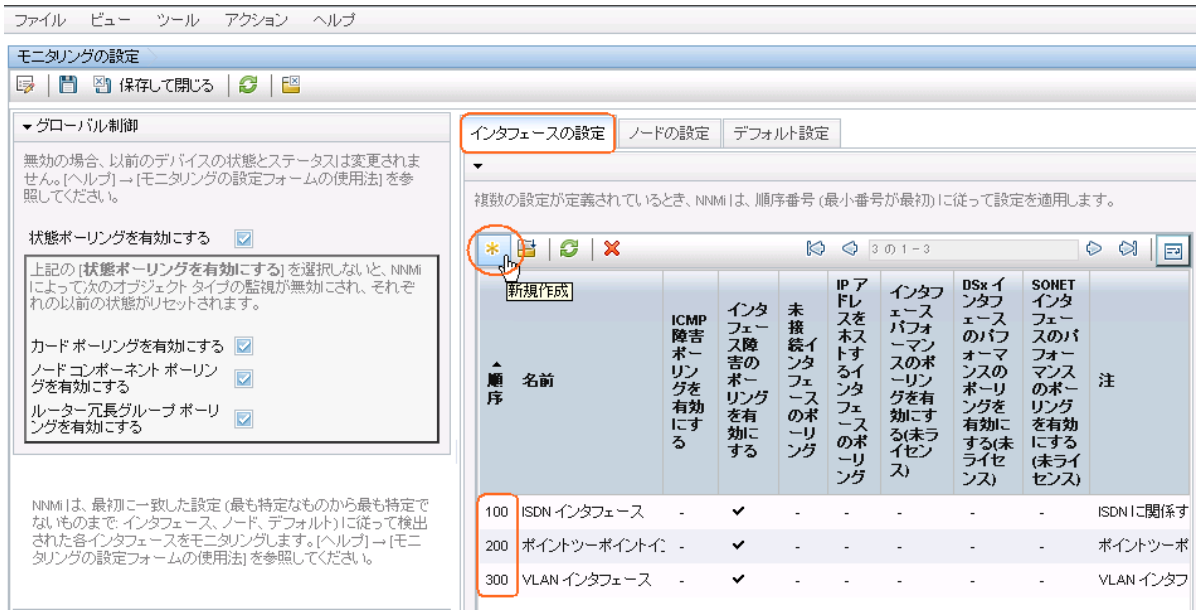


2. **[インタフェースの設定]** タブをクリックします。

ヒント: 現在の [順序] の値に注意してください。インタフェースが複数のグループに属している場合、これらによって優先度が定義されます。

この例の最も高い優先度は 100 です。

図 26: 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. 他の設定よりもこの設定の方が優先されるような **[順序]** の値を入力します。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。今後の設定を考慮した **[順序]** の値を選択することもできます。たとえば、この数値を最も高い優先度である 1 に設定すると、今後のエントリを制限できます。この例では、50 が入力されています。

5. 監視範囲を拡張します。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] 領域のすべてのチェック 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、新しく作成されたインタフェース 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。

7. **[モニタリングの設定]** フォームの上部にある **[保存して閉じる]** をクリックして変更を保存します。

図 27: インタフェースの設定: 保存して閉じる

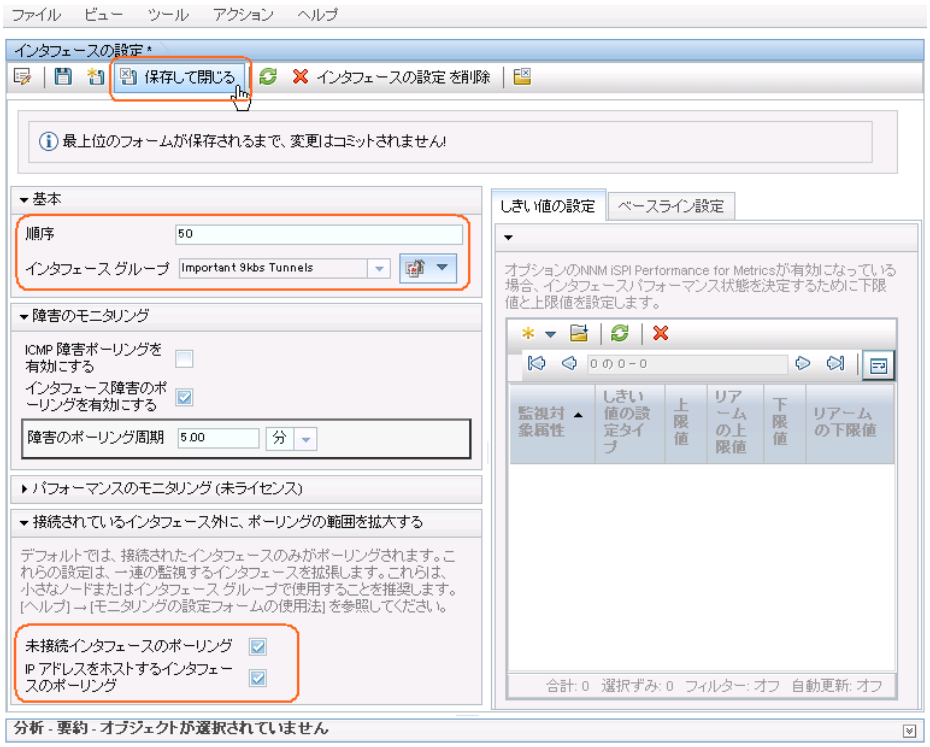
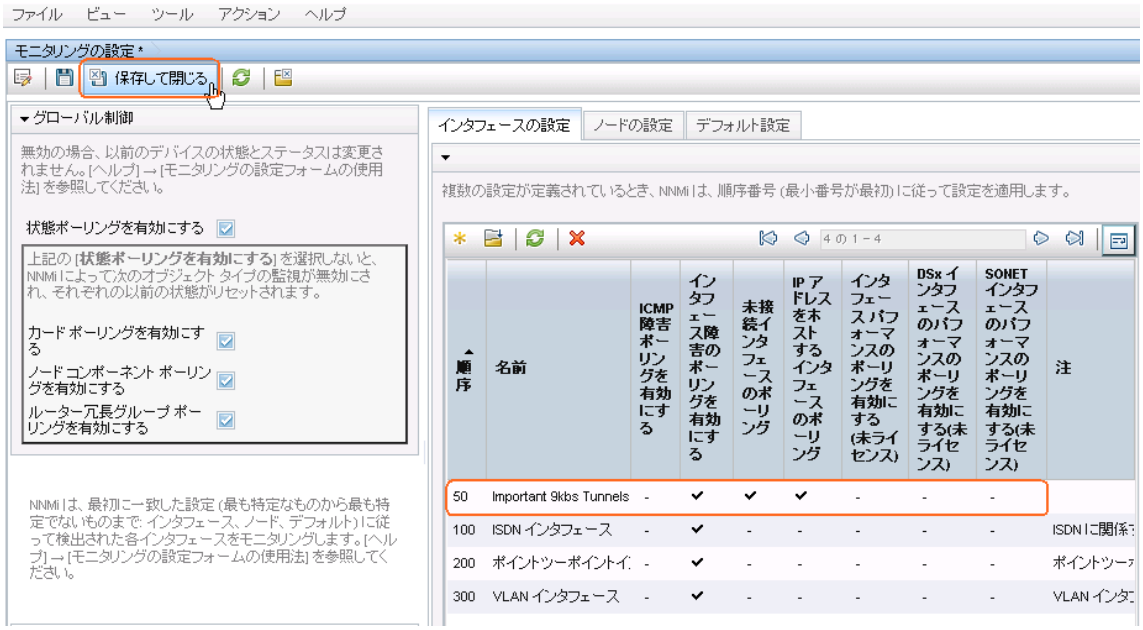


図 28: モニタリングの設定: 保存して閉じる



これで、このインタフェース グループのすべてに監視設定が適用されました。これにより、NNMi では SNMP を使用して `Important 9kbs Tunnels` フィルタに一致するインタフェースが監視されます。

監視設定のテスト

さまざまな方法で新しい監視設定をテストできます。この例では、以下の手順が使用されています。

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、**[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、新しいインタフェース グループ `Important 9kbs Tunnels` を選択します。

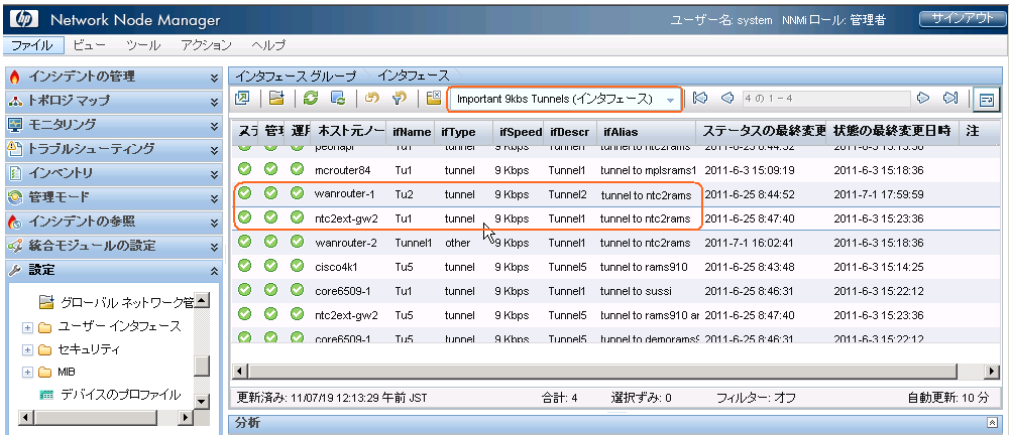
これにより、このインタフェース グループのインタフェースのみが表示されるようにテーブルがフィルタされます。

ヒント: 一部のインタフェースの [管理状態] が [未ポーリング] になっていることがあります。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。これらのすべてでステータスの取得が開始されます。

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、**[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 ポーリングを開始します。

図 29: インタフェース: Important 9kbs Tunnels フィルタ

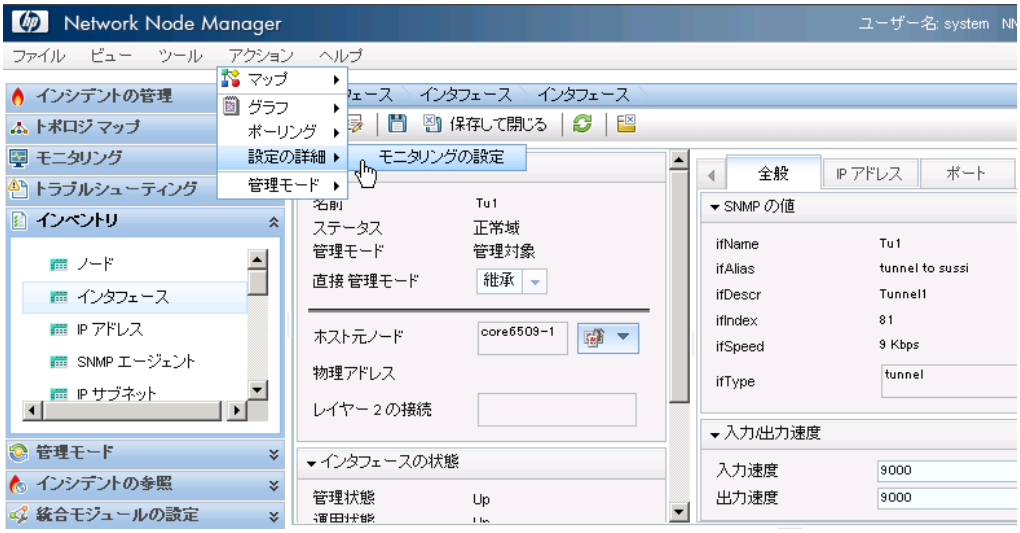


前の図で強調表示されているいずれかのインタフェースを開き、監視設定をチェックして監視設定が正常に動作していることを確認します。

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、選択したインタフェースの監視設定を表示します。

図 30: アクション: モニタリングの設定

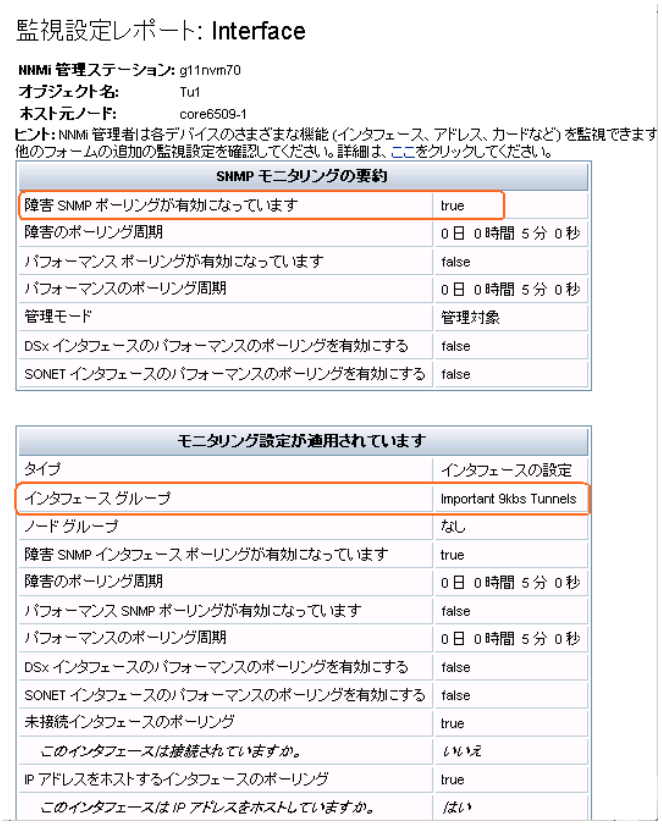


このレポートの例では、監視設定が正常に動作していることがわかります。

まず、NNMi によって `Important 9kbs Tunnels` グループの監視設定がこのインタフェースに適用されています。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 `SNMP` ポーリングが有効になっています] が true に設定されています。これは、新しい監視設定が `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 31: 監視設定レポート: インタフェース



監視設定レポート: Interface

NNMi 管理ステーション: g11nvm70
オブジェクト名: Tu1
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機能 (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監視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。

SNMP モニタリングの要約	
障害 SNMP ポーリングが有効になっています	true
障害のポーリング周期	0 日 0 時間 5 分 0 秒
パフォーマンス ポーリングが有効になっています	false
パフォーマンスのポーリング周期	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

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
ノード グループ	なし
障害 SNMP インタフェース ポーリングが有効になっています	true
障害のポーリング周期	0 日 0 時間 5 分 0 秒
パフォーマンス SNMP ポーリングが有効になっています	false
パフォーマンスのポーリング周期	0 日 0 時間 5 分 0 秒
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
未接続インタフェースのポーリング	true
このインタフェースは接続されていますか。	*いいえ*
IP アドレスをホストするインタフェースのポーリング	true
このインタフェースは IP アドレスをホストしていますか。	*はい*

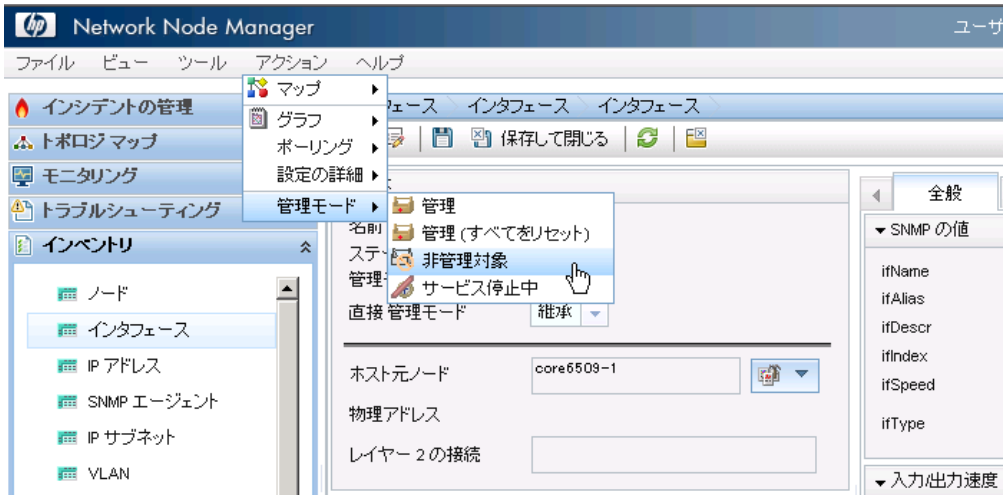
監視の除外

インタフェースまたはノードを手動で強制的に監視対象外にできます。

[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、インタフェースを管理対象外にします。

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 32: アクション: 管理モード: 非管理対象



インタフェースを強制的に監視対象外にするために NNM で使用されている方法は、現在 NNMi では提供されていません。現時点では、インタフェースを管理対象外にする方法は、*管理対象外になるようにオーバーライドすることだけです。*

NNMi で強制的にインタフェースを監視する方法については、http://h20230.www2.hp.com/selfsolve/manuals にある『Forcing an Interface to be Polled』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

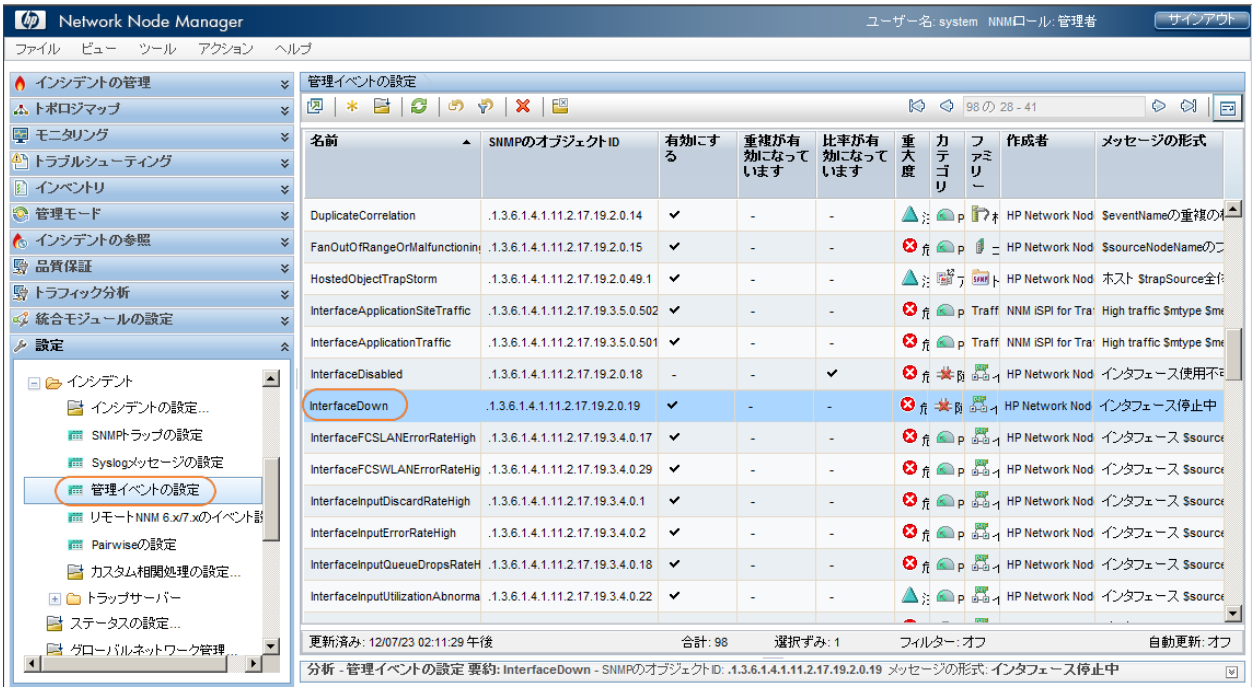
インシデントの設定

NNMi では、インシデントの特定の側面を変更できます。一部の例には、インシデントの有効化、メッセージの形式設定、重複削除の有効化、レート相関処理の有効化が含まれています。

この例では、インタフェースのエイリアスがメッセージに含まれるように `InterfaceDown` (インタフェース停止中) インシデントを改善する方法が説明されています。

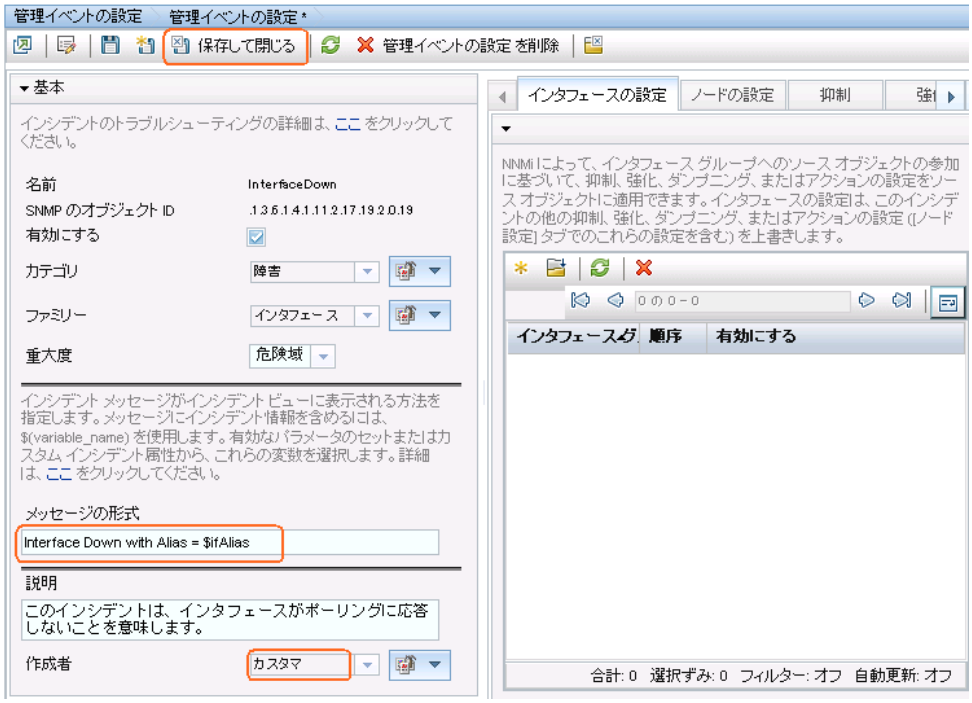
1. ワークスペースのナビゲーション パネルで **[設定]** ワークスペースを選択し、**[インシデント] > [管理イベントの設定]** をクリックします。
2. `InterfaceDown` インシデント設定をダブルクリックします。

図 33: 設定: 管理イベントの設定



3. 続行する前に NNMi ヘルプの *「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」* を参照して、メッセージ形式に追加できる引数を確認してください。この例では、引数 `$ifAlias` が以下の例のようにインシデント メッセージに追加されています。

図 34: 管理イベントの設定: メッセージの形式

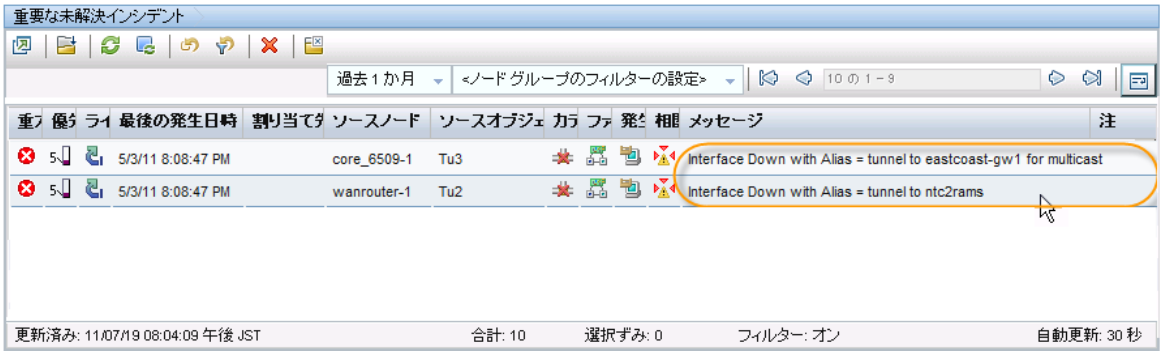


4. **[クイック検索]** を使用して **[作成者]** を **[カスタマ]** に変更します。
5. 最後に、このフォームと **[管理イベントの設定]** フォームで **[保存して閉じる]** をクリックします。

以下の **[重要な未解決インシデント]** ビューの例のように、すべての `InterfaceDown` インシデントに `$ifAlias` パラメータが表示されます。

注: インタフェースにエイリアスがない場合、NNMi ではエイリアスの代わりに `null` が表示されます。

図 35: 重要な未解決インシデント



トラップの設定

ヒント: NNMi でのトラップの使用の詳細については、http://h20230.www2.hp.com/selfsolve/manuals にある『Step- by-Step Guide to Incident Management』を参照してください。

注: トラップを NNMi インシデント ブラウザで受信するには、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。

この例の場合、3 つの MIB をロードして依存関係を満たす必要があります。まず、`ruggedcom.mib` ファイル、`rcsysinfo.mib` ファイルの順にロードします。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` 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` 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。

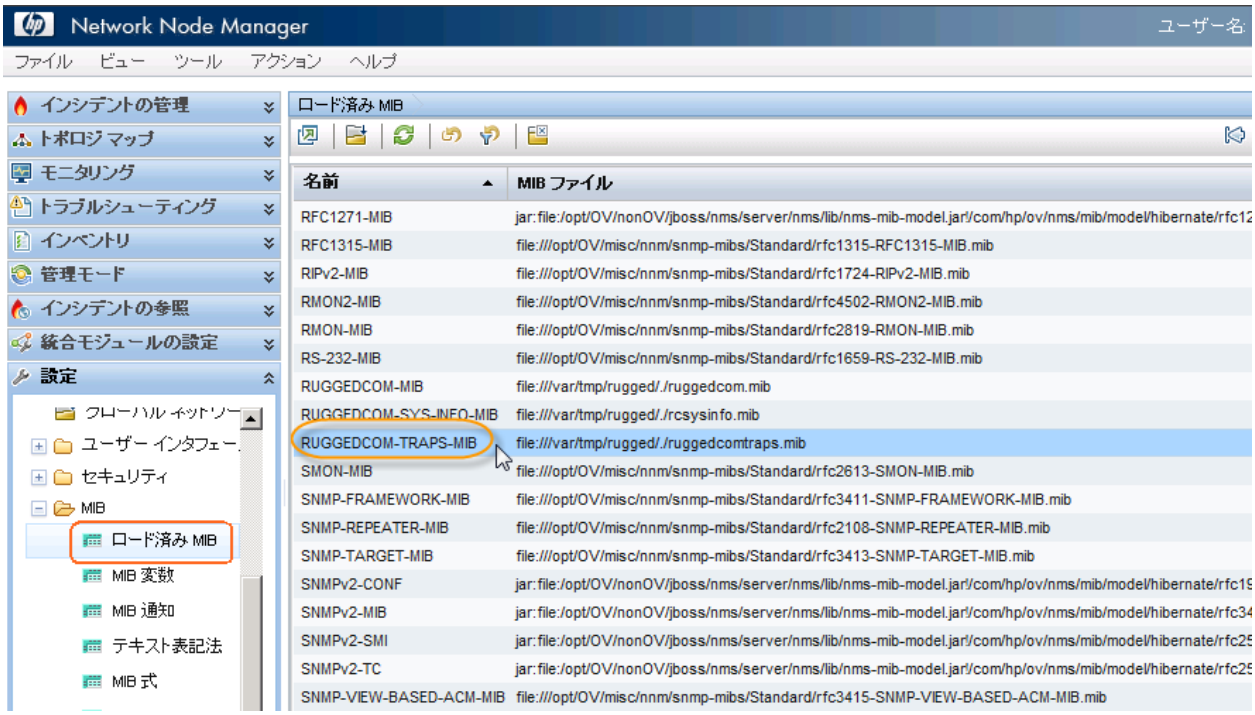
次に、MIB がロードされていることを確認します。

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、**[MIB] > [ロード済み MIB]** をクリックします。

   `Rugged Com` MIB が新たにロードされています。

2. トラップ モジュール (`RUGGEDCOM-TRAPS-MIB`) に注意してください。 次のコマンドでこれが必要になります。

図 36: 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。

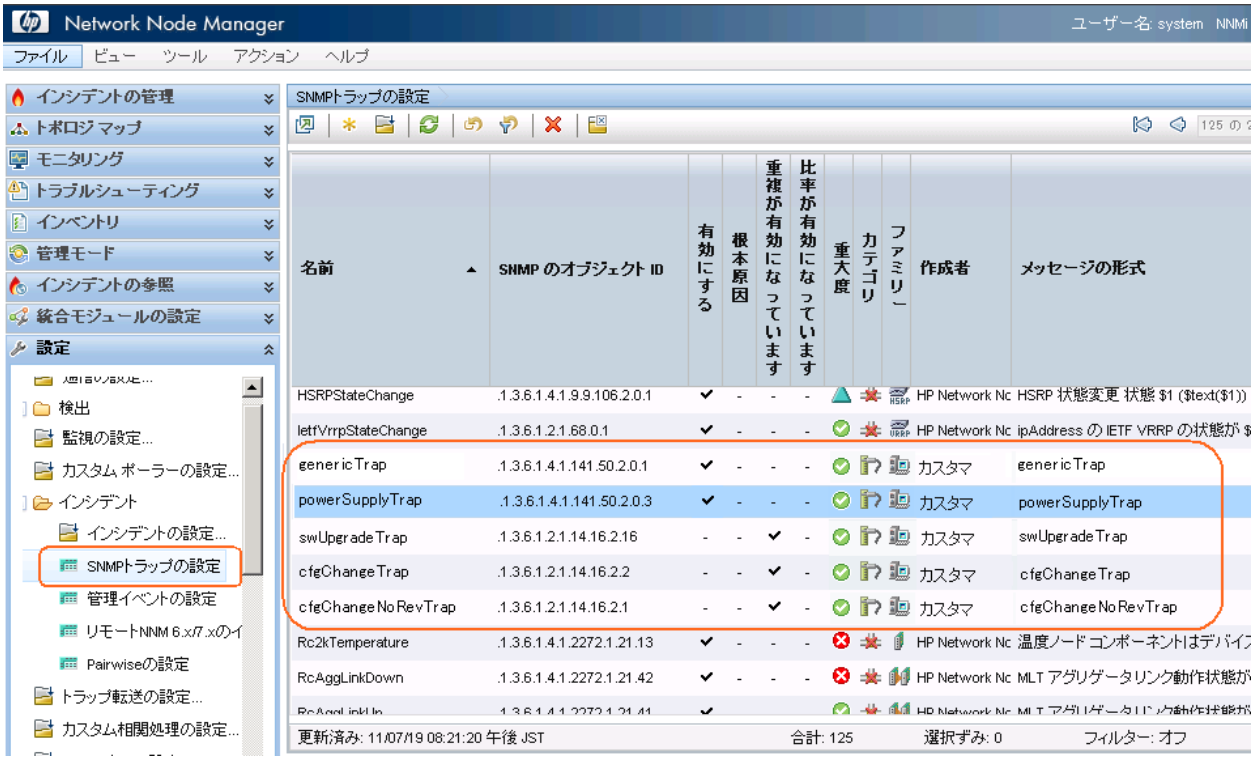
```
MIB モジュールからの SNMP トラップがロードされました: RUGGEDCOM-TRAPS-MIB。
トラップ数: 5。
次のトラップがインシデントの設定に追加されました:
cfgChangeNoRevTrap - .1.3.6.1.4.1.15004.5.5
cfgChangeTrap - .1.3.6.1.4.1.15004.5.4
powerSupplyTrap - .1.3.6.1.4.1.15004.5.2
swUpgradeTrap - .1.3.6.1.4.1.15004.5.3
genericTrap - .1.3.6.1.4.1.15004.5.1
```

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、**[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。

すべてのトラップが *有効化された状態*でロードされています。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 37: 設定: SNMP トラップの設定



自動アクションの設定

インシデントの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 用の Java インタープリターが使用されるため、これらのスクリプトは `Jython` として参照されます。

NNMi では、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ぞれぞれアクションを実行するように NNMi を設定できます。これを行うには、`InterfaceDown` インシデントで両方のアクションを設定しますが、一方のアクションに関連付ける [ライフサイクル状態] を [登録済み] に設定し、もう一方のアクションに関連付ける [ライフサイクル状態] を [解決済み] に設定します。通常、NNMi では、関連付けられている動作中インシデントは生成されません。

注: NNMi でインシデントが生成されると、[登録済み] 状態がインシデントに割り当てられます。

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から、このディレクトリにアクセスするには、`root` または `administrator` である必要があります。

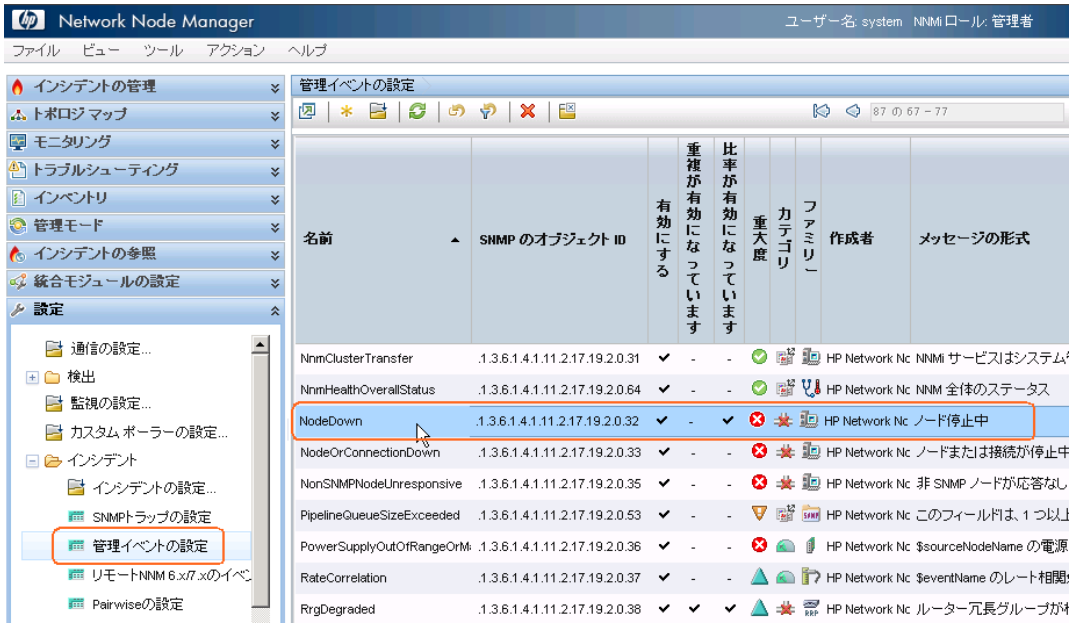
   この例では、`actions` ディレクトリが以下の場所にあることが想定されています。

   - *Windows*: `\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared\nnm\actions`
   - *UNIX*: `/var/opt/OV/shared/nnm/actions`

actions ディレクトリの場所は、NNMi をどのようにインストールしたかによって異なります。この例では、スクリプトの名前は writelog.ovpl になっています。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。

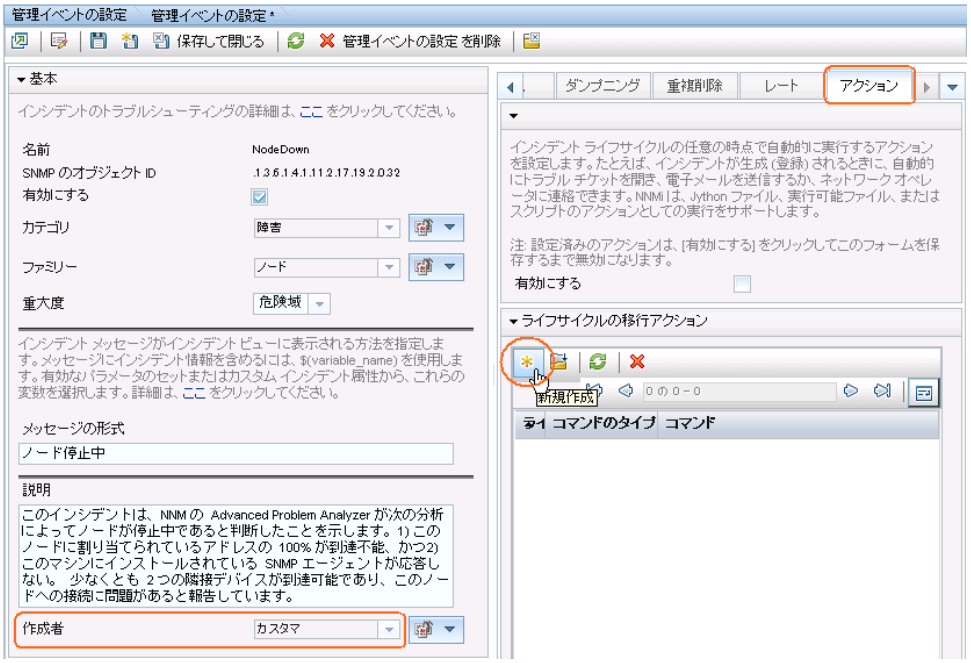
2. このスクリプトをこのインシデントのアクションに関連付けるには、以下の手順を実行します。
   a. ワークスペースのナビゲーション パネルで **[設定]** ワークスペースを選択します。
   b. **[インシデント] > [管理イベントの設定]** をクリックします。
   c. NodeDown インシデントをダブルクリックします。

図 38: 管理イベントの設定: NodeDown インシデント



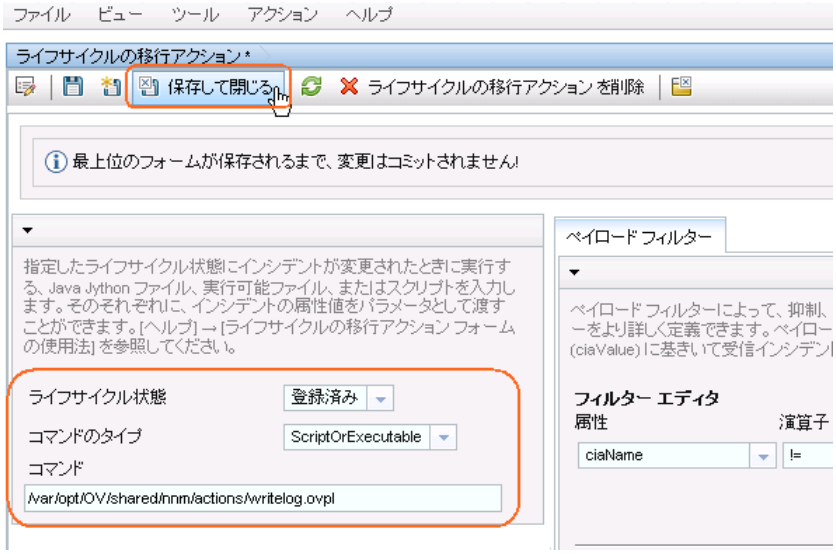
3. **[作成者]** を **[カスタマ]** に変更し、**[アクション]** タブをクリックして ✱ アイコンをクリックします。

図 39: 管理イベントの設定: [アクション] タブ



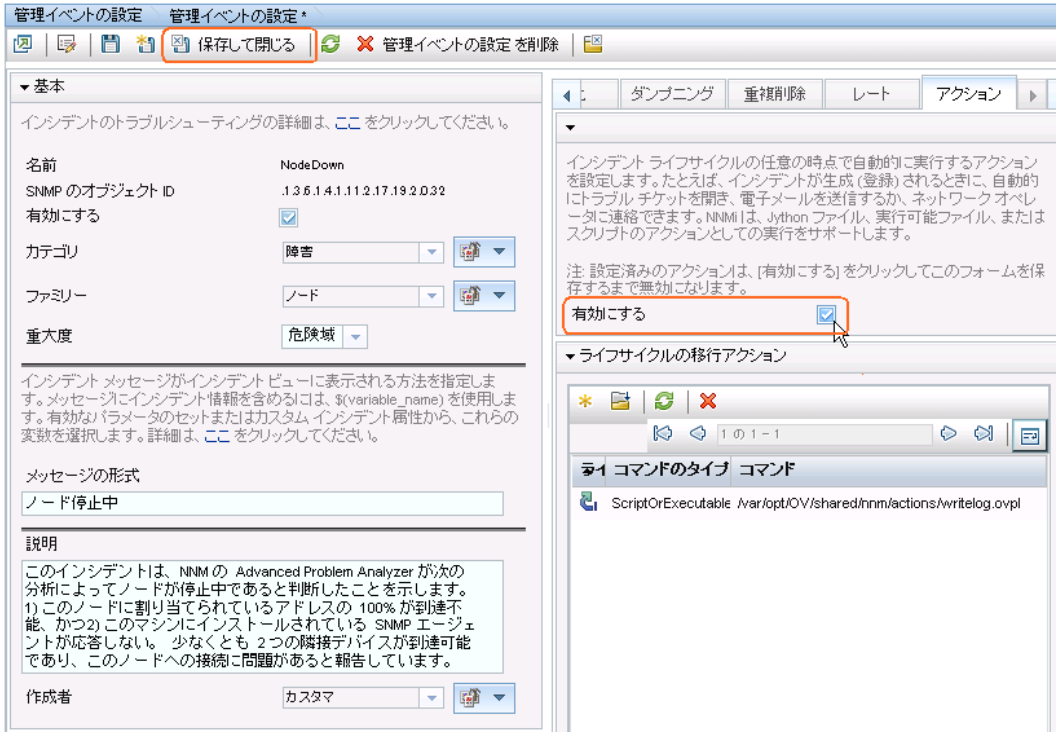
4. 適切な **[ライフサイクル状態]** (この例では [登録済み]) を選択します。
5. **[コマンドのタイプ]** を `ScriptOrExecutable` に設定します。
6. 実行可能ファイルへの完全パスを含めたコマンド名を入力し、**[保存して閉じる]** をクリックします。

図 40: ライフサイクルの移行アクション



7. **[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。

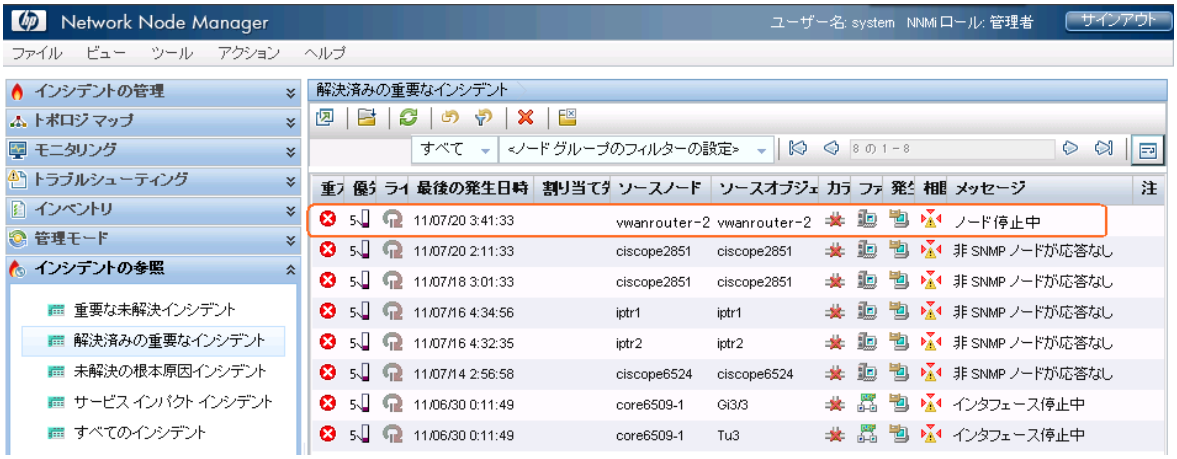
図 41: 管理イベントの設定: [アクション] タブ: アクションの有効化



次に、アクションをテストする必要があります。これを行う最も簡単な方法は、以前に発生した 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、**[解決済みの重要なインシデント]** をクリックします。

図 42: 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 によって解決済みにされた NodeDown インシデントを開きます。

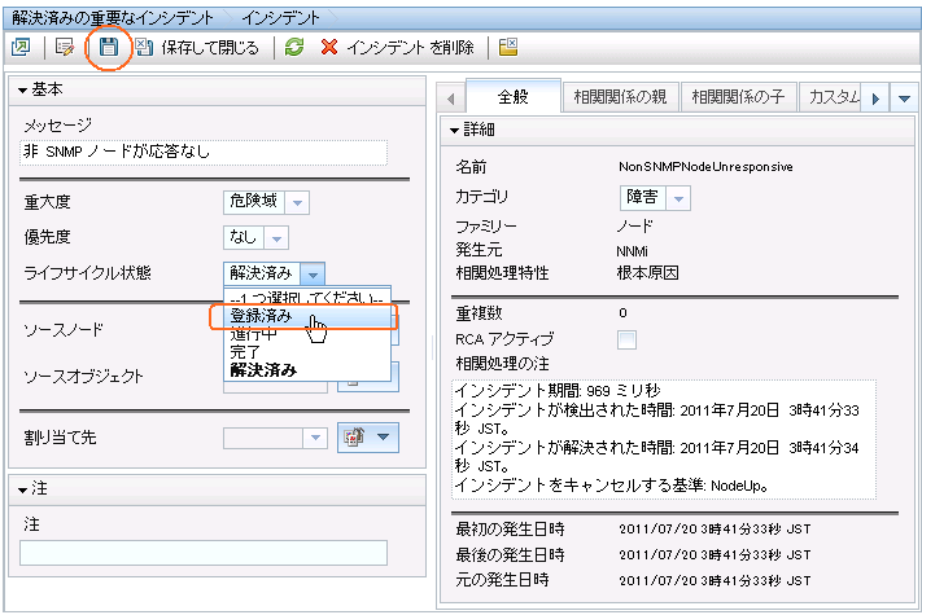
この例の解決済みは、インタフェースが動作中に戻ったことを意味します。障害がなくなると NNMi によって自動的にインシデントが解決済みにされます (**[ライフサイクル状態]** を [登録済み] に設定すると、インシデントをもう一度開くことができます。この操作を実行すると、アクションを実行するときにインシデントを初めて開いたように NNMi が動作します)。

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 (**[ライフサイクル状態]** の変更を保存) した後でアクションが実行されます。**[ライフサイクル状態]** を変更してもその変更を保存しないと NNMi でアクションは実行されません。

4. **[ライフサイクル状態]** を保存するたびに **[保存]** をクリックします。

図 43: [インシデント] フォーム: [登録済み] の [ライフサイクル状態]



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。テストが完了したら **[ライフサイクル状態]** を [解決済み] に設定してインシデントを保存し、元の状態に戻します。

NNMi コンソールの設定

ノード グループの設定

診断を強化するには、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、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』の *「ノード グループの実際的な使用例」* を参照してください。

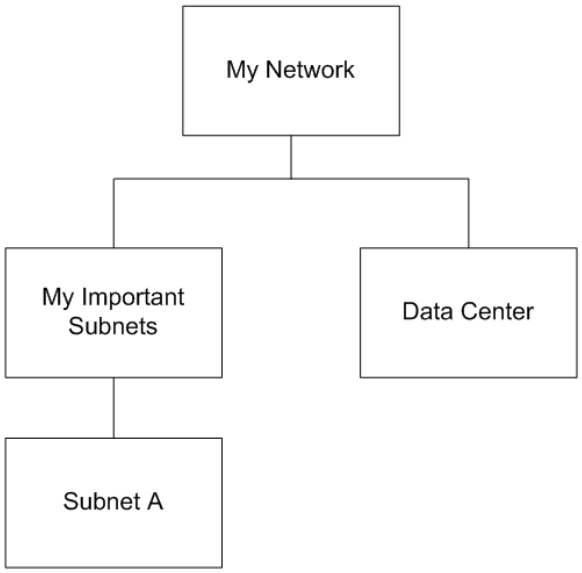
この例では、いくつかの異なるサブネットのノード グループが作成されています。

ヒント: これらのノード グループで、ノードのアドレスではなく管理アドレスを参照するようにします。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 44: 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

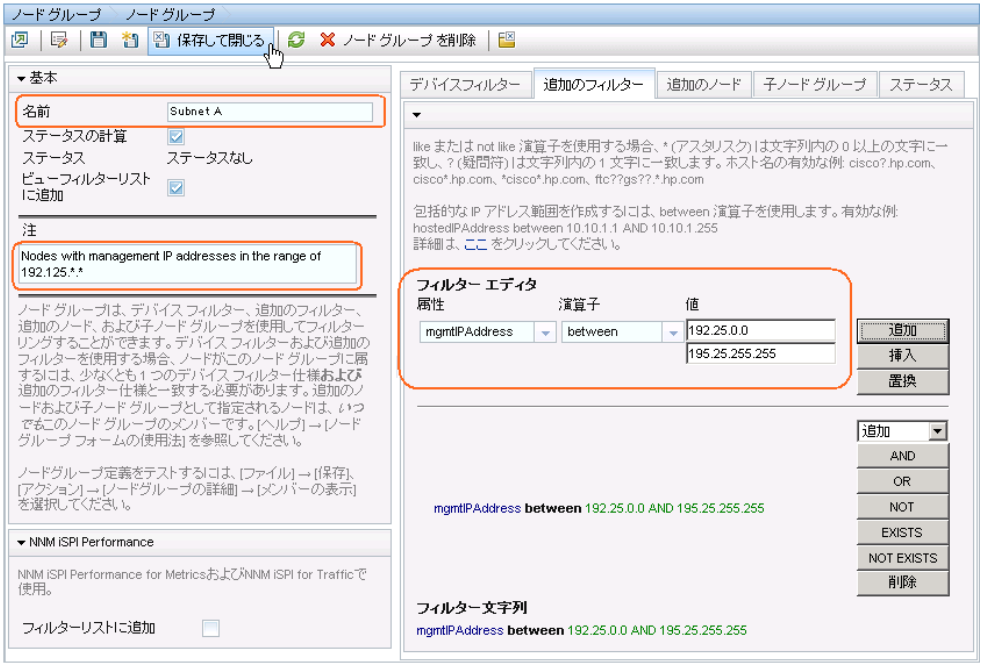
以下の項に注意してください。

- Subnet A ノード グループと Data Center ノード グループのみにノードが設定されています。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. 以下の例のように Subnet A ノード グループを作成します。

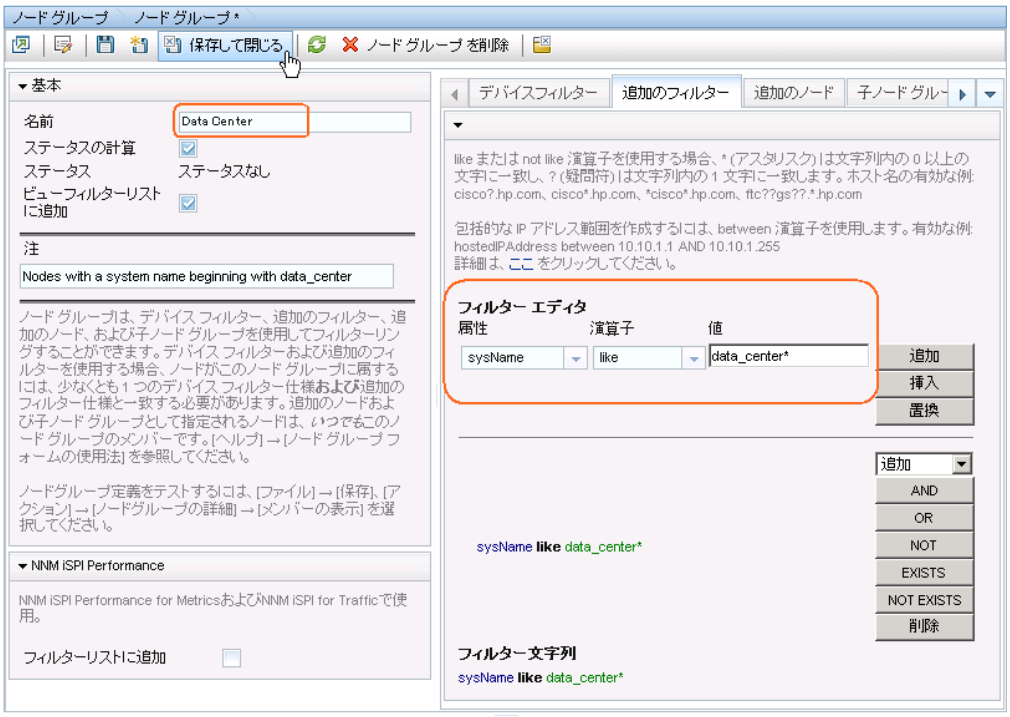
ヒント: IP アドレス範囲の独特の表現に注意してください。

図 45: 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。

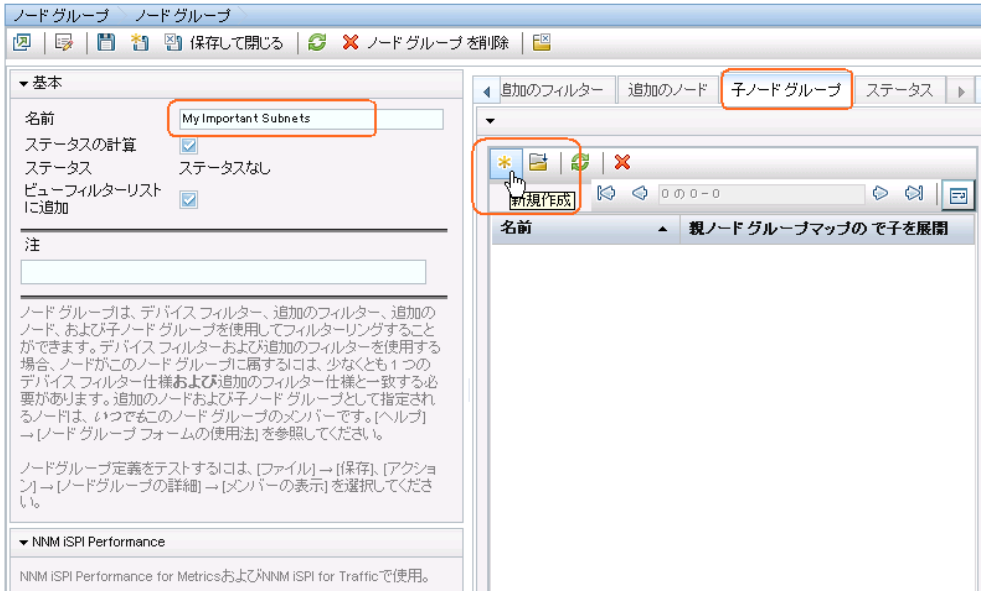
図 46: ノード グループ: [追加のフィルター] タブ



次に、My Important Subnets ノード グループを作成します。

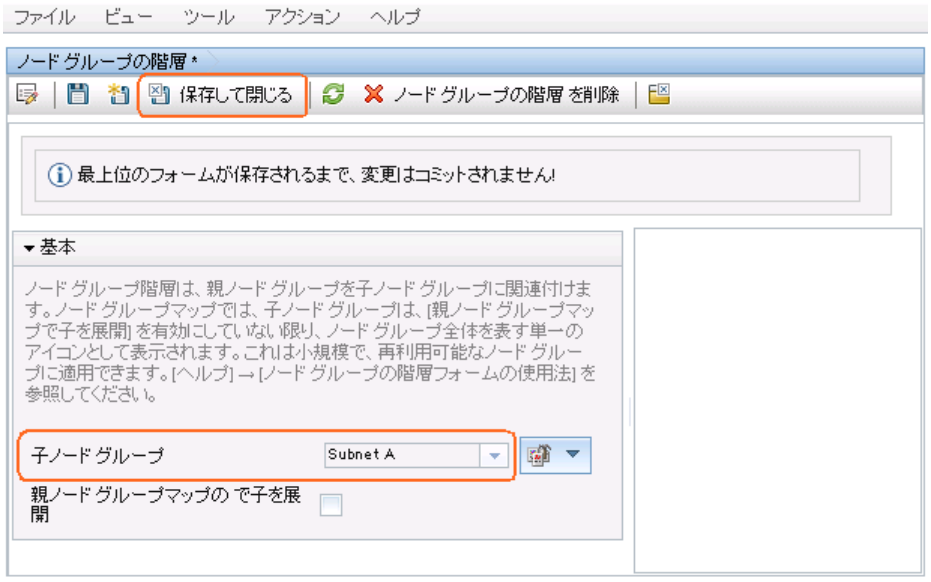
1. [ノード グループ] フォームで、* アイコンをクリックします。
2. **[名前]** テキスト ボックスに **`My Important Subnets`** と入力します。
3. **[子ノード グループ]** タブをクリックし、* アイコンをクリックします。

図 47: ノード グループ: [子ノード グループ] タブ



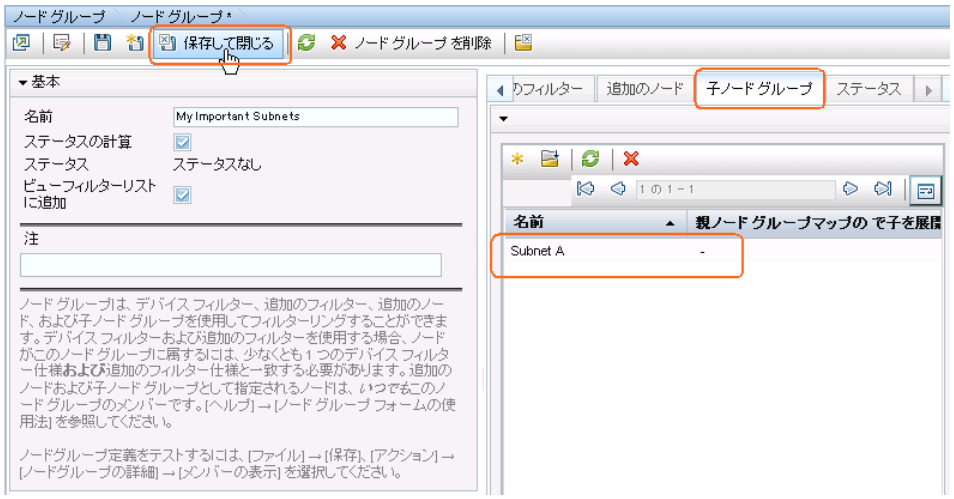
4.  をクリックして、**[クイック検索]** をクリックします。 **Subnet A** 子ノード グループをクリックし、**[OK]** をクリックします。

図 48: ノード グループ階層: 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。My Important Subnets ノード グループに子ノード グループ Subnet A が作成されました。

図 49: [子ノード グループ] タブ: 保存して閉じる



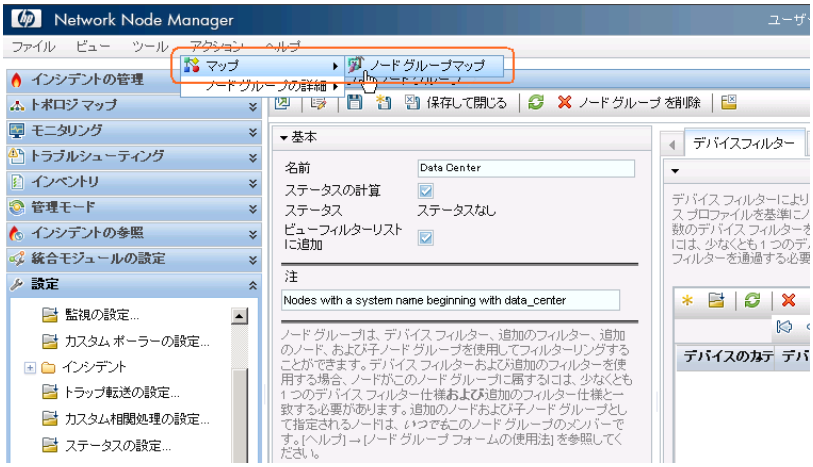
最後に、Data Center および My Important Subnets *子ノード グループを含む* My Networkノード グループを作成します。

ヒント: 各ノード グループを保存したら、必ず **[アクション] > [ノード グループの詳細] > [メンバーの表示]** をクリックしてメンバーシップをテストしてください。

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。

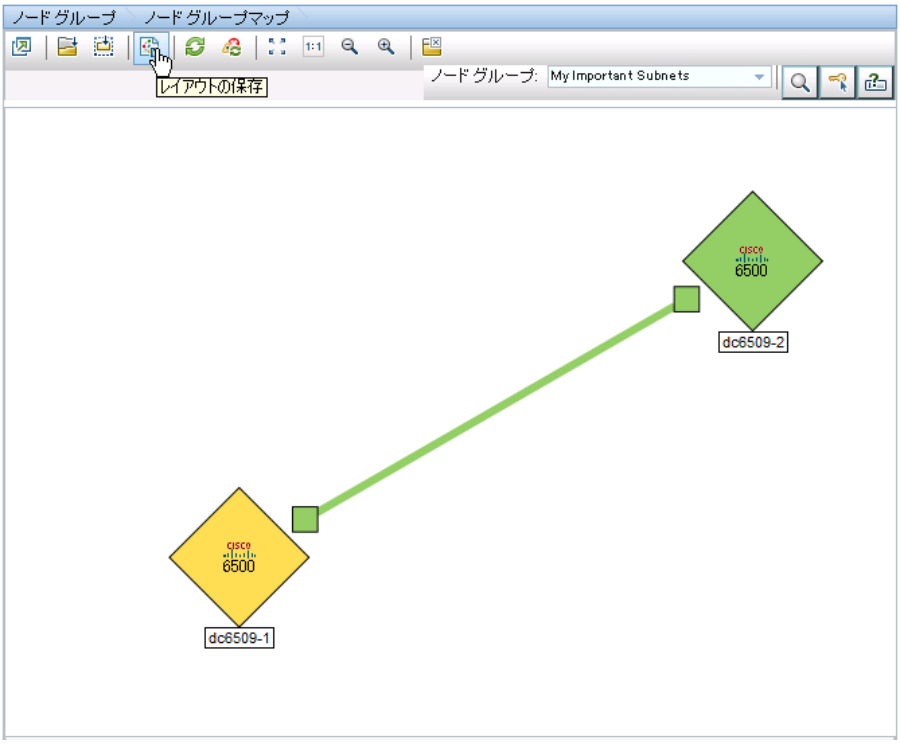
1. **[アクション] > [マップ] > [ノード グループ マップ]** をクリックしてマップを開きます。

図 50: アクション: マップ: [ノード グループ マップ] の選択



2. **[レイアウトの保存]** をクリックします。

図 51: ノード グループ マップ: ノード グループ マップのレイアウトの保存



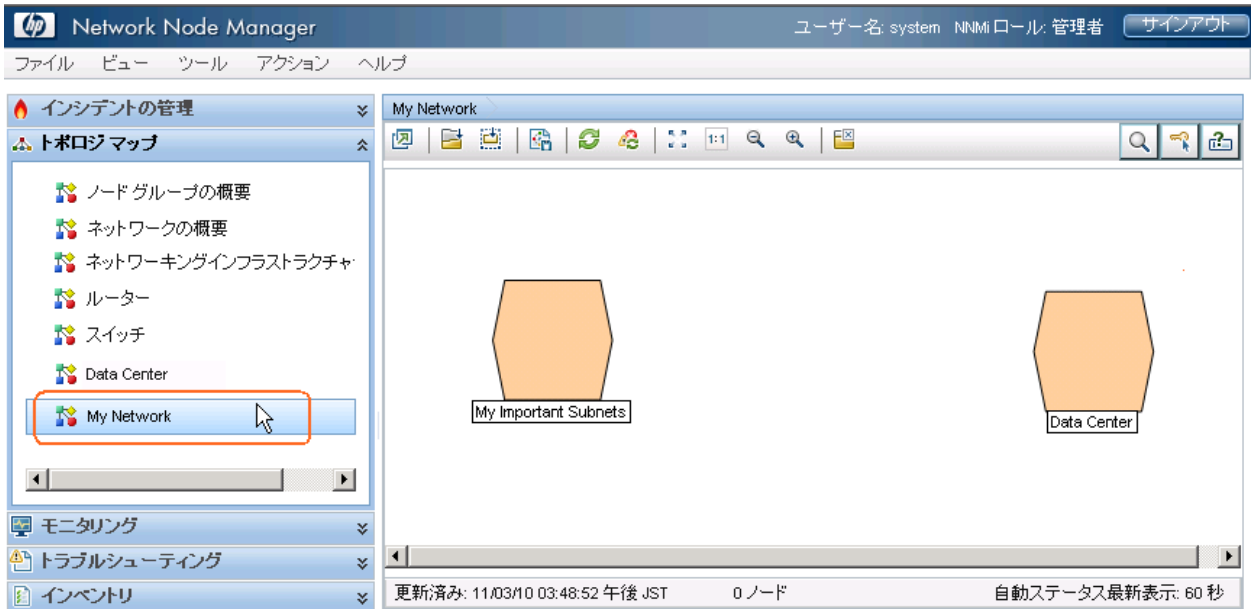
変更を保存すると、ノード グループ マップが作成されたことを通知するメッセージが NNMi に表示されます。

階層全体でこれと同じ手順を繰り返します。ノード グループにステータスがすべて伝播されるのに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

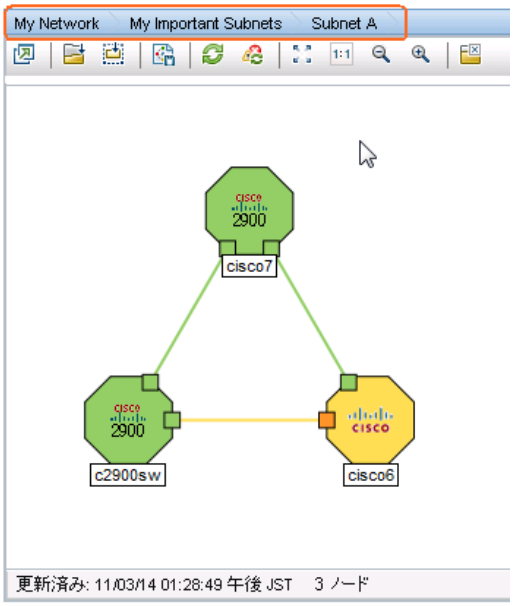
これでマップ階層内を移動できるようになりました。ワークスペースのナビゲーション パネルで **[トポロジ マップ]** ワークスペースを選択します。新しく作成したノード グループ マップが表示されていない場合、ブラウザをリフレッシュするか、NNMi をサインアウトしてからもう一度サインインしてください。

図 52: My Network トポロジ マップ



上部の階層リンクは、階層内のどこにいるのかを示しています。

図 53: 階層リンク



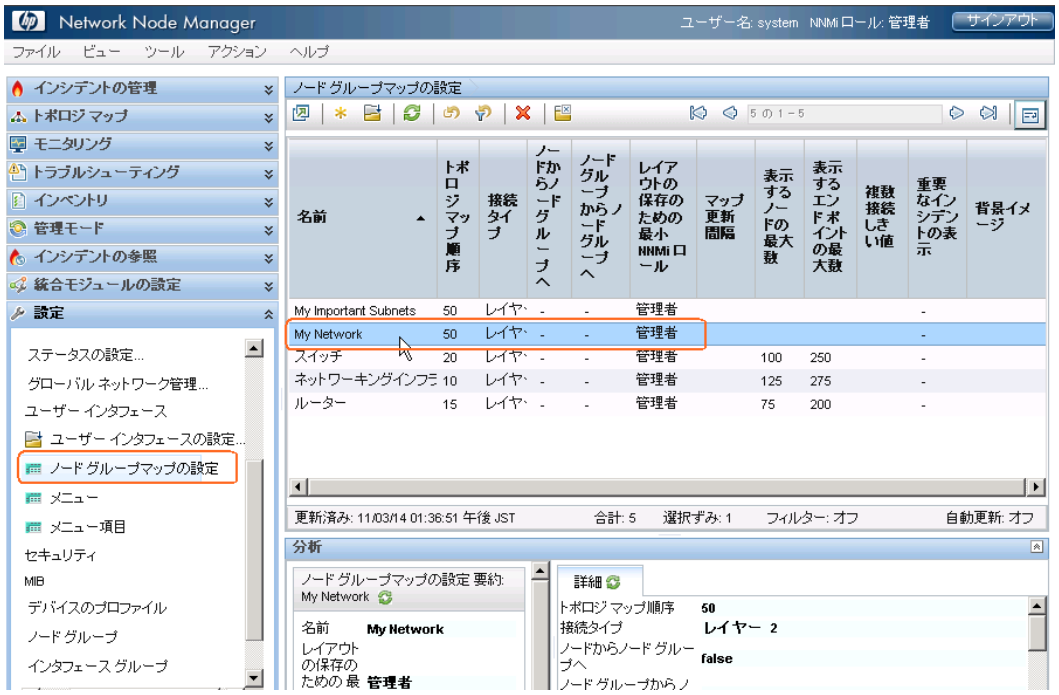
[ノード グループ マップの設定] オプションでは、ノード グループを配置したり、背景グラフィクスを追加したり、接続オプションを変更したりできます。

マップに背景グラフィクスを配置するには、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 **[設定]** ワークスペースを選択し、**[ユーザー インタフェース]** フォルダを展開します。次に、**[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] の値に注意してください。 現在使用されている数値で最も低いのは 10 です。

図 54: ノード グループ マップの設定

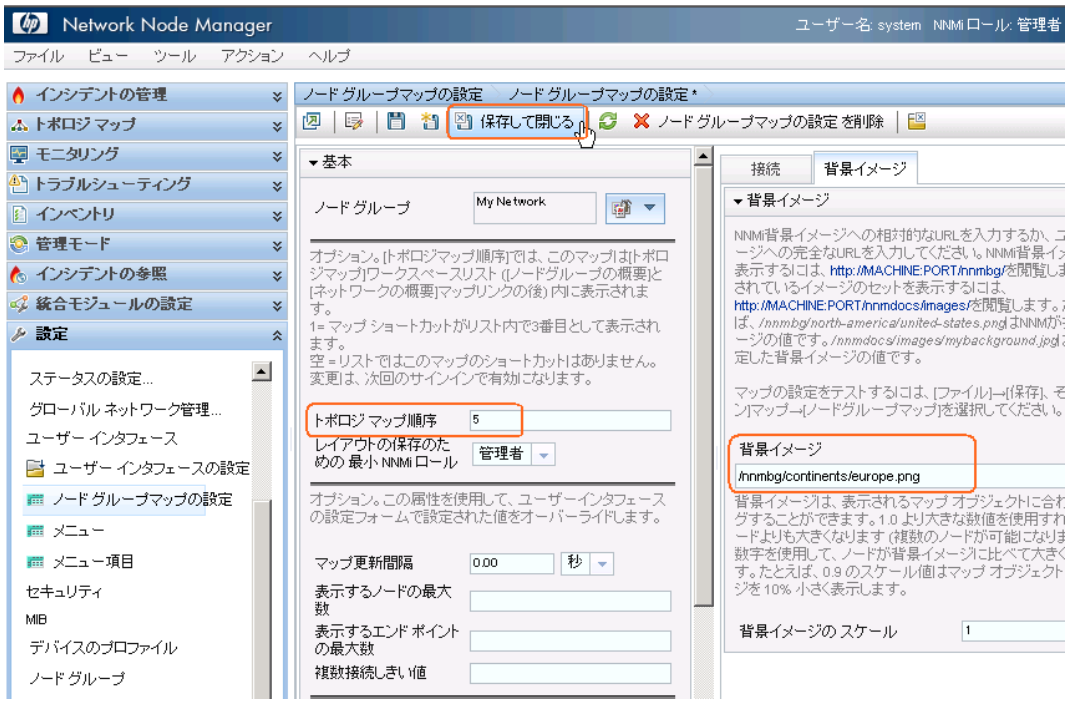


2. My Network をダブルクリックします。
3. 背景イメージを追加します。

ヒント: パスの前に `http://<machine name>` を含めないで `/nnmbg/continents/europe.png` などのローカル パスを使用します。これにより、アプリケーション フェイルオーバー機能が正常に動作します。

4. **[トポロジ マップ順序]** の値が前の例で使用されていた最小値よりも低くなるように、この値を 5 に変更します。
5. **[保存して閉じる]** をクリックします。

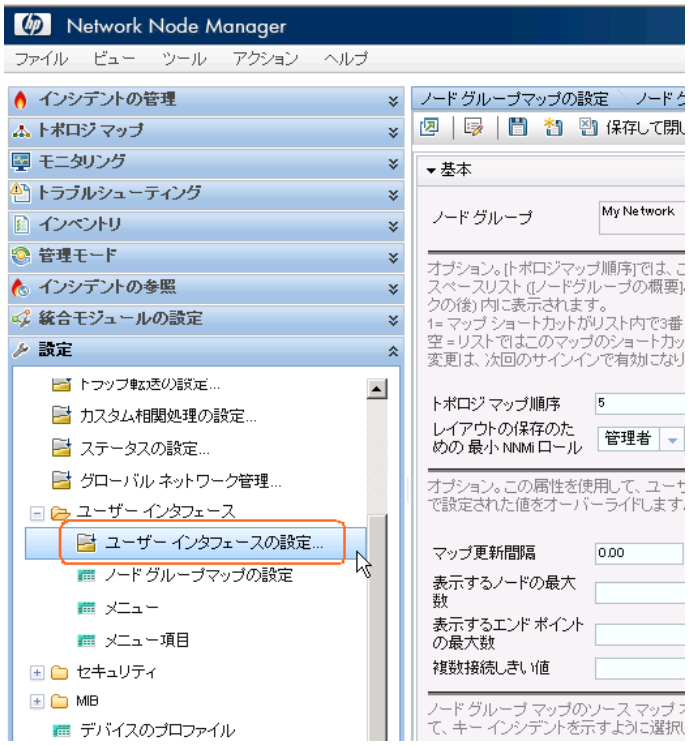
図 55: ノード グループ マップの設定の保存



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

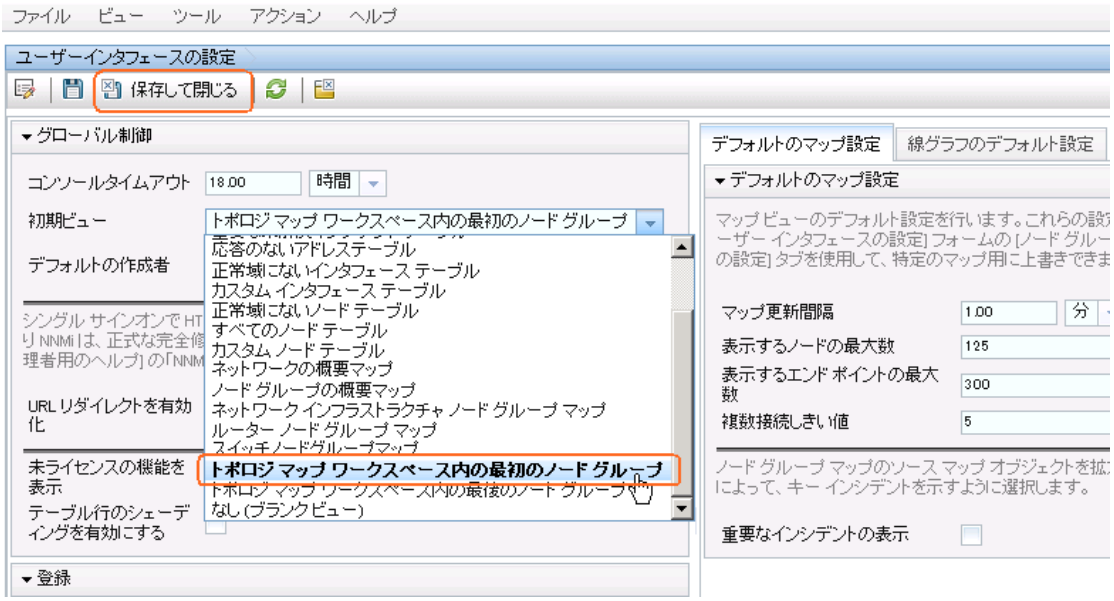
6. **[ユーザー インタフェースの設定]** をクリックします。

図 56: 設定: ユーザー インタフェースの設定



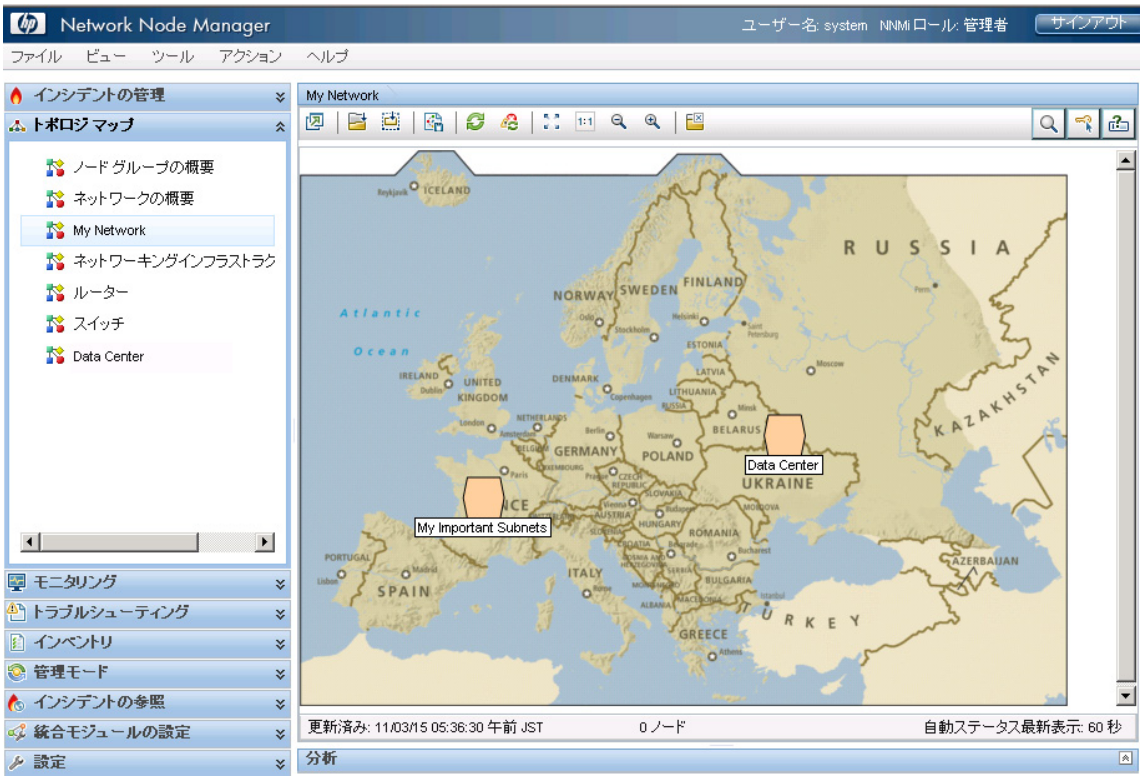
7. **[初期ビュー]** の選択を **[トポロジ マップ ワークスペース内の最初のノード グループ]** に変更します。**[トポロジ マップ順序]** 属性の値を 5 に設定してあるため、これは My Network マップになります。
8. **[保存して閉じる]** をクリックします。

図 57: ユーザー インタフェースの設定の保存



9. NNMi をサインアウトしてからもう一度サインインすると、初期ビューが My Network マップになっています。

図 58: My Network マップ



NNMi の保守

NNMi データのバックアップおよびリストア

NNMi には、データの保護に役立つバックアップ スクリプトおよびリストア 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。このスクリプトは*オンライン*または*オフライン*で使用します。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 環境をリストアするために必要なすべての要素が含まれています。

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
```

前のコマンドで `nnm-bak-20110504145143.tar` のような名前のファイル名が作成されます。

関連付けられたリストア スクリプトは `nnmrestore.ovpl` です。このコマンドでは、`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になります。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。

以下に、`nnmrestore.ovpl` スクリプトの使用例を示します。

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

ソース ディレクトリには、バックアップのすべてのファイルまたは 1 つの tar ファイルが含ま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に tar ファイルが抽出されます。リストアが完了するとスクリプトによって一時フォルダが削除されます。

注意: NNMi の複数のパッチ バージョンにまたがってバックアップをリストアしたり、NNMi の以前のパッチ レベルからバックアップをリストア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 コードにリストアしないでください。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されているパッチのバージョンを追跡します。たとえば、バックアップ ディレクトリに patch4 という名前を付けます。

NNMi 設定のエクスポートとインポート

NNMi の設定は最も重要なタスクの 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 に含まれている nnmconfigexport.ovpl および nnmconfigimport.ovpl スクリプトを使用することも検討してください。これらのスクリプトでは、NNMi 設定のリストアを柔軟に行うことができます。これらのスクリプトを使用すると、以下のことが可能になります。

- 現在の NNMi 設定のスナップショットの作成
- 設定の細分化
- 最新のスナップショットに戻す必要がある場合、1 つの NNMi 設定をリストアするだけで済む

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、インシデントなど (他にも多数あります) の設定領域を指定します。また、NNMi にはすべての設定情報をエクスポートする all 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 UNIX のマンページを参照してください。

以下に、nnmconfigimport.ovpl スクリプトの使用例を示します。

```
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。

/var/tmp/origconfig/incident.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 スクリプトでは、ファイルに日時スタンプは生成されません。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。

設定をリストアするには、nnmconfigimport.ovpl スクリプトを使用します。

ヒント: 設定領域はファイルの内容でわかるため指定する必要はありません。

以下に、nnmconfigimport.ovpl スクリプトの使用例を示します。

```
nnmconfigimport.ovpl -f /tmp/nodegroup.xml
```

nnmbackup.ovpl および nnmbackupembdb.ovpl スクリプトと同様に、これらのスクリプトを複数のパッチ バージョンにまたがって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 スクリプトでは、形式が正しければ現在の設定がオーバーライドされます。

注: NNMi では、他の NNMi 管理サーバーの構成をインポートすることはできません。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。サーバー間で転送できるのは、完全バックアップ (nnmbackup.ovpl) だけです。

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 データベースのトラップを定期的にトリムします。必要に応じてこれらのトラップをアーカイブできます。

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

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

この使用例では、1 週間以上前のトラップがトリムされます。 この使用法では、トラップはアーカイブされません。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 UNIX のマンページを参照してください。

ヒント: cron ジョブに nnmtrimincidents.ovpl を使用して、不要な古いトラップ インシデントを定期的に消去します。

注: NNMi データベースの制限 (100,000 トラップ) に達すると、最終的にトラップの保存を停止して NNMi データベースのトラップをトリムするように NNMi から求められます。

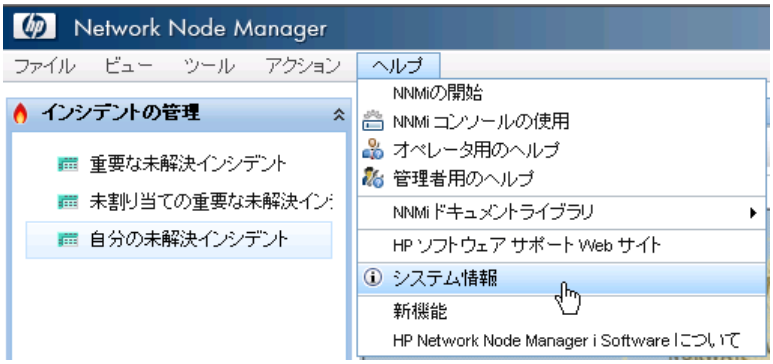
この NNMi データベースのリファレンスは、トラップ データストアとは異なります。詳細については、http://h20230.www2.hp.com/selfsolve/manuals にある『Step- by-Step Guide to Incident Management』を参照してください。

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。

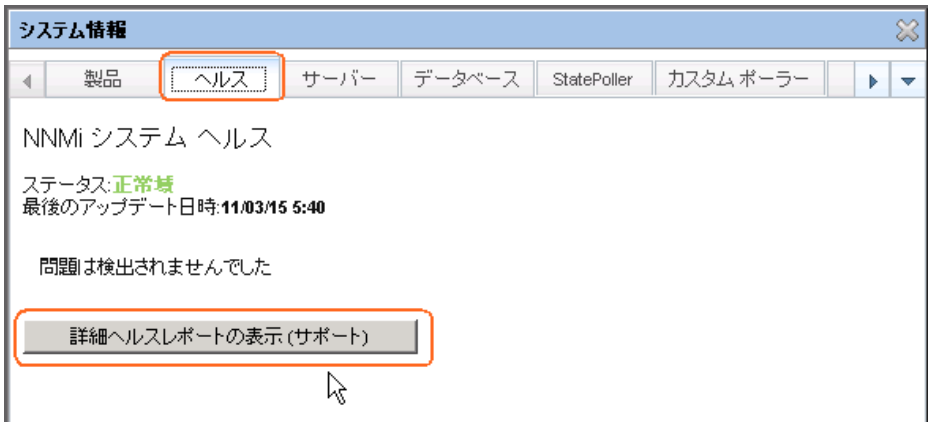
NNMi コンソールで **[ヘルプ] > [システム情報]** をクリックし、いくつかの重要な情報を一覧表示します。

図 59: 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 60: 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。ノードに現在のステータスが設定されている理由を理解するために **[結果]** タブをクリックしてデータを確認します。
- **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

このセクションには、3 つの使用シナリオが記載されています。これらのシナリオでは、NNMi のみを使用できることが想定されています。

例外管理

NNMi では、ネットワーク障害に関連する根本原因の問題が重要なインシデントとして特定されます。

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。

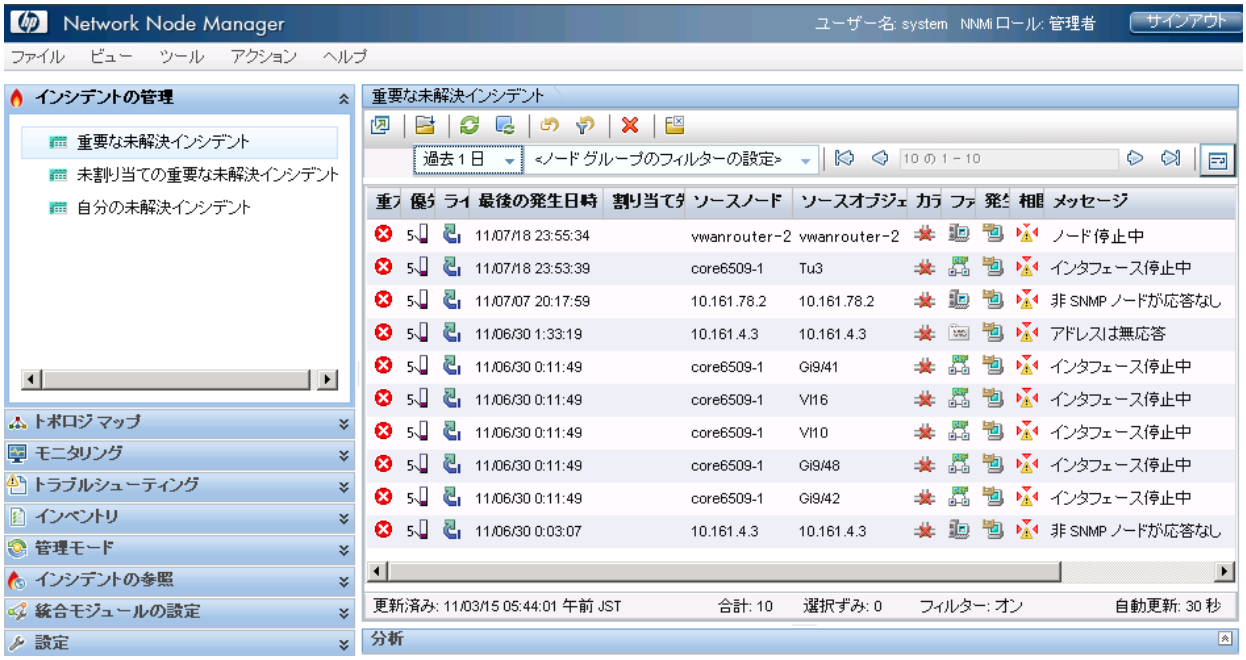
1. ワークスペースのナビゲーション パネルで **[インシデントの参照]** ワークスペースを選択します。
2. **[重要な未解決インシデント]** をクリックします。

NNMi には、ネットワークの重要な未解決インシデントがすべて表示されます。このリストは 30 秒ごとに更新されます。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 では、[重要な未解決インシデント] ビューが時間でフィルタされます。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、過去 1 日に発生したすべての重要な未解決インシデントが表示されています。この例の場合、過去 24 時間に 1 つのノードが停止しています。

図 61: 重要な未解決インシデント



[重要な未解決インシデント] ビューを監視することで、ネットワークの問題の正確な原因を特定し、解決に向けて作業を開始できます。インシデント ビューには、これらの *例外* (停止) が表示されるため、これは *例外管理* になります。

*例外管理*アプローチには、以下のメリットがあります。

- 問題の根本原因をすばやく確認できます。
- 問題のソースを *ソース オブジェクト* (インタフェース、アドレス、ノードなど) として簡単に識別できます。
- 重要なインシデント を NNMi から他の製品 (HP Operations Manager (HP OM) など) に転送できます。

*例外管理*アプローチを使用する場合、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、停止しているノードが他の多くのノードへの接続に影響している可能性があります。停止範囲を把握できるように **[トポロジ マップ]** ビューを確認します (詳細については、以下の「*マップベース管理*」セクションを参照してください)。
- すべてのノード停止中インシデントの重要性が同じというわけではありません。追加のツール (**[トポロジ マップ]** ビューなど) やノード グループ名を使用して、これらのインシデントに優先順位を付けます (詳細については、以下の「*マップベース管理*」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。

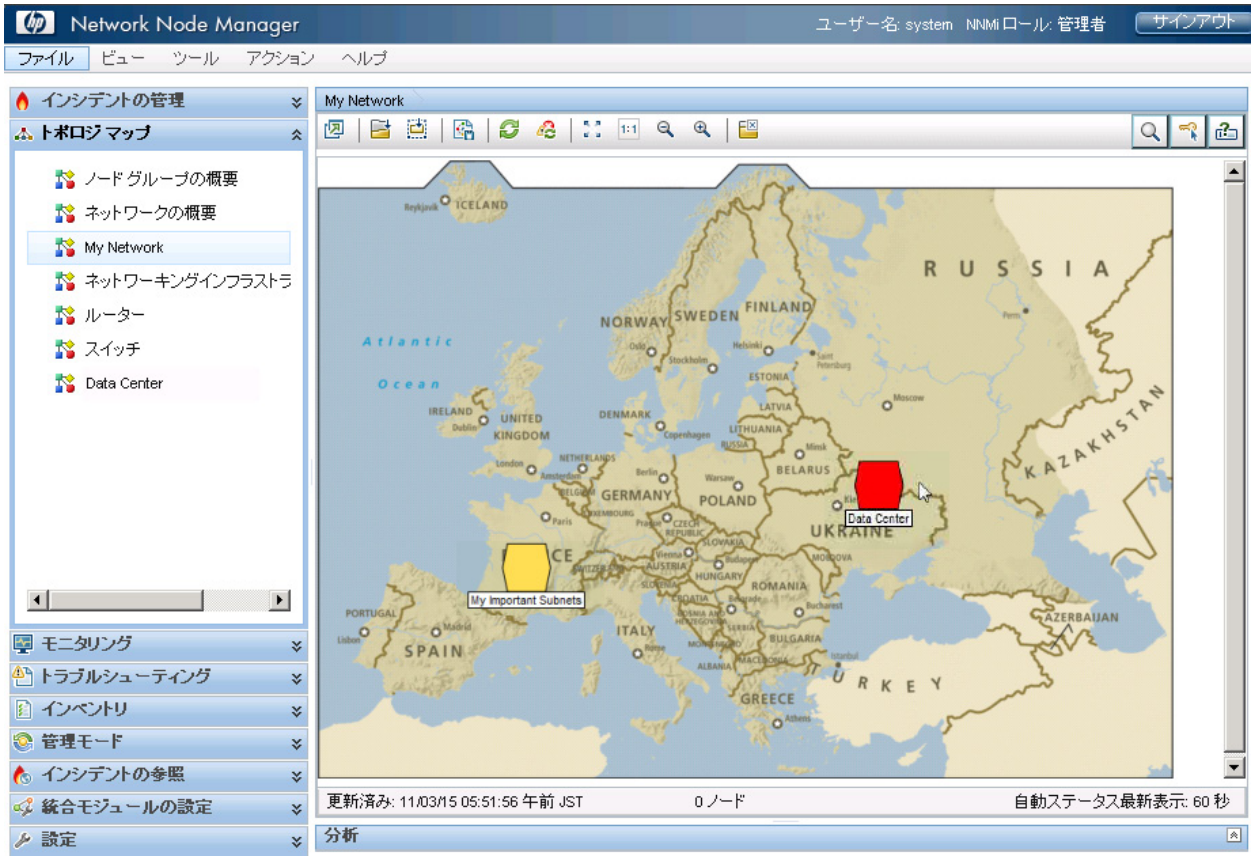
- ステータスは、*子ノード グループのノード*から親ノード グループのマップまで伝播されます。
- NNMi では、デフォルトでノード グループの最もクリティカルなノード ステータスが階層の上方向に伝播されます。これにより、高いレベルからノード ステータスを監視できます。
- トップレベルのノード グループ マップの色が緑から赤、黄、またはオレンジに変わった場合、問題のノードが見つかるまでノード グループ マップに移動できます。問題のノードに達したら、前のセクションで説明されているようなアクションを実行し、問題のトラブルシューティングを行うことができます。
- トラブルシューティングの進行状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。

以下のスクリーン ショットに、修正すべき問題がある My Network マップの例を示します。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、最初にサインインした後に 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、目的のマップ名を選択します。

図 62: My Network トポロジ マップ



マップベース*管理*アプローチには、以下のメリットがあります。

- 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*アプローチを使用する場合、以下の点に注意してください。

- 問題のソースを見つけるには、ノードを開いて **[結果]** タブに移動し、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。
- NNMi では、ノード ステータスは他のツール (HP Operations Manager (HP OM) など) に伝播されません。

リストベース管理

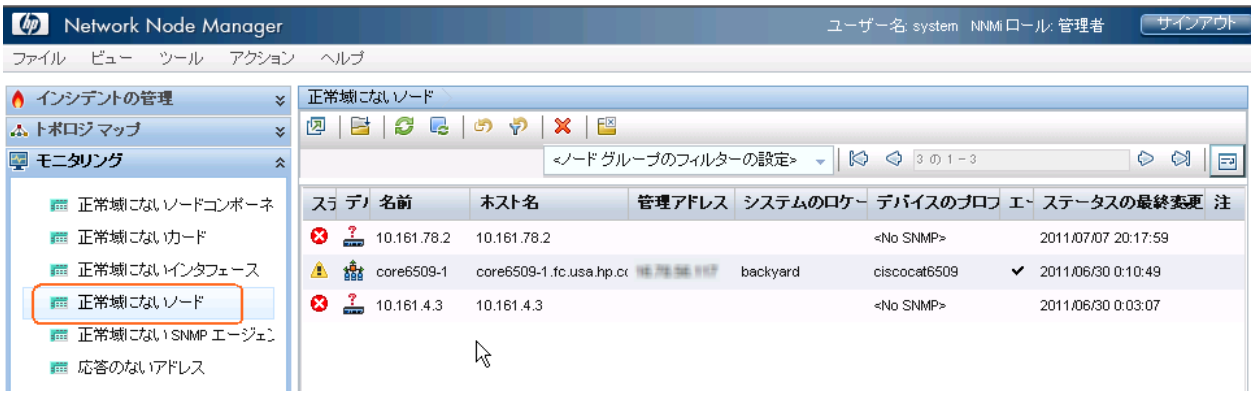
NNMi では、動的なリストでネットワークを管理できます。NNMi には、問題が発生しているノードまたはインタフェースを表示するテーブルが用意されており、動的に更新されます。このリストは、通常 15 秒ごとに NNMi によって更新されます。前のセクションで説明されているように、リストからツールを使用して問題を診断および修正できます。このリストは動的であるため、ノードまたはインタフェースが正常なステータスに戻ると、NNMi によってノードまたはインタフェースがこのリストから削除されます。

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。

以下の例のように、 ステータスが正常ではないすべてのノードが NNMi に表示されます。

図 63: 正常域にないノード



*リストベース管理*アプローチには、以下のメリットがあります。

- 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。
- NNMi では、ノード ステータスは他のツール (HP Operations Manager (HP OM) など) に伝播されません。

結論

このドキュメントでは、小規模なテスト ネットワークへの NNMi の導入について説明してきました。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。

2011 年 6 月 15 日

ご注意

保証について

HP 製品とサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載で追加保証を意図するものは一切ありません。HP では、ここに記載されている技術的、または編集上の不正確さや脱漏については責任を負いません。

ここに記載されている情報は、予告なく変更されることがあります。

権利制限について

機密性のあるコンピュータ 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からの正式な使用許諾が必要です。FAR 12.211 および 12.212 に準拠し、商用コンピュータ ソフトウェア、コンピュータ 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

商標に関する通知

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

HP 9000 コンピュータ上の 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。

Microsoft® および Windows® は、Microsoft Corporation の米国における登録商標です。

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

UNIX® は The Open Group の登録商標です。

Oracleテクノロジー — 権利制限について

国防省連邦調達規則補足 (DOD FAR Supplement) に従って提供されるプログラムは、「商用コンピュータ ソフトウェア」であり、ドキュメントを含む同プログラムの使用、複製および開示は、該当する Oracle 社のライセンス契約に規定された制約を受けるものとします。それ以外の場合は、連邦調達規則に従って供給されたプログラムは、「制限されたコンピュータ ソフトウェア」であり、関連文書を含むプログラムの使用、複製、および公開は、FAR 52.227-19、『商用コンピュータ ソフトウェア - 制限された権限』(1987 年 6 月) に記載されている制限に従うものとします。Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Oracleライセンスの全文は、NNMiの製品DVD上にあるlicense-agreements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 で開発されたソフトウェアが含まれています。

(http://www.apache.org)

この製品には、Indiana University Extreme! Lab で開発されたソフトウェアが含まれています。

(http://www.extreme.indiana.edu)

サポート

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

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

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

大部分のサポートには、HP Passport へのユーザー登録とログインが必要です。また、サポート契約が必要な場合もあります。HP Passport ID のご登録は、次の URL で行ってください。

http://h20229.www2.hp.com/passport-registration.html

アクセス レベルに関する詳細は、次の URL で確認してください。

http://h20230.www2.hp.com/new_access_levels.jsp