

HPE Network Node Manager i Software 10.20

NNMi を導入するためのステップバイステップ ガイド

ホワイトペーパー

目次

目的	3
基本ステップ: ロードマップ	3
ライセンスの適用	4
NNMiへのサインインとユーザーの作成	5
初期サインイン	5
ユーザーアカウントとロールの作成	5
通信の設定	7
検出の設定	
ハイパーバイザーと仮想マシンの検出の設定	
モニタリングの設定	
ESXiサーバーとVMwareのモニタリング設定	
監視対象インタフェース グループの作成	
インタフェースグループへの監視の適用	
監視設定のテスト	
モニタリングの例外	
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	
トラップの設定	
自動アクションの設定	
NNMiコンソールの設定	
概要	55
ノードグループの設定	
ノードグループマップの設定	61
NNMiの保守	
NNMiデータのバックアップおよび復元	
NNMiの設定のエクスポートとインポート	
データベースのトラップのトリム	
NNMiヘルスの確認	
ベストプラクティス	
使用シナリオの例	
例外管理	
マップベース管理	
リストベース管理	71
結論	
フィードバックをお寄せください	

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、『HPE 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。

メモ

最新の『HPE Network Node Manager iSoftware デプロイメントリファレンス』を見つけるには、https://softwaresupport.hpe.com/ を 参照してください。

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『HPE Network Node Manager i Softwareシステムとデバイス対応マトリックス』(<u>https://softwaresupport.hpe.com/</u>) 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。

注意: 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。

メモ:

最新の『HPE Network Node Manager iSoftware デプロイメントリファレンス』を見つけるには、https://softwaresupport.hpe.com/ を 参照してください。

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. 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、<u>https://softwaresupport.hpe.com/</u>にある『HPENetwork 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

- HPE Operations Manager (HPE OM)、HPE Universal Configuration Management Database (HPE UCMDB) などの他の HPE 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、https://softwaresupport.hpe.com/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、<u>https://softwaresupport.hpe.com/</u>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 HPE 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、HPE 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、HPE 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。

メモ

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、<u>https://softwaresupport.hpe.com/</u>にある『HPENetwork Node Manager i Softwareリリースノート』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。

- 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。
- -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

Hewlett Packard Enterprise
Network Node Manager i
ユーザー名
パスワード
サインイン

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



Network Node Manager i	ファイル(F)	ツ−ル (T)	ヘルプ(H)		ユーザー名:syst	em NNMill – J	は 管理者 リインアウト
山山 ダッシュボード							
₀≁ インシデントの管理	セキュリティウィ	パザード *	1				
▲ トポロジマップ	7 JOET		このページを使用して、次の	ついずれかを実行します:			
 日 モニタリング	> 1000	- アカウンドをエート - グルニプトセキュ	 ユーザーアカウントの作成す 割り当て、ユーザーアカウン 	5よひ削除、ユーサークル トへのユーザーグループ(ーフの作成および削除、ユーヤ の割り当て、ユーザーアカウンM	ナーク ループへの ・のマッピングの間	ユーサーアカウントの JD院。
▲ トラブルシューティング	>> ⊥ → >> z= →	ラル ラビビキュ ニャグループへの	コーザーアカウント	コーザーアカウントの	マッドング	コーザーグルー	7
	※ 変更振る	ありまた 夏の表示	* * %			* 🕯 %	·
			3	ユーザーアカウント	ユーザーグループ	名前	表示名
			Q. ユーザーアカウント	の作成	NNMi Webサービスクライア	admin	NNM管理者
るく インシテントの参照			IPT_system		21	level1	NNMiレベル1オペレーター
⊯ Cisco IPテレフォニー			MCAST_system	IPT_system	NNMi Webサービスクライア	level2	NNMiレベル2オペレーター
			MPLS_system	MCAST_system	NNMi Webサービスクライア	client	NNMi Webサービスクライ アント
						guest	NNMiゲストユーザー
Avaya IPテレフォニー Microsoft IPテレフォニー				MPLS_system	NNMI Web9 ービスクライア ント	globalops	NNMグローバルオペレー
🖉 MPLS							~
🖋 IPマルチキャスト							
🖋 Quality Assurance							
🌶 トラフィック分析							
� 統合モジュールの設定							
▶ 設定							
▼ セキュリティ ◆ ア セキュリティウィザード 田 ユーザーアカウント 田 コーザーアカウント							
				<前	次> キャン	・セル 🧧	保存して閉じる

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。

ユーザーアカウントの作成 🗙						
名前	Administrator					
729	•••••					
~F						
	追加	閉じる				

- 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。
---------------------------------------	-------------------------------

Network Node Manager i	ファイル(F) ツール(T) へル	ブ(H)		2	Lーザー名 : system	NNMill = /b;)	管理者 サインアウト
山 ダッシュボード	オキュリニンウンザード・						
ℴ≁ インシデントの管理	2+1071010-P- 2 ようごそ						
🛔 トポロジマップ	スラビビ アカウントとユーザー・	このページを使用して、次のいず ユーザーアカウントの作成および	れかを実行します: 削除、ユーザーグルー!	ブの作成および削除、コ	レーザーグループへの	のユーザーアカウ	いたの割り当て、ユ
🖵 EIQUVØ	ユーザーグループとセキュリテ・	ーザーアカウントへのユーザーグ	ループの割り当て、ユー	ーザーアカウントのマット	シグの削除。		
▲ トラブルシューティング	🎾 セキュリティグル ープへのノード	ユーザーアカウント	<u></u> ፲−ቻ− <u></u> <u>ア</u> カウント ወ	0マッピング	ユーザ	ーグループ	
■ ብ⁄ベ⊁リ	≫ 変更概要の表示	* 🖹 %			*	â %	
♪ 管理モード		名前	ユーザーアカウント	ユーザークループ		名前	表示名
Q インシテントの参照		Administrator	Administrator	NNMEETER	<	admin	NNM管理者
💋 Cisco IPテレフォニー					+	level1	NNMiレベル1オペレ
💉 Acme IPテレフォニー							NNM6L & th 2 th 4 L
🖌 Nortel IPテレフォニー					+	level2	-2-
💉 Avaya IPテレフォニー					+	client	NNMi Webサービスク
🖋 Microsoft IPテレフォニー							71/25
🖉 MPLS					+	guest	NNMiゲストユーザー
<u>∲</u> IPマルチキャスト					4	clobalons	NNMiグローバルオペ
💉 Quality Assurance					`	giobalopa	レーター
💅 トラフィック分析							
& 統合モジュールの設定							
▶ 設定							
▼ ► セキュリティ							
セキュリティウィザード マ	۰ ۲			<前 次>	キャンセ	ゆう 保護	存して閉じる

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

[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。

ファイル(F) ビュー(V	/) ツール <mark>(</mark> T) アクショ	aン(c) ヘルプ(H)	
通信の設定 🗙			
C 🖺 🖻 🛛 🕄			
■ SNMPのデフォルト	設定	デフォルトのSNMPv1/v2 弐ュニティ文字列	デフォルト
詳細は、ここをクリックして	ください。	▼ 読み取りコミュニティ文字列	
SNMPアドレス再検出を 有効にする		詳細は、ここをクリックしてください。	
Get-Bulkの有効化		* 🗃 😂 🖘 🖀	
* SNMPのタイムアウト	5.00 秒 👻	▲読み取りコミュニティ文字列	
例:タイムアウト = 3秒、U	~ライ数 = 4。NNMiはSNMPを使	t ntc public الم	
用して通信を試み、応答を 行では、NNMiは再試行の	:3秒待ちます。 それぞれの追加語 (前に 3.秒を追加し, 6, 9, 12.秒	public	
後に合計 30秒間試行しま 参照してください。	ます。詳細は、オンラインヘルプを	£	
* SNMPのリトライ数	2		
* SNMPボート	161		
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、 覐 [保存して閉じる] をクリックします。

ファイル(F) ビュー(\	/) ツール(T)	アクション <mark>(c)</mark>	ヘルプ <mark>(H)</mark>
デフォルトの読み取りコミ	ュニティ文字列 🗙		
C 🖺 🖺 関	C 📋		
() 最上位のフォーム	が保存されるまで、変	更はコミットされませ	:6!
•			^
読み取りコミュニティ文 字列			
順序			•

▼ 分析 - 要約 - オブジェクトが選択されていません

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。

ファイル(F) ビュー(V) ツール(T) アクション(c)	ヘルプ(H)
通信の設定*X 図 四 図 2	
 ■ SNMPのデフォルト設定 	< デフォルトのSNMPv1/v2 コミュニティ文字列 デフォルトS
詳細は、ここをクリックしてください。	▼ 読み取りコミュニティ文字列
SNMPアドレス再検出を 有効にする	詳細は、ここをクリックしてください。
Get-Bulkの有効化 💽	* 🗃 😂 🖘 🖀
*SNMPのタイムアウト 5.00 秒 💌	▲読み取りコミュニティ文字列
例: タイムアウト = 3秒、リトライ数 = 4。NNMilt SNMP を使 用して通信を試み、応答を3秒待ちます。それぞれの追加試 行では、NNMilt 再試行の前に 3 秒を追加し、6, 9, 12 秒	commstr1 ntcpublic
後に合計 30秒間試行します。詳細は、オンラインヘルプを 参照してください。	public
* SNMPのリトライ数 2	
* SNMPボート 161	
SNMPプロキシアドレス	
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。

メモ

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。

Network Node Manager i
山山 ダッシュボード
ℴ≁ インシデントの管理
🛔 トポロジマップ
🖵 モニタリング
A トラブルシューティング
■ ብ⁄ベ⊁リ
⚠ 管理モード
♀ インシデントの参照
� 統合モジュールの設定
▶ 設定
🛅 通信の設定
▼ 📂 検出
🛅 検出の設定
■ シード
田 テナント
────────────────────────────────────

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。

7.7.4.(E) Kaso(い いっし(エ) マクション(の) へし	. 7 (H)						
	/) 9-W(I) 79999(c) (W	(Z)(N)						
検出の設定 🗙								
C 🖻 🖻 C								
								~
▼ グローバル制御		<	スケジュールの)設定 💧	動検出ルール	/ サブネ	ット接続ル	ール 無番号
パフォーマンスモニタリン	/							
クのATM/フレームリレ ーインタフェースの抽出		(デフォ	・ルト のテナント	のみ) NNMil:	t、自動検出 [、]	で検出された	ノードからア	ドレスを収集しま
を有効にする		に使う	アドレスを制御	するルールを	定義します。	ルールがアド	レスに当て	はまらない場合、
白動摘出Dingフィープ	ግን ታ በ ~ ሀ (IBv/ ወ ቅ)	ます。	詳細は、ここを幼	フリックしてくオ	eatr.			
		*		🦘 🖀			₩ ←	0-0表示中、
このコンドロールは、すべ 択肢を上書きします。	くの自動検出ルールの [Pingスイーノを有効]とす	「つ」」選	- ~	Ding 7.4				
	451	L A	● 一致するノ	ープを有効	イスの検	チョーショー	名前	注
Ping X1 = 7	al 🗸	牙	ートの検出	にする	出	検出		
スイーブ間隔	24.00 時間 👻							
ノード名の解決		_						
* 1番目の選択	短いDNS名 ▼							
* 2番目の選択	短い sysName 👻							
* 3番目の選択	IPアF レス 💌							
LZB. Matter . T								
図 11: 検出の設定: 自動相	食出ルール							

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。

ファイル(F) ビ	ュー(V) ツール(T) アクション(c) ヘルプ(H)				
自動検出ルール*:	×				
C 🖻 🖪	🛛 C 📋				
•	· —				
(1)最上位のフォ	ームが保存されるまで、変更はコミットされません!				
- +++					
★ 基本	ブラムリレニ ナッル みつ コンタロ ナヤ キオ	IPの範囲	システムオブジェクトのID範囲		
自動検出ルールは、		= ⊂ຫ.	ルールの自動検出開始ポイント		
* 名前	MyNetwork	」(IPv4のみ)	このルールのPingスイーブを有効にす	する場合は、1つのルール内のネットワー	クの最大数である星
* 順序	10	2つのオクテ をクリックし	・ット (/16) より多くのオクテットを掴定し てください。	ないてくたさい。自動検出ルールのPing	スイーノの詳細は、
注		摘出の一下	の代われて、またけ摘出のことに加え	・てのDingフィーブの佐田 /IDy/ のみ)	
			「「なちかにす	COFINGAT 200600 (IFV4 004)	
		Pingス1 = る			
▼ この自動検出	出ルールの目的				
有効な場合、NNMil	はこのルールの基準に準拠しているすべてのノードを検出しま	- ZØ.	ルールの IPアドレス範囲		
す。無効な場合、NN します。詳細は、ここ	NMIはこのルールの基準に準拠しているすべてのアートを把き Tをクリックしてください。	a このルールI	に含めるIPアドレス範囲を指定します。	このルールで無視する、それらのIPアド	レスのサブセットを打
→致するノードの核		ともできます	(別のルールでは使用できます)。詳¥	まは、ここをクリックしてください。	
		EDH: WAN	Iの IPアドレス範囲ごとに1つのシードを	指定します。	
▼ デフォルトの	動作の拡張(ルーターおよび スイッチ外)	* *	i a 5 🕯	🖌 🖌 🛛 - 0表示中、省	
有効な場合、NNMil	は、SNMPに応答しこのルールの基準に準拠しているすべて		■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●		
のノートを視出しよ。	す。詳細は、ここをクリックしてくたさい。	新規	見作成		
SNMPテハイスの					
有効な場合、NNMII ノードを検出します。	は、ICMPに応答しこのルケルの基準に準拠しているすべての 「詳細は、ここをクリックしてください。	,			
非 SNMPデバイス 出	の 検				
図 12: 自動検出ル	レール: [順序] 属性				

- 4. 蒂 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。

ファイル(F) ビュー(V)	ツール(T)	アクション <mark>(c)</mark>	ヘルプ <mark>(H)</mark>				
IPの自動検出範囲*X							
Image:	C 📋						
(***) (i)最上位のフォー』保	存して閉じる。変更	ēはコミットされませ	1.61				
▼ 基本							
IPアドレス範囲は、ワイルド	カードまたは <mark>CIDR</mark> 表	記法で入力できま	ġ.				
IPv4 例: 10.2-3.*.1 10.2.120.0/21							
IPv6の例: 2001:D88:0:A00-AFF:* S2001:d88:0:a00::/56	*-*-*						
その他の例および詳細は、[ヘルプ] → [(このフォームの) 使用法]を参照してくだ さい。							
* IPの範囲	10.2.*.*						
* 範囲のタイプ	ルールに含める 🚽						

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:環境内で 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. 蒂 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、 関 [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 変更されます。

Network Node Manager i	ファイル(F)	ビュー(V) ツ	ール(T) アクション(c)	ヘルブ(H)	
<u> 山 </u> ダッシュボード					
₀~ インシデントの管理	୬ - F x				
	C' *		5 5 🗎		
日本 1000 100	▲ホスト名/IP	初期検出テナント	検出シードの結果	最終変更日時	注
A トラブルシューティング	10.161.4.3			2015/11/26 10:27:12	My Router
	16.78.56.2	デフォルトテナント	ノードが作成されました	2015/11/06 11:16:20	
目 42ペオリ	16.78.57.2	デフォルトテナント	ノードが作成されました	2015/11/06 11:16:39	
☆ 管理モード					
♀ インシデントの参照	更新日時:15/1	1/26 10:31:17 午前			合計::
� 統合モジュールの設定					
▶ 設定	▼ 分析				

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。

メモ:

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、『HPENetwork 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。

メモ:

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。

Network Node Manager i
<u>山</u> ダッシュボード
ℴ≁ インシデントの管理
🚠 トポロジマップ
🖵 τ _タリング
▲ トラブルシューティング
📑 ብንላንቶሀ
⚠ 管理モード
♀ インシテントの参照
� 統合モジュールの設定
▶ 設定
音 通信の設定
▶ 🖿 検出
▶ 🖿 モニタリング
▶ 🖿 インシチント
🛅 ステータスの設定
늘 グローバルネットワーク管理
▶ 🖿 ユーザーインタフェース
セキュリティ



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。

ファイル(F) ビュー(V) ツール(T)	アクション(c)	ヘルプ(H)				
通信の設定 🗙							
C 🖺 関 C							
SNMPのデフォルト 詳細は、ここをクリックしてい	設定 ください。	î	《 格証明	デフォルトの)信頼された証明書	領域 特定ノード	:の設定 > 🗸
<mark>SNMPアドレス再検出を</mark> 有効にする		_	詳細は、ここを	クリックしてく	tiatu.		
Get-Bulkの有効化	✓		* 🗃	C 🕈	Î		
* SNMPのタイムアウト	5.00 秒 🔻	·			₩ 🗲 1-	- 1表示中、合計 1行) 🔶 🕅 📄
 例:タイムアウト = 3秒、小 して通信を試み、応答を3秒 では、NNMiは再試行の前 会計 20 20 割() 	・ライ数 = 4。NNMiはS 少待ちます。それぞれの に 3 秒を追加し、6、9、 詳細は、ホッティン・4	NMPを使用 D追加試行 . 12 秒後に レブを差昭し	SNMP通信 を有効にす る	ICMP通信 を有効に する	▲ タ ーゲットホスト名	読み取りコミュニ ティ文字列	優先管理アドレス
てください。	a+ +⊞la (-1 / / -1 / - ()	V V CISYAH C	~	~	myesxserver.hp.com	public	
* SNMPのリトライ数	2						
* SNMPボート	161						
SNMPプロキシアドレス							
SNMPプロキシポート							
◆ SNMP最小セキュリティ レベル	⊐≋⊐⊒77 ▼						

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。

ファイル(F) ビュー(V) ツール(T) アクション	′(c) へルブ(H)
特定ノードの設定* 🗙	
C 🖻 🖪 関 C 📋	
() 最上位のフォームが保存されるまで、変更はコミットさ	(れません)
▼ 基本	🔺 < SNMPv1/v2コミュニティ文字列 SNMPv3設定 デ > 🗸
ご使用の環境でスパイラル検出が使用する必要がある 完全修飾ホスト名を入力してください (ドメインネームシス テム (DNS) に登録されているホスト名): * ターゲットホスト名 myesyserver bp.com	 ■ 読み取りコミュニティ文字列 読み取りコミュニティ文 字列
(オプション)ノードに複数のIPアドレスがある場合に使用 します。 優先管理アドレス 説明	 コミュニティ文字列の書き込み (コミュニティ文字列の設定) 書き込みコミュニティ文 字列
 ▼ SNMPの設定 	

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。

ファイル(F) ビュー(V	/) ツール(T)	アクション(c)	ヘルプ (H)				
特定ノードの設定*業								
C 🗎 🖺 関	C 📋							
() 最上位のフォームか	が保存されるまで、変更	[はコミットされま	せん!					
▼ 基本		-	✓ Pv3設定	デバイスの資	格証明	信頼された証明書	>	~
ご使用の環境でスパイラ) 完全修飾ホスト名を入力し テム (DNS) に登録されて	レ検出が使用する必要 こてください (ドメインネ・ いるホスト名):	がある ームシス	▼ このテーブル	にはデバイス資格	証明エントリ	」を1つだけ設定しま	वं.	
* ターゲットホスト名	myesxserver.hp.co	m	* 🗃	3	Î			
(オプション) ノードに複数(します。	のIPアドレスがある場合	合に使用		₩ ←	— 0 - 0表示中	•、合計0行 →	H	
優先管理アドレス			<u></u> ▲タイプ	ユーザー名				
說明								

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。

ファイル(F) ビュー(V) ツール(T) アクション(c) ヘル	ブ(H)					
特定ノードの設定 * 🗙						
C 🖻 🖪 🛛						
(1) 最上位のフォームが保存されるまで、変更はコミットされません!						
 ✓ 基本 	-	SNMPv1/v2コミュニティ文字列	SNMPv3設定	デバイスの姿格証明	信頼された証明書	
ご使用の環境でスパイラル検出が使用する必要がある完全修飾ホスト名 入力してください (ドメインネームシステム (DNS) に登録されているホスト 名):	14	 ▼ 証明書 詳細は、ここをクリックしてください。 	, ,			
* ターゲットホスト名 myesxserver.hp.com						
(オブション) ノードに対数の107ドしつがあろ根会に使用します		<mark>≄₀∖≣∣≎∣∽</mark> ∖î	i	🖌 🗲 🛛 - 0表	示中、合計0行 🔶	N 📰
(タンション)シートに後数のドアトレスかのの後日に使用します。 優先管理アドレス		▲ mbiest DM 証明書のアップロード	Valid From	•	Valid To	
説明						

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。

ファイル(F) ビュー 特定ノードの設定*X	(V) ツール(T) アクション(c) へル	7 (H)					
	l C 📋						
()最上位のフォーム	が保存されるまで、変更はコミットされません!						
▼ 基本		-	SNMPv1/v2コミュニティ文字列	SNMPv3設定	デバイスの資格証明	信頼された証明書	
ご使用の環境でスパイラ 入力してください <mark>(</mark> ドメイ) 名):	うル検出が使用する必要がある完全修飾ホスト名を ンネームシステム (DNS) に登録されているホスト		 ▼ 証明書 詳細は、ここをクリックしてください 	.).			
* ターゲットホスト名	myesxserver.hp.com						
(オブション)ノードに対象	かいロマドレスがある堪合に使用します.		🕹 🗃 😂 🖣 🕯		🖌 🗲 1-1表	示中、合計1行 🔶	
(4) / 10 / 10 / 10 / 10 / 10 / 10 / 10 / 1			▲ Subject DN	Valid From		Valid To	
説明]	CN=Adobe Root CA, OU=A	dobe Tr 2003/01/09 7:	37:23	2023/01/09 8:07:23	

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。

ファイル(F) ビュー(V) ツール(T) アクション(c)	ヘルプ(H)
通信の設定* 🗙	
 SNMPのデフォルト設定 詳細は、ここをクリックしてください。 	< 格証明 デフォルトの信頼された証明書 領域 特定ノードの設定 >
SNMPアドレス再検出を 有効にする	詳細は、ここをクリックしてください。
Get-Bulkの有効化 🛃	* 🗃 3 4 🖹
*SNMPのタイムアウト 5.00 秒 💌	
 例: タイムアウト = 3秒、リトライ数 = 4、NNMiは SNMPを使用して通信を試み、応答を3秒待ちます。それぞれの追加試行では、NNMiは再試行の前に 3秒を追加し、6、9、12 秒後に	SNMP通信 ICMP通信 を有効にす を有効に ターゲットホスト名 ニティ文字列 る する する たかい なった たい なった たい なった たい なった たい なった たい ない
日前の時間に行じます。詳細に、オンノインへのノを多頭してください。	✓ ✓ ntvqa-esx-host1 ntcpublic

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>

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。
 本 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 関 をクリックします。



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。

Network Node Manager i	ファイル <mark>(F)</mark>		년고 ~ (V)	ツール(T) アクション	'(c) ヘルプ	(H)	ב-	・ザー名:sys
<u>山山</u> ダッシュボード								
ℴ≁ インシデントの管理	7-r x							
▲ トポロジマップ		12		ъ 🔳	<2 m - 25	/イルターか3	≇ca> -	• • •
🖵 € 二タリング	ステータス	デパ	名前	ホスト名	管理アドレス	システムの	▲デバイスのブ	ロファイル
A トラブルシューティング	A	ATM	nortelnetsw1	16.78.56.12	16.78.56.12	5 upper e	VMware ESX/E	SXi
ー ■ インベルリ	0	勮	nortel5510	nortel5510.fc.usa.hp.co	16.78.56.118	building 6	VMware ESX/E	SXi
	8	2	losangeles-p1	losangeles-p1.fc.usa.hp			VMware Virtua	l Machine
	8	2	miami-ce1	miami-ce1.fc.usa.hp.com			VMware Virtua	l Machine
	8	2	cat2950	cat2950.fc.usa.hp.com			VMware Virtua	l Machine
田 SNMPエージェント	8	2	cisco2522	cisco2522.fc.usa.hp.com			VMware Virtua	l Machine
	8	2	mplspe07	mplspe07.fc.usa.hp.com			VMware Virtua	I Machine
田 IPサブネット	8	2	mplspe04	mplspe04.fc.usa.hp.com			VMware Virtua	I Machine
	8	2	mplsp04	mplsp04.fc.usa.hp.com			VMware Virtua	I Machine
	8	2	mplsce51	mplsce51.fc.usa.hp.com			VMware Virtua	I Machine

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。

Network Node Manager i	ファ	ብル <mark>(</mark> F	F) ビュー(V)	ツール(T)	アクション(c)	ヘルプ(H)	
辿 ダッシュボード							
。 インシデオの管理		F ×					
▲ トポロジマップ	ß		00	ъ			
🖵 モニタリング	ステ	-97	デ/▲名前	ホオト名	管理アドレン	ステナント	セキュリティク
▲ トラブルシュー テ ィング	0		• 8 • core6500-1 オトロズ辞史	core6509-1 fc	use 18 78 58,1	デフォルトテナンオ	デフォルトのも
■ ብሥሩታり	4		リート		.2	デフォルトテナンオ	デフォルトのも
■ <i>/</i> -ド	0		フィルター		.2	デフォルトテナンオ	デフォルトのも
■ インタフェース			CSVICエクスポー	-ŀ-			
IPアドレス			ダッシュボードを	開く			
囲 SNMPエージェント		1	マップ(M)		•		
■ Webエージェント			//===(c)				
田 IPサブネット			シリノ(G) ノードアクセス(N				
			ボーリングの	/			
			設定の詳細(C)				
			MIB情報		•		
			ノードグループメ	ンバーシップ(0)	•		
曲 ノートセンサー			カスタム属性(u)		•		
■ 初理センリー			Enterprise Unifi	ed Communicat	tions Map 🕨		
== ノード (すべての尿性)			IPテレフォニー		•		
■ インタフェース(すべての属性)			トラフィックマップ		•		
■ IPアドレス(すべての属性)			Quality Assuran	ice	•		
III MIB変数		Ê	削除				
■ シャーシ冗長グループ			管理モード(t)		•		
■ カード冗長グループ		0	ベースライン診断	íの実行 <mark>(評価)</mark>			
■ ルーター冗長グループ			接続されたエンド	ノードの表示			
■ ルーター冗長メンバー			ハイバーバイザー	- (v)		ハイパーパイザー	ග Wheel
■ ノードグループ 🚽	-				-	ハイバーバイサー	ரLoom

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

/-F x /-F x	1.2. Î												
▼ 基本		<	全般	IP7	۴IJ	ス インタ	フェース シャ・	-シ カ・	-6	ポート	VLANポート	ルーターの冗長	性 ケーノ
名前	c2900xl-1												
ホスト名	c2900xI-1.fc.t(#a fig) arter:	_				-							
管理アドレス	16.78.56.53	6	s 💼	ີ	1	`						M 4	€ 1 - 9表示
ステータス	正常域	•	ステータン	管理	運用	ifName	ifType	ifSpeed	ifInde	ifAlias	物理アドレス	レイヤー2の接	ה
* ノード 管理モード	管理対象 👻			0	\odot	Fa0/2	ethernetCsmac	100 Mbps	3	HSRP D	00036BF790C2	c2900xI-1[Fa0/	2],mplspe03[
		0	>	6	5	Fa0/1	ethernetCsmac	100 Mbps	2	HSRP D	00036BF790C1		
テハイスのフロファイル	ciscoCat2912XL	0	>	6	5	Fa0/3	ethernetCsmac	100 Mbps	4	HSRP D	00036BF790C3		
検出		0	3	6	5	Fa0/4	ethernetCsmac	100 Mbps	5	Link to e	00036BF790C4		
検出状態	検出が完了	0	3	6	6	Fa0/5	ethernetCsmac	100 Mbps	6		00036BF790C5		

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。

2-F 🗙 🖊 🥂 🗙									
	C 🗎								
▼ 基本		< 全般	IP75 J.2	र ि रः	タフェー ス	24-2	カード	ボート	VLANボート ルーターの
名前		•							111
ホスト名	1000	-2 L 50		_					
管理アドレス	A CONTRACT OF A	6	0	_					
ステータス	警戒域	▼ ステータス	管理状影	運用状態	ifName	ifType ifSpee	d	ifIndex	ifAlias
* ノード 管理モード	管理対象 👻	0	5	5	Fa3/31	ethernetCsmacd	100 Mbps	33	connection to testw laptop
デバイスのプロファイル	cierorat6509	0	E	6	Fa3/34	ethernetCsmacd	100 Mbps	36	monitor port to gig probe
27712102 H 277110		0	100 C		Tu1	tunnel	9 Kbps	72	tunnel to demorams9 for area
* テナント	デフォルトテナント 🛛 🐨 👻	0	E	63	Tu2	tunnel	9 Kbps	73	tunnel to demorams9 for area
* セキュリティグループ	デフォルトのセキュリティ 🔻 🌃 🚽	0	6	6	Lo0	softwareLoopba	8 Gbps	63	
検出		0	6	6	Se2/1/3	propPointToPoints	1.5 Mbps	62	
検出状態	検出が完了	0	6	6	Se2/1/2	propPointToPoint	1.5 Mbps	61	
最後の完了日時	2015/11/30 10時47分26秒 CST	0	6	6	Se2/1/1	propPointToPoint	1.5 Mbps	60	
注		.0.	5	5	Se2/1/0	propPointToPoints	1.5 Mbps	59	

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。

 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。

ノードグループ ×										
ଜା 🛊 🗃 😂 छ 🏷 ଅନ୍ 📋										
ステータ ス	▼名前	ビューフ イルター リストに 追加	フィルタ ーリスト に追加	ステータ スの計算	ステータスの最終変 更日時	注				
0	非SNMPデバイス	~	-	-	2015/11/06 11:02:4	検出プロセスでSNMP照会に応答しな				
0	隣接接続フィルター	-	-	-	2015/11/06 11:02:4	ノードグループマップの隣接接続の計				
0	重要なノード	~	~	-	2015/11/06 11:02:4	エッジルーターのような重要なノードは				
0	仮想マシン	~	~	-	2015/11/06 11:02:4	仮想マシン				
0	ルーター	~	~	-	2015/11/06 11:02:4	ルーティングを行うノードを含みます。				
0	ネットワーキングインフラストラク	~	-	-	2015/11/06 11:02:4	ネットワーキングインフラストラクチャラ				
0	スイッチ	~	~	-	2015/11/06 11:02:4	切換えを行なうノードを含みます。				
0	VMware ESXホスト	~	~	-	2015/11/06 11:02:4	VMware ESX차자				
0	Subnet A	~	-	~	2015/11/30 10:04:3					
0	Name	~	-	~	2015/11/26 16:06:1					

図 35:設定:ノードグループ

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。

ファイル(F) ビュー(V) ツール(T) アクション	∕(c)	へルプ <mark>(</mark>	H)				
モニタリングの設定* 🗙							
C 🗈 📓 C							
▼ グローバル制御 無効の退金 以前のデバイフの状態とフニックフけ変更	1	インタフェー	スの設定	ノードの設定	デフォルト	設定	
されません。詳細は、ここをクリックしてください。		▼ 複数の設定;	が定義されて	いるとき、NNMil	は、順序番号	<mark>(</mark> 最小番号が	最初)に従っ
状態ポーリングを有効に する		* =	c •	∽ 💼	M	← 1-	2表示中、合調
上記の[状態ボーリングを有効にする]を選択しないと、 NNMIによって次のオブジェクトタイプのモニタリングが無 効にされ、それぞれの以前の状態がリセットされます。							
カードポーリングを有効 にする							
シャーシボーリングを有 効にする							
ノード センサーボーリング を有効にする				ノードの SNMP ポーリングと	管理アドレ	IPアドレス 防空 ポーリ	インタフェ 〜 <i>ス</i> 障害
物理センサーボーリング を有効にする		▲順序	名前	Webポーリン グを有効にす	スホーリン グを有効 にする	いた ングを有効 にする	のポーリン グを有効
ルーター冗長グループボ ーリングを有効にする				る	- 3 0		にする
NNNNNA、#810「ニー 取した設定 (#80付足なものから乗り 特定でない順にインタフェース、ノード、デフォルト) に従っ て検出された各インタフェースをモニタリングします。詳細 は、ここをクリックしてください。							
		40	虚拟机	~	~	~	~

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] では、ハイパーバイザーグループ、たとえば「VMWare ESX Hosts」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。

ノードの設定*× ② □ □ □ □ □ □ □ □ □ □								_	
① 最上位のフォームが保存さ	れるまで、変更!	は ネット されません!		_					
- ▼ 基本				<u>^</u> し	きい値の設定	ベースライン語	没定		
詳細は、ここをクリックしてください	, ¹ .				•				
* 順序 520				才	プションのNNM iS と上限値を設定し	PI Performa ੜ ਰੋ.	nce fo	r Metric	s)ນີ
* ノードグループ VMware	ESX차가		- 🖷 -		** 🖬 😂	5 📋			
ノードのSNMPボー リングとWebボーリ ✔ ングを有効にする					▲監視対象属性	しきい値の 設定タイプ	上眼 値	リアー ムの 上眼 値	下随
▼ 障害のモニタリング									
詳細は、ここをクリックしてくたさい	. ^۱ ۰								
ICMP障害モニタリング									
● 管理アドレスホーリン 「グを有効にする」									
IPアドレス降害ボー リングを有効にする 降害のモニタリンク									
インタフェース障害の ポーリングを有効に ✔ する									

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 覐 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。

Network Node Manager i	ファイル(F) ビュー(V) ツー	Jk(T)	アクション(c)	ヘルプ <mark>(H)</mark>	
่ш่ ⊈รงวิวส์∽⊦ี					
ℴ≁ インシテントの管理					
🛔 トポロジマップ	C \star 🖷 I C I 🤊 1	5 🔳			
🖵 モニタリング	▲名前	ビューフィ ルターリス	フィルター リストに追	ノードグループ	注
A トラブルシューティング		トに追加	ha		
■ インベオリ	ATMインタフェー ス	~	~		非同期伝送モード (ATM) リンクとして識別されるインタ
♪ 管理モーF	DSxインタフェー ス	~	~		デジタルシグナル 1 (DS1、別名T1) リンクとして識別a
Q インシテントの参照	ISDNインタフェー ス	~	-		ISDNに関係するインタフェースタイプで指定されるイン
💉 Cisco IPテレフォニー	Important 9kbs Tunnels	~	-		
🖋 Acme IPテレフォニー	Nortel-Virtual-Interfaces	~	-		
🖋 Nortel IPテレフォニー	SONETインタフェー ス	~	~		同期光学ネットワーク (SONET) または同期デジタル
🖋 Avaya IPテレフォニー	VLANインタフェー ス	~	-		VLANインタフェースは、信頼性のあるパフォーマンス)
🖋 Microsoft IPテレフォニー	WLANインタフェー ス	~	~		無線ローカルエリアネット ワーク (WLAN) リンクとして語
🖋 MPLS	ソフトウェアル ープ バックインタフェース	~	-		ソフトウェアループバックインタフェースは、よく知られて
💉 IPマルチキャスト	フレームリレーインタフェース	~	~		フレームリレーリンクとして識別されるインタフェースで
🖋 Quality Assurance	ボイスインタフェース	~	-		音声関係のインタフェースタイプで識別されるボイスイ
🖋 トラフィック分析	ポイントツーポイント インタフェース	~	-		ポイントツーポイント インタフェースは、通常、ダイヤル
◆ 統合モジュールの設定	リンクアグリゲーション インタフェース	~	-		リンクアグリゲーションプロトコルの中で、アグリゲータ
▶ 設定					
• 🖿 мів					
囲 デバイスのプロファイル	更新日時: 15/11/30 02:05:23 午後				合計:13
▼ 🖕 オブジェクトグループ					
Ⅲ ノードグループ	▼ 分析				
田 インタフェー スグループ	要約				0

図 39: 設定: インタフェースグループ

- 2. 蒂 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。

メモ

Network Node Manager i ビュー(V) ツール(T) アクション(c) ファイル(F) ヘルプ(H) ユーザー名: system NNMiロール: 管理者 サインアウト 山 ダッシュボード インタフェー スグループ 💥 📗 インタフェー スグループ* 🗙 ₀♪ インシデントの管理 2 2 1 3 1 3 2 ▲ トポロジマップ 📮 モニタリング ▼ 基本 ifTypeフィルター 追加のフィルター A トラブルシューティング * 名前 Important 9kbs Tunnels ビューフィルターリストに 罰 インベオリ likeまたはnot like演算子を使用する場合、*(アスタリスク)は文字列内のO以上の文字に→致 追加 ☆ 管理モード し、?(疑問符)は文字列内の1文字に一致します。 ノードグループ - 🖬 -包括的なIPアドレス範囲を作成するには、between演算子を使用します。有効な例: ipAddress between 10.10.1.1 AND 10.10.1.255 🔮 Cisco IPT L 7t = -注 詳細は、ここをクリックしてください。 ۶ Acme IPテレフォニー フィルターエディタ Ś Nortel IPテレフォニー 属性 演算子 値 インタフェー スグループは、ifTypeフィルターと追加のフィルター を使用してフィルターリングすることができます。ifTypeフィルタ 🖋 Avaya IPテレフォニー ifAlias ▼ like 追加 tunnel to* 插入 ø Microsoft IPテレフォニー - と追加のフィルターの両方を使用する場合、インタフェースが このインタフェースグループに属するには、少なくとも 1つの 罟換 🖋 MPLS ifTypeフィルター仕様および付加的なフィルター仕様と一致する 必要があります。ノードグループを選択する場合、インタフェ 💅 IPマルチキャスト 挿入 スは、そのノードグループのメンバーになっているノードに属す AND ø Quality Assurance る必要があります。[ヘルプ] → [インタフェースグループフォーム の使用法]を参照してください。 AND 🖋 トラフィック分析 OR ifSpeed = 9000 NOT 🗞 統合モジュールの設定 インタフェースグループ定義をテストするには、[ファイル] → [保 ifAlias like tunnel to 存]、[アクション] → [インタフェースグループの詳細] → [メンバーの表示 (子グループを含む)] を選択してください。 EXISTS ♪ **設**定 NOT EXISTS 🎹 デバイスのプロファイル 削除 🔻 🗁 オブジェクトグループ NNM iSPI Performance フィルター文字列 NNM iSPI Performance for MetricsおよびNNM iSPI for (ifSpeed = 9000 AND ifAlias like tunnel to*) Ⅲ ノードグループ Traffic で使用。 日 インタフェースグループ

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。

ファイル <mark>(F)</mark>	ビュー(V)	<u>ッ</u> -	・ル <mark>(T)</mark> アク・	ション(c)	ヘルプ <mark>(H)</mark>					ユーザー名:sy	stem NNMip ール: 管理:	昔 サインアウト
インタフェー	スグループ 🗙	インタ	フェースグループ	* 1 2	タフェース 🗙							
ଅ 🖿	C 💈 🕇		5				Impo	rtant 9kbs Tu	unnels	- H +	1-3表示中、合計3行	→ N 📰
▲ ステータ:	管理状態	運用	ホスト元ノード	ifName	ifType	ifSpeed	ifInde	ifDescr	ifAlias	物理アドレス	ステータスの最終変更日間	∮ 状態の最終変更E
0	0	\bigcirc	core6509-1	Tu5	tunnel	9 Kbps	85	Tunnel5	tunnel to		2015/11/16 16:32:30	2015/11/16 16:40
0	0	\bigcirc	core6509-1	Tu4	tunnel	9 Kbps	84	Tunnel4	tunnel to		2015/11/16 16:32:30	2015/11/16 16:40
0	0	\bigcirc	core6509-1	Tu1	tunnel	9 Kbps	81	Tunnel1	tunnel to		2015/11/16 16:32:30	2015/11/16 16:40
•												۱.
更新日時:1	5/11/30 11:11:58 午	前			合計:3	逶	択済み	: 0	フィルタ	ト:オン	自動	リフレッシュ: 10 分

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。

メモ

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。

ファイル(F) ビュー(V) ツール(T) アクション(c)	ヘルブ	(H)									
モニタリングの設定 🗙											
▼ グローバル制御 🔶	インタフ	エースの設定 ノー	・ドの設定	デフォルト副	u 定						
無効の場合、以前のデバイスの状態とステータスは変更されません。詳細は、ここをクリックしてください。		定が定義されている。	とき、NNMilt	、順序番号(最小番号が最	景初)に従って	[設定を適用	_ます。			
状態ポーリングを有効に する	*	🗃 🕫 🖴	Î				M	← 1-3表	示中、合計3	行 🔶 🕴	N [
上記の【 状語ボーリングを有効にする 】を選択しないと、 NNMiによって次のオブジェクトタイプのモニタリングが無 効にされ、それぞれの以前の状態がリセットされます。	▲ JĒ	夕前	IPアドレス 障害ポーリ	インタフェ 〜 2障害 のポーリン	未接続イン タフェース	IPアドレス をホストす るインタフ	リンクアグ リゲーショ ンインタフ	インタフェ ー スパフォ ー マンスの	DSxインタ フェースの パフォーマ	SONETイ ンタフェー スのパフォ	ATM フェー フォー
カードボーリングを有効 にする シューショガーリングを有効	序		ングを有効 にする	グを有効 にする	のポーリン グ	エースのポ ーリング	エースのボ ーリング	ポーリング を有効に する	ンスのポー リングを有 効にする	ポーリング を有効に オス	スのシングをした。
効にする	100	ISDNインタフェー ス	-	~		-	-	-		-	-
ノードセンサーボーリング 🔽	200	ポイントツーポイント・	•	~						-	-
物理センサーボーリング を有効にする	300	VLANインタフェー ス	-	~	-	-	-	-	-	-	-
ルーター冗長グループポ ーリングを有効にする											
NNMit 島知に一致した設定 (最も特定なものから最も特 -					合計:3	選択済み	:0 74	(ルター: オフ		自動リフレッ	シュ: ス

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 <u>ष</u> [保存して閉じる] をクリックして、変更を保存します。

ファイル(F) ビュー(V) ツール(T) アクション(c)	^	いレブ	(H)									
モニタリングの設定* 🗙												
C 🖻 関 C												
	_											
▼ グローバル制御 🔶	1-バル制御 合 インタフェースの設定 ノードの設定 デフォルト設定											
無効の場合、以前のデバイスの状態とステータスは変更されません。詳細は、ここをクリックしてください。		•										
	複夢	対の設	と定が定義されていると	: き、NNMilt	、順序番号(最小番号が最	景初)に従って	「設定を適用」	します。			
状態ボーリングを有効に する			5 0 5	a				ы	▲ 1.3志	志中 合計3	লি ১ ।	N I Í
上記の「状態ボーリングを有効にする」を選択しないと、		T		-					< [1- 346			n [
NNMiによって次のオブジェクトタイプのモニタリングが無									インタフェ	DSxインタ	SONET-1	ATM
効にされ、それぞれの以前の状態がリセットされます。				IPアドレス	12971	未接続イン	IPアトレス	リンクアク	ースパフォ	フェースの	2971-	71-
カード ボーリングを有効 にする	ار ار	▲ 順 序	名前	障害ポーリ ングを有効 にする	ー ス障害 のポーリン グを有効	タフェース のポーリン グ	をホスト g るインタフ エースのポ	リケージョ ンインタフ エースのポ	ーマンスの ポーリング を有効に	パフォーマ ンスのポー リングを有	スのハフォ ーマンスの ポーリング	フォー スの: ング3
					1-90		~999	-029	する	効にする	を自効に	しまする
シャーシルーリンジを有 🛃	L CO	-		-							90	
	5	50	Important 9kbs Tunn	-	~	~	~	~	-	-	-	
ノート センサーボーリング を有効にする	1	100	ISDN Interfaces	-	~	•	-	•	•			
物理センサーボーリング	2	200	Point to Point Interfa	-	~	-	-	-	-	-	-	
を有効にする 💌	3	300	VLAN Interfaces	-	~		-	-	1		-	
ルーター 元長クルーフボ												

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。
- 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。

C 🖿			, ,							Important §	9kbs Tunnels	-	K	€ 1-3
▲ ステータ	2 管理状態 🖓	運用	ホスト元ノード	ifName	ifType	ifSpeed	ifInde	ifDescr	ifAlias	1	カ理アドレス	ステー	マスの最終	漆更日時
9	0		core6509-1	Tu5	tunnel	9 Kbps	85	Tunnel5	tunnel to demorams	9		2015/1	1/16 16:3	2:30
0	0	0	core6509-1	Tu4	tunnel	9 Kbps	84	Tunnel4	tunnel to rams910			2015/1	1/16 16:3	2:30
9	0		core6509-1	Tu1	tunnel	9 Kbps	81	Tunnel1	tunnel to sussi			2015/1	1/16 16:3	2:30
0	0		core6509-1	Tu1	tunnel	9 Kbps	81	Tunnel1	tunnel to sussi			2015/1	1/16 16:3	-

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。

Network Node Manager i	ファイル <mark>(</mark> F)	년고 ~ (V)	ッー	л⊬ (т)	アクション(c) ヘルプ(H)		
山 ダッシュボード					№ マップ(M)	•	
₀≁ インシデントの管理	42971-	- 2 ×			箇 グラフ(G)	•	
🎄 トポロジマップ	2 🖬	0 12 1		5	ポーリング(I) 恐定の詳細(C)	•	
🖵 モニタリング	▲ ステータ:	「管理状態」>	運用	ホスト元	あたのよう (C) カスタム属性(U)		モニタリングの設定
▲ トラブルシューティング	0	0	0	core650	Enterprise Unified Communications	Map 🕨	Tunnel5
	0	0	0	core650	トラフィックマップ	•	Tunnel4
==×		\odot	\odot	core650	Quality Assurance	•	Tunnel1
田 インタフェース					管理モード(t)	•	
III IPアドレス					ハイバーバイザー (v)	•	
III SNMPエージェント							
⊞ Webエージェント							
田 IPサブネット							

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。

モニタリング設定レポート: Interface

NNMi管理 ステーション: オブジェクト名: Tu5 ホスト元ノード: core6509-1 ビンナ:NNM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								
パフォーマンスのボーリング間隔	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ボ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									
917	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								
パフォーマンスのボーリング間隔	0日 0時間 5分 0秒								

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。

Network Node Manager i	ファイル(F) ビ	ユー(V) ツー	///(T)	アクション(c) ヘルプ(H)	_		
<u> 山 </u> ダッシュボード				<mark>™</mark> マップ(M)	•		
ℴ≁ インシデントの管理	インタフェース 🗙	インタフェース	×	📓 グラフ(G)	•		
▲ トポロジマップ	୮୯ 🚍 😂	12 5 1	5	ボーリング(1) 恐定の詳細(C)	2		
□ T =ないガ	▲ ステータン 管理状	[態▽ 運用	ホスト元	カ コク 人 属性 (u)	(I	le: ifDescr	ifAlias
	Ø Ø	0	core650	Enterprise Unified Communications Ma		Tunnel5	tunnel to de
	00	0	core650	トラフィックマップ		Tunnel4	tunnel to ra
言 インヘントリ	0 0	0	core650	Quality Assurance		Tunnel1	tunnel to su
📥 المر 🖽 📩		Ŭ					
田 インタフェース				管理モード(t)	•	▶ 管理	
IPアドレス				ハイパーパイザー (v)	•	🍾 管理 (すべてを!	リセット)
III SNMPIージェント						🔀 非管理対象	6
						🏠 サービス停止中	4
☆ 管理モード							_
♀ インシテントの参照							
🖋 Cisco IPテレフォニー	更新日時:15/11/30	02:59:25 午後			合計:	3	ሕ 1

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.hpe.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。

- 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。



 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。

 基本 インシデントのトラブルシュー 名前 In SNMPオブジェクトID (OID) が NNMiでは、ワイルドカート フしてください。 SNMPのオブジェクトID .1 有効にする 	ティングの詳細は、ここをク nterfaceDown 属性は、OIDの最後に指定 ドは、1.3.6.1.4以降のOID 1.3.6.1.4.1.11.2.17.19.2.0.	リックしてください。 する必要がある1文字の でのみ有効です (プライ)ワイルドカード (*) を5 ベートMIB)。詳細は、;	受け付けま こをクリッ	インタフェー スの - NNMilによって、・ す。インタフェー、
インシデントのトラブルシュー 名前 Ir SNMPオブジェクトID (OID) が す。NNMiでは、ワイルドカート フしてください。 SNMPのオブジェクトID .1 有効にする .	ティングの詳細は、ここをク hterfaceDown 属性は、OIDの最後に指定 ドは、1.3.6.1.4以降のOID 1.3.6.1.4.1.11.2.17.19.2.0.	リックしてください。 する必要がある1文字0 でのみ有効です (プライ)ワイルドカード (*) を5 ペートMIB)。 詳細は、(受け付けま ここをクリッ	NNMilによって、 す。インタフェー
名前 Ir SNMPオブジェクトID (OID) が す。NNMiでは、ワイルドカート フしてください。 SNMPのオブジェクトID .1 有効にする 、	nterfaceDown 属性は、OIDの最後に指定 ドは、1.3.6.1.4以降のOID 1.3.6.1.4.1.11.2.17.19.2.0.	する必要がある1文字0 でのみ有効です (プライ)ワイルドカード (*) を勢 ベートMIB)。詳細は、(- 受け付けま ここをクリッ	NNMilによって、 す。インタフェー
名前 Ir SNMPオブジェクトID (OID) / す。NNMiでは、ワイルドカー フしてください。 SNMPのオブジェクトID .1 有効にする 、	nterfaceDown 属性は、OIDの最後に指定 ドは、1.3.6.1.4以降のOID 1.3.6.1.4.1.11.2.17.19.2.0.	する必要がある1文字0 でのみ有効です (プライ)ワイルドカード (*)をst ベートMIB)。詳細は、。	受け付けま ここをクリッ	す。インタフェー
SNMPオブジェクトID (OID) / す。NNMiでは、ワイルドカー りしてください。 SNMPのオブジェクトID .1 有効にする	属性は、OIDの最後に指定 ドは、1.3.6.1.4以降のOID 1.3.6.1.4.1.11.2.17.19.2.0.	する必要がある1文字0 でのみ有効です (プライ)ワイルドカード (*)を∮ ベートMIB)。詳細は、(受け付けま ここをクリッ	
1、NNMICは、ワイルドカー りしてください。 SNMPのオブジェクトID 1 有効にする	トは、1.3.6.1.4以降のOID 1.3.6.1.4.1.11.2.17.19.2.0.	でのみ有効です (ノフィ	ベードMIB)。詳細は、 (ここをクリッ	
SNMPのオブジェクトID .1 有効にする	1.3.6.1.4.1.11.2.17.19.2.0.				* •
SNMPのオブジェクトID パ 有効にする	1.3.6.1.4.1.11.2.17.19.2.0.				▲ インタフェ·
有効にする 💽		19			
	2				
カテゴリ 隆	辛害		-	- 🗊 -	
77202	17971-7			▼ 199	
重大度 f	包険域 👻				
olicは、\$(variable_name) る D変数を選択します。詳細は メッセージの形式 Interface Down with Alias	E使用します。有効なパラメ: 、ここをクリックしてください ■ SifAlias	-タのセットまたはカス!	ネムインシデント属性か	"6. Zh6	
説明 このインドレギントは インタコ	7フがポートングに広体	しかいことを会味します			
201777771a. 1737	71-700-9771-108	UALICE EAST UAS	*		
作成者 九	コスタマー			- 🖬 -	

4. 「「フイック検索] 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。

メモ

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。

重要	をな未	解決	インシデント 🗙									
Z			0 12 5	۳, 📋								
重大	優先	51	▼最後の発生日時	割り当て先	ソースノード	ソースオブジェク	カテ	77	発生	相関	テナント	メッセージ
۲	5	5	11/17/15 3:39:37 AM		192.174.63.04	192.159 All 18	**		•	Þ <u>⊼</u> 4	デフォルト	Node Down
\triangle	5	5	11/17/15 3:37:17 AM		j4200-3	j4200-3.fc.usa.h	*	P	1	₽ <u>a</u> ∎	デフォルト	No secondary card in Card Redundancy Group
8	5	5	11/17/15 4:49:16 AM		wanrouter-1	Tu2	*		Ъ	Þ <u>⊼</u> 4	デフォルト	Interface Down with Alias = tunnel to ntc2rams
0	5	5	11/17/15 4:49:01 AM		napervillepr	Gi0/1	*		ъ	▶ <u>₩</u> 4	デフォルト	Interface Down with Alias = connection to napervillepe1 g0/0
8	5	5	11/17/15 3:37:44 AM	-	wan-bo2-sw1	Fan Sensor		1	Ъ	Þ <u>⊼</u> 4	デフォルト	Fan on wan-bo2-sw1 is malfunctioning
8	5	5	11/17/15 3:37:45 AM		nortelnetsw1	Fan Sensor		1	ъ	Þ <u>⊼</u> 4	デフォルト	Fan on nortelnetsw1 is malfunctioning
8	5	5	11/17/15 3:37:29 AM		mplspe01	Fan 1		1	Ъ	Þ <u>⊼</u> 4	デフォルト	Fan on mplspe01 is malfunctioning
8	5	5	11/17/15 3:37:29 AM		mplspe01	Fan 2		1	1	Þ <u>⊼</u> 4	デフォルト	Fan on mplspe01 is malfunctioning
8	5	5	11/17/15 3:37:44 AM		mplsp04	Fan 4		1	1	Þ <u>⊼</u> 4	デフォルト	Fan on mplsp04 is malfunctioning

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.hpe.com で入手できる『Step- by-Step Guide to IncidentManagement』を参照してください。

メモ:

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。

メモ:

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。

<u>山</u> ダッシュボード								
☆~ インシテントの管理								
歳 トポロジマップ		9						
	▲名前	MIB77-11						
		file:///opt/OV/misc/nnm/snmp-mibs/Standard/rtc5060-PIM-STD-MIB.mib						
	POWER-ETHERNET-MIB	file:///opt/UV/misc/nnm/snmp-mibs/Standard/rtc3621-PUWER-ETHERNET-MIB.mib						
	PertHist-TC-MIB	tile:///opt/OV/misc/nnm/snmp-mibs/Standard/rtc3593-PertHist-TC-MIB.mib						
	Q-BRIDGE-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc4363-Q-BRIDGE-MIB.mib						
Q インシデントの参照	RAPID-CITY	file:///opt/OV/misc/nnm/snmp-mibs/Vendor/Nortel/RAPID-CITY.mib						
💉 パフォーマンス分析	RFC-1212	vfs:/opt/OV/NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc1212-RFC1212.mib						
9、 抜合モジュールの設定	RFC-1215	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc1215-RFC1215.mib						
L are	RFC1155-SMI	vfs:/opt/OV/NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc1155-RFC1155-SMI.mib						
	RFC1213-MIB	vfs:/opt/OV/NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc1213-RFC1213-MIB.mib						
- 通信の設定	RFC1271-MIB	vfs:/opt/OV/NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc1271-RFC1271-MIB.mib						
▶ ■ 検出	RFC1315-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc1315-RFC1315-MIB.mib						
▶ 🖿 モニタリング	RIPv2-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc1724-RIPv2-MIB.mib file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc2819-RIMON-MIB.mib file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc4502-RMON2-MIB.mib						
▶ 🖿 インシデント	RMON-MIB							
🦰 ステータスの設定	RMON2-MIB							
🛅 グローバルネットワーク管理	RS-232-MIB	file:///OV/misc/nnm/snmp-mibs/Standard/rfc1659-RS-232-MIB.mib						
▶ 🛅 ユーザーインタフェース	RUGGEDCOM-MIB	file:///var/tmp/rugged/ruggedcom.mib						
セキュリティ セキュリティ	RUGGEDCOM-SYS-INFO-MIB	file:///var/tmp/rugoed/rcsvsinfo.mib						
🔻 🗁 МІВ	PUCCEDCOM TRAPS MIR	file:///var/tmp/rugged-comtrage_mit						
田 ロード済みMIB								
────────────────────────────────────	SMUN-MIB	Tile ///op/2017/misc/nnm/snmp-mios/standard/rfc2613-SMUN-MIB.mib						
III MIB通知	SNMP-FRAMEWORK-MIB	file:///op//UV/misc/nnm/snmp-mibs/standaro/rtc3411-SNMP-rRAME/WORK-MIB.mib						
田 テキスト表記法 日 日	SNMP-REPEATER-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc2108-SNMP-REPEATER-MIB.mib						
III MIBK	SNMP-TARGET-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc3413-SNMP-TARGET-MIB.mib						
	SNMP-VIEW-BASED-ACM-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc3415-SNMP-VIEW-BASED-ACM-MIB.mib						
⊞ ifTypes	SNMPv2-CONF	vfs:/opt/OV/NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc1904-SNMPv2-CONF.mib						
	SNMPv2-MIR	vfs:/ont/OV/NNM/server/lib/oms_mib_model.jar/com/bn/ov/oms/mib/model/hibernate/rfc3418_SNMPv2_MB mib						

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。

SNMP trap(s) from mib module loaded: RUGGEDCOM-TRAPS-MIB. Number of traps: 5. The following traps were added to incident configuration: 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。

- 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。

h	ダッシュボード											
م م	ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー	SNMPトラップの設定 🗙										
	トポロジマップ	3 * 1	5									
Ģ	モニタリング					重複	ν -	Ŧ	ħ	7		
A	トラブルシューティング	名前	▲ SNMPのオブジェクトID	有効にす る	根本 盾因	削除 の有	トの 有効	t	テゴ	ž	作成者	メッセージの形式
	ብንላንትሀ			-		効化	1L	度	ÿ	U L		
2	管理モード											
2	イバリデントの券照	RcVrrpStateChange	.1.3.6.1.2.1.46.1.3.0.1	~	-	-	-			URRP	HP Network No	RC VRRP State Change on group Id \$2
		letfVrrpStateChange	.1.3.6.1.2.1.68.0.1	×	-	-	-	\triangle	*	URRP	HP Network No	IETF VRRP State Change on ipAddress
<i>)</i> #	NJ7-4JX30	SiteScopeAlertEventv1	.1.3.6.1.4.1.11.15.1.4.0.1	~	-	-	-	0	*	-	HP SiteScope	Alert "\$.1.3.6.1.4.1.11.15.1.3.1.2" was tr
go	統合 モジュールの設定	SiteScopeAlertEventv2	.1.3.6.1.4.1.11.15.1.4.1	~	-	-	-	8	*	5	HP SiteScope	Alert "\$.1.3.6.1.4.1.11.15.1.3.1.2" was tr
Je	2. 設定	ArcSightEvent	.1.3.6.1.4.1.11937.0.1	-	-	-	-	0	*	B	HP ArcSight	\$.1.3.6.1.4.1.11937.1.46.1
	🛅 通信の設定	NetScoutServerAlarm	.1.3.6.1.4.1.141.50.2.0.1	~	-	-	-	A	0		HP Network No	NetScout Server Alarm: Threshold \$3; V
	▶ ▶ 検出	NetScoutServerClear	.1.3.6.1.4.1.141.50.2.0.3	~	-	-	-	0	0		HP Network No	NetScout Clear Alarm
		genericTrap	.1.3.6.1.4.1.15004.5.1	~	-	-	-	Ø	Þ		カスタマー	genericTrap
	▼ 屋 インシテント ■ インシデントの設定	powerSupplyTrap	.1.3.6.1.4.1.15004.5.2	~	-	-	-	0	17	1	カスタマー	powerSupplyTrap
	■ SNMPトラップの設定	swUpgradeTrap	.1.3.6.1.4.1.15004.5.3	~	-	-	-	0	Þ	1	カスタマー	swUpgradeTrap
	III Syslogメッセージの設定	cfgChangeTrap	.1.3.6.1.4.1.15004.5.4	~	-	-	-	0	17	1	カスタマー	cfgChangeTrap
	Ⅲ 管理イベントの設定	cfgChangeNoRevTrap	.1.3.6.1.4.1.15004.5.5	~	-	-	-	0	17	1	カスタマー	cfgChangeNoRevTrap
	囲 Pairwiseの設定	fanBankTrap	.1.3.6.1.4.1.15004.5.6	~	-	-	-	0	Þ		カスタマー	fanBankTrap
	🛅 カスタム相関の設定	hotswapModuleStateChangeT	.1.3.6.1.4.1.15004.5.7	~	-			0	b	1	カスタマー	hotswapModuleStateChangeTrap
	▶ 🖿 トラップサーバー 🎦 ステータスの設定	weakPasswordTrap	.1.3.6.1.4.1.15004.5.8	~	-	-	-	0		1	カスタマー	weakPasswordTrap

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 ー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。

メモ:

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。

メモ

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。

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。

[インシデント] > [管理イベントの設定] をクリックします。

[NodeDown] インシデントをダブルクリックします。

Network Node Manager i	ファイル(F) ビュー(V) ツール(T) ア	'クション <mark>(</mark> c) ヘルプ(H)				
山 ダッシュボード		1						
♂~ インシデントの管理	管理イベントの設定 🗙							
▲ トポロジマップ	C * 🖷 3	🕤 🔥 🖀						
🖵 र=२ग्र///			有効に	重複削除の有効	レートの有効	重	カテ	773
▲ トラブルシューティング	▲名町	SNMPのオフジェクトID	する	化	1L	大度	1	IJ~
弓 わべオリ								
☆ 管理モード	NnmClusterStartup	.1.3.6.1.4.1.11.2.17.19.2.	~	-	-	0		10 ノー
Q インシテントの参照	NnmClusterTransfer	.1.3.6.1.4.1.11.2.17.19.2.	~	-	-	\bigcirc		10 ノー
🖋 Cisco IPテレフォニー	NnmHealthOverallStatu	.1.3.6.1.4.1.11.2.17.19.2.	× .	-	-	0		ИИ ВУ
💉 Acme IPテレフォニー	NodeDeleted	.1.3.6.1.4.1.11.2.17.19.2.	-	-	-	0	Þ	10 ノー
🖋 Nortel IPテレフォニー	NodeDown	.1.3.6.1.4.1.11.2.17.19.2.	×	•	~	8	≭	追ノー
💉 Avaya IPテレフォニー	NodeOrConnectionDow	.1.3.6.1.4.1.11.2.17.19.2.	~	•	-	⊗	*	1-
🖋 Microsoft IPテレフォニー	NodePaused	.1.3.6.1.4.1.11.2.17.19.2.	-	-	~	8	*	10 ノー
💋 MPLS	NodePoweredDown	.1.3.6.1.4.1.11.2.17.19.2.	-	•	~	⊗	*	10 ノー
🖋 IPマルチキャスト	NodeTraffic	.1.3.6.1.4.1.11.2.17.19.3.	×	-	-	8		Traffic
💋 Quality Assurance	NodeUnmanagable	.1.3.6.1.4.1.11.2.17.19.2.	-	-	~	۸	*	10 ノー
🖋 トラフィック分析	NonSNMPNodeUnresp	.1.3.6.1.4.1.11.2.17.19.2.	~	-	-	8	*	10 ノー
♀ 統合モジュールの設定	NortellSetStatusUnregis	.1.3.6.1.4.1.11.2.17.19.3.	~	-	-	۸	*	IPT
▶ 設定	PIMInterfaceNotInServi	.1.3.6.1.4.1.11.2.17.19.3.	~	-	-	8	*	PIMイン
 ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー	PIMInterfac eNotNormal	1.1.3.6.1.4.1.11.2.17.19.3.	~	-	-	▲	*	マルチョ
🛅 インシデントの設定	PIMInterfaceTransient	.1.3.6.1.4.1.11.2.17.19.3.	×	-	-	\triangle	*	PIMイン
田 SNMPトラップの設定	PIMNeighborInconsister	.1.3.6.1.4.1.11.2.17.19.3.	~	-	-	8	*	PIMイン
🌐 Syslogメッセージの設定	PIMNeighborInvalid	.1.3.6.1.4.1.11.2.17.19.3.	v	-	-	$\boldsymbol{\Delta}$	*	РІМИХ
■ 管理イベントの設定	更新日時: 15/11/25 10:53	3:47 午前						合

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 粩 アイコンをクリックします。

ファイル(F) ビュ	ー(V) ツール(T) アクショ	ン(c) ヘルプ(H	+) ユーザー名: system NNMiロール: 管理者	サインアウト
管理イベントの設定: 【2】 【 2】 【 2】	★ 管理イベントの設定 * ★ 1<			
 有効にする カテゴリ ファミリー 重大度 インシデントメッセージ 	 ✓ 降害 ノード 危険域 ▼ ジがインシデントビューに表示される方 	 ■ ■<th>く ノードの設定 抑制 強化 ダンブニング 重複削除 レート アクション インシデントライフサイクルの任意の時点で自動的に実行するアクションを設定します。たとえば、インが生成(塗益)されるときに、自動的にトラブルチケットを開き、電子メールを送信するか、ネットワーグ ターに連絡できます。NNMilt、Jythonファイル、実行可能ファイル、またはスクリプトのアクションとし をサポートします。 注:設定済みのアクションは、有効にする1をクリックしてこのフォームを保存するまで無効になります。</th><th>> マ ノシデント クオペレー ての実行</th>	く ノードの設定 抑制 強化 ダンブニング 重複削除 レート アクション インシデントライフサイクルの任意の時点で自動的に実行するアクションを設定します。たとえば、インが生成(塗益)されるときに、自動的にトラブルチケットを開き、電子メールを送信するか、ネットワーグ ターに連絡できます。NNMilt、Jythonファイル、実行可能ファイル、またはスクリプトのアクションとし をサポートします。 注:設定済みのアクションは、有効にする1をクリックしてこのフォームを保存するまで無効になります。	> マ ノシデント クオペレー ての実行
す。メッセージにイン3 用します。有効なパラ ら、これらの変数を選 * メッセージの形式	ッデント情報を含めるには、S(variable メータのセットまたはカスタムインシラ 択します。詳細は、ここをクリックして・	e_name) を使 Fント属性か ください。	 有効にする ライフサイクルの移行アクション ★ ■ ② ◆ 章 K ← □- 0表示中、合計0行 →) 	H 🗊
ノート停止中 説明 このインシデントは、 折によってノードがイ	NNMのAdvanced Problem Analyz 尊止中であると判断したことを示します ているスピームの100% が習ばまで除い	erが次の分 f。1)このノ h) つつ	▲ラ コマンドのタイプ コマンド	
- Filalの当(られ マシンにインストー) なくとも2つの隣接ラ 問題があると報告し * 作成者	ているアドレスの100%か到達小能、 しされているSNMPエージェントが応答 「パイスが到達可能であり、このノード ています。 カスタマー	かっ2) 200 \$しない。少 への接続に	合計:0 選択済み:0 フィルター:オフ 自動リフレッ?	シュ: オフ

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。

ファイル(F) ビュー(V) ツール(T) アクション(c) ヘル ライフサイクルの参行アクション * × ② 『 『 『 』 』 ② 章	レブ(H)			
(i)最上位のフォームが保存されるまで、変更はコミットされません!				
▲ 指定したライフサイクル状態にインシデントが変更されたときに実行す る、Java Jythonファイル、実行可能ファイル、またはスクリプトを入力し ます。そのそれぞれに、インシデントの属性値をパラメータとして渡すこ とができます。[ヘルプ] → [ライフサイクルの移行アクションフォームの 使用法]を参照してください。	ペイロードフィルター マイロードフィルター り、アクションを実行 しく定義できます。^ (cia/alue)に基さい	・ によって、操作に参け したり、pairwiseに参 くイロードフィルターで って受信インシデントを	加するインシデント、たと 5加したりするインシデン 1は、カスタムインシデン 5選択します。詳細は、2	たば抑制、強化、ダンブニングされた トの選択に使用するフィルターをより詳 ト属性の名前 (ciaName)と値 ここをクリックしてくたさい。
* ライフサイクル状態 登録済み ▼ * コマンドのタイプ ScriptOrExecutable ▼	フィルターエディタ 属性	演算子	値	
שעקב	ciaName	▼ !=	•	追加
/var/opt/OV/shared/nnm/actions/writelog.ovpl				挿入 置換
	現在フィルターが定う	義されていません。		追加 ▼ AND OR NOT EXISTS NOT EXISTS

図 58: 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。

ファイル(F) ビュー(V) ツール(T) アクション(c) ヘル	ブ(H)	ユーザー名: system NNMiロール: 管理者 サインアウト
管理イベントの設定 🗶	管理イベントの設定 * ¥ 図 2 音		
▼ 基本		. .	く ノードの設定 抑制 強化 ダンブニング 重複削除 レート アクション > ~
インシデントのトラブルシュ	- ティング の詳細は、 ここをクリックしてくださ		•
L ¹ .			インシデントライフサイクルの任意の時点で自動的に実行するアクションを設定します。たとえば、インシデント
24.45	NedeDavie	1	が生成 (登録)されるときに、自動的にトラブルチケットを開き、電子メールを送信するか、ネットワークオペレー
名前	NodeDown	1	ターに連絡できます。NNMiは、Jythonファイル、実行可能ファイル、またはスクリプトのアクションとしての実行
SNMPオブジェクトID (OIE))属性は、OIDの最後に指定する必要がある	3	をサポートします。
1文子のワイルドカード(*) は 13614以降のの回	を受け付けよ 9 。NNMI Cは、ワイルトガート でのみ有効です (プライベート MIB)、詳細け		は、恐定这番のマクションは「広効にする」をクリック」アニのフォットを保存するまで無効にかります。
ここをクリックしてください。		ŕ	生成にする 「
SNMPのオブジェクトID	.1.3.6.1.4.1.11.2.17.19.2.0.32		- ライフサイクルの移行アクション
有効にする		- 1	
* += 111			* 薈 ② 勺 章
- 75-10			▲ラ コマンドのタイプ コマンド
* ファミリー	७ म 💽 🖬 🚽		■. ScrintOrEvecutable /var/ont/O\//shared/nnm/actions/writelog.ovpl
* 五十 庄	全 隐拉 —		
- 里入版			
インシェントメッセージがス	いいゴントビューにまませれる方法を指定しま		
す。メッセージにインシデン	小情報を含めるには、S(variable name)を使		
			谷計:1 選択済み:0 フイルター:オフ 自動リフレッシュ:オフ

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。

Network Node Manager i	ファイル	(F)	ビュー(V) ツ	∽ル(T)	アクション(c)	ヘルプ(H)						
山山 ダッシュボード	47214 14	1										
ℴ≁ インシデントの管理	解决演	解決済みの更要なインジテント 業										
▲ トポロジマップ	S.		0 5 K	Ĩ								
■ モニタリング	重大 優	先ライ	▼最後の発生日時	割り当て先	ソースノード	ソースオブジェク	カテ	ファニチ	生相	ミテナント	メッセージ	
	🛛 🕄 5,	<u>ີ</u> ດ	11/12/15 4:26:55 PM	4	R5	UDP Jitter Probe		Qua 🖥	b 😼	I		Positive jitter is high from the destination to the
	😣 5.	<u>ີ</u> ດ	11/12/15 4:26:55 PM	1	R5	UDP Jitter Probe		Qua 📲	5 😼	I I		Negative jitter is high from the source to the d $\boldsymbol{\varepsilon}$
- 言 インベントリ 	🙆 5.	ເທ	11/12/15 4:26:55 PM	4	R5	UDP Jitter Probe		Qua 🗒	a 💑	1		Positive jitter is high from the source to the dea
☆ 管理モード	0.		11/12/15 4·26:55 PM		R5	UDP litter Probe		Qua 🗏	h 🗸			High round trip time for the QA Probe LIDP Litte
Q インシデントの参照			11/12/15 4:25:44 PM	4	allinone	allinone		ila H		Default T	e Local	Node Down
=====================================			11/12/15 4:25:40 PL		D5	DNS Test		0		Dendeler		OA Prohe DNS Test failed to run. Reason: Ons
	S 5		11/12/13 4.23.40 Ph		RJ RJ	DNS TEST			9 🔼			CA Probe Divo rest failed to full. Reason. Ope
	▲ 5	1 65	11/12/15 4:25:40 PM	1	R5	UDP Echo Probe	*	Qua T	9 🔼			QA Probe UDP Echo Probe has returned an er
田 未解決の根本原因インシテント	🛛 🕴 5	n	11/12/15 4:25:40 PM	4	R5	UDP Echo Probe	*	Qua 🖥	3 😼	1		QA Probe UDP Echo Probe is in Disabled state
田 サービスインパクトインシデント 一	😣 5.	1 Q	11/12/15 4:25:19 PM	4	PE1SIM4619	TCP Connect to		Qua 📲	s 🔬	Default T	e Local	High round trip time for the QA Probe TCP Con



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。

ファイル(F) ビュー(V) ツール(T) アクション(c) ヘルブ(H)		
重要な未解決インシデン	 ・ × ・ × ・ × ・ × 		
 基本 メッセージ インタフェース停止中 		 全般 相関関係の親 ● 詳細 名前 	相関関係の子 カスタム属性 診断 登録 InterfaceDown
* 重大度 * 優先度 * ライフサイクル状態	 た映知 	カテゴリ ファミリー 発生元 相関特性	障害 マ インタフェース NNMi 根本原因
ソー スノード ソー スオブジェクト	1つ選択してくたさい <u> 登録済み n</u> 進行中 完了	重複数 RCAアクティブ 相関の注	0
割り当て先 注 	解決済み	最初の発生日時 最後の発生日時	2015/11/16 16時 33分 27秒 CST 2015/11/16 16時 33分 27秒 CST
		元の発生日時	2015/11/16 16時 33分 27秒 CST

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。

C 🗃 🚠 🖪 C 🕏 🛛 X 🗉 Q Q

・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
 し変わります。



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.hpe.com で入手できる『HPENetwork 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。

メモ:

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。



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。
- [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。

ノードグループ 🗶 ノードグループ* X	
♂ ♂ ₾	
 ● 基本 各前 Subnet A ステータスの計算 ステータス ステータスなし ビューフィルターリストに 注 Nodes with management IP addresses in the rage of 	 デバイスフィルター 追加のフィルター 追加のノード 子ノードグループ ステータス weまたはnot ike演算子を使用する場合、*(アスタリスク)は文字列内の0以上の文字に一致し、?(疑問符)は文字列内の1文字に一致します。ホスト名の有効な例: cisco?.hp.com. cisco*.hp.com. *cisco*.hp.com. ftc??gs??.*.hp.com 包括的なIPアドレス範囲を作成するには、between演算子を使用します。有効な例: hostedIPAddress between 10.10.1.1 AND 10.10.1.255 詳細は、ここをクリックしてください。
ノードグループは、デバイスフィルター、追加のフィルター、追加のノード、および子 ノードグループを使用してフィルターリングすることができます。デバイスフィルター および追加のフィルターを使用する場合、ノードがこのノードグループに属するに は、少なくとも 1つのデバイスフィルター仕様 および 追加のフィルター仕様と一致す る必要があります。追加のノードおよび子ノードグループとして指定されるノード は、いつであこのノードグループのメンバーです。[ヘルプ] → [ノードグループフォ ー ムの使用法] を参照してくたさい。 ノードグループ定義をテストするには、[ファイル] → [保存]。[アクション] → [ノード グループの詳細] → [メンバーのブレビュー (現在のグループのみ)] を選択してくた さい。	届性 演算子 値 mgmtlPAddress ▼ between ▼ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
 NNM iSPI Performance NNM iSPI Performance for MetricsおよびNNM iSPI for Traffic で使用。 フィルターリストに追加 	NOT EXISTS 削除



2. 次に、Data Center ノードグループを作成します。

ノードグループ 🗱 ノードグループ* X								
♂ ♂ □ □ □ □ □								
▼ 基本	デバイスフィルター 追加のフィルター 追加のノード 子ノードグループ ステータス							
 名前 Data Center ステータスの計算 マ ステータス ステータスなし ビューフィルターリストに 送 注 	■ Image: The second seco							
Nodes with a system name beginning with data_center ノードグループは、デバイスフィルター、追加のフィルター、追加のノード、および子 ノードグループを使用してフィルターリングすることができます。デバイスフィルター および追加のフィルターを使用する場合、ノードがこのノードグループに属するに は、少なくとも1つのデバイスフィルター仕様および追加のフィルター仕様と一致す る必要があります。追加のノードおよび子ノードグループとして指定されるノード は、いつでもこのノードグループのメンバーです。[ヘルプ]→[ノードグループフォー ノードグループマス	フィルターエディタ 属性 演算子 値 sysName ▼ like ▼ data_center 挿入 置換 追加 ▼							
ノードグループ定義をテストするには、[ファイル] → [保存]、[アクション] → [ノード グループの詳細] → [メンバーのブレビュー (現在のグループのみ)]を選択してくだ さい。	AND OR sysName like data_center NOT							
 NNM iSPI Performance NNM iSPI Performance for MetricsおよびNNM iSPI for Traffic で使用。 フィルターリストに追加 	CASTS NOT EXISTS 可除 SysName like data_center							

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。

- a. [ノードグループ] フォームで 粩 アイコンをクリックします。
- b. [名前] テキストボックスに「My Important Subnets」と入力します。
- c. [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。

ノードグループ 🗙 ノードグループ* X		
♂ ♂ □ 🖪 🕱 😂 💼		
 を本 名前 My Important Subnets ステータスの計算 ステータス ステータス	デバイスフィルター 追加のフィルター 追加のノード *	子ノードグループ ステータス K ◆ 0-0表示中、合計0行 → SFを展開
および追加のフィルターを使用する場合、ノードがこのノードグループに属するに は、少なくとも 1つのデバイスフィルター仕様 および 追加のフィルター仕様と一致す る必要があります。追加のノードおよび子ノードグループとして指定されるノード		

図 65: ノードグループ: [子ノードグループ] タブ

d. *● 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。

ノードグループの階層 ¥ 図 □ □ □ 図 ()最上位のフォーム/	 ご 倉 第保存されるまで、変更はコミットされません」
 	ノードグ ループを子ノードグ ループ に関連付けます。ノー ノードグ ループは、[親ノードグ ループマップで子を展開]を ードグ ループ全体を表す 単一 のアイコンとして表示されま
す。これは小規模で、再利 ードグループの階層フォー *子ノードグループ 親ノードグループマップ で子を展開	I用可能なノードグループに適用できます。[ヘルプ] → [ノ - ムの使用法]を参照してください。 Subnet A

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

e. [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。

ノードグループ 🗙 ノードグループ* X					
C C D D D C 1					
····································	デバイスフィルター	追加のフィルター	追加のノード	チノードグループ	ステータス
* 名前 My Important Subnets	•				
ステータスの計算 💽 ステータス ステータスなし	* 🖬 🛛 😂	5 🖀		【 ← 1 - 1表示	市中、合計1行 🔶
ビューフィルターリストに Sean	▲名前 Subnot A	親ノード	グループマップ て	「子を展開	
注 ノードグループは、デバイスフィルター、追加のフィルター、追加のノード、および子 ノードグループを使用してフィルターリングすることができます。デバイスフィルター および追加のフィルターを使用する場合、ノードがこのノードグループに属するに は、少なくとも1つのデバイスフィルター仕様 および 追加のフィルター仕様と一致す る必要があります。追加のノードおよび子ノードグループとして指定されるノード は、いつでもこのノードグループのメンバーです。[ヘルプ]→[ノードグループフォー しの使用注する表現してたさい、					

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。

ファイル(F)	ビュー(V) ツール(T)	アクション(c)	ヘルブ((H)			
ノードグルー C *	-7 × Data Center *	💈 マップ (M) Enterpris トラフィック ノードグル) e Unified Co フマップ ノーブの詳細(mmunication	► Is Map ► ►	🛒 /-FØ	ルーブマップ
ステータス	▲名前	Quality A 管理モー	ssurance ^F (t)		• •	り最終変更日	注
Ø	Data Center	~	-	~	2015/11/30	9:56:30	Nodes with a sys
0	Microsoft Windowsシステム	~	-	-	2015/11/06	6 11:02:43	サーバー、デスクト
0	Name	~	-	~	2015/11/26	6 16:06:14	
0	VMware ESXホスト	~	~	-	2015/11/06	3 11:02:43	VMware ESXホス
0	スイッチ	~	~	-	2015/11/06	3 11:02:43	切換えを行なうノー
0	ネット ワーキングインフラストラクチャデ	~	-	-	2015/11/06	5 11:02:43	ネットワーキングイ

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。

- 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)。
- 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。

Network Node Manager i										
山山 ダッシュボード										
ℴ≁ インシテントの管理										
🛔 トポロジマップ										
🖵 モニタリング										
A トラブルシューティング										
言 インベオリ										
☆ 管理モード										
♀ インシテントの参照										
▶ 設定										
🛅 通信の設定	4									
▶ 🛅 検出										
▶ 🛅 モニタリング										
A 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2										
● ステーダスの設定										
 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… 										
■ ■ ノードグルーブマップの設定										
■ メニュー項目										
田 アイコン	Ŧ									

図73:設定:ユーザーインタフェースの設定

 [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。

	⁽) ビュー(V) ツール(T) アクション(c) ヘルプ(H)	
 「クローバル制御 「フォルトのマップ設定	インタフェースの設定 🗶	
 グローバル制御 コンソールタイムアウト 18.00 時間 ▼ デフォルトのマップ設定 ネ デフォルトのマップ設定 マップビューのデフォルト設定を行います。これらの設定 マップビューのデフォルト設定を行います。これらの設定 		
 グローバル制御 コンソールタイムアウト 18.00 時間 ▼ デフォルトのマップ設定 ネ デフォルトのマップ設定 マップビューのデフォルト設定を行います。これらの設定 アンビューのデフォルト設定を行います。これらの設定 		
 コンソールタイムアウト 18.00 時間 ▼ デフォルトのマップ設定 マップビューのデフォルト設定を行います。これらの設定 ア設定] タブを使用して、特定のマップ用に上書 	コーバル制御 デフォルトのマップ設定 線グラフのデフォルト設定	;
 初期ビュー デフォルトインストール ▼ マップビューのデフォルト設定を行います。これらの設定 ひ設定] タブを使用して、特定のマップ用に上書 	ルタイムアウト 18.00 時間 ▼ ・ デフォルトのマップ設定	
・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	- デフォルトインストール ▼ マップビューのデフォルト設定を行います。これらの設定	elt.
* デフォルトの作成者 すべてのノートテーブル ノードテーブル (すべての属性)	トの作成者 すべてのノードテーブル フードテーブル (すべての属性)	}きて
シングルサインオンでNNM ネットワークの概要マップ 修飾ドメイン名に要求を見ダ ノードグループの概要マップ シードグループの概要マップ シノードの最大数 125	ナインオンでNNM ネットワークの概要マップ ソフレッシュ間隔 60.00 ジット マップ ソードグループの概要マップ シュードの最大数 125	
「NNMIコンジ ^{ールを開く」を} ネットワークインフラストラクチャノードグループマップ ルーターノードグループマップ UBLUダイレクトを有効		
CNC シント としん スイッチ ノードグ ループ マップ たしきい値 5 化 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	スイッチノードグループ マップ 見しきい値 5 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	_
未ライセンスの機能を表 クイックアクセスマップフォルダの最後のノードグループ ノードグループマップでソースマップオブジェク 示 なし (プランクビュー) 本	ンスの機能を表 クイックアクセスマップフォルダの最後のノードグループ (***) ノードグループマップでソースマップオブジェク なし (プランクビュー)	7トを
テーブル行のシェーディ	行のシェーディ ニマニ リンジェンドを示 回効にする す す	

図 74: ユーザーインタフェースの設定の保存

3. 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

66 ページ

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にアップグレードした。

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 のマニュアル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。

メモ:

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。

メモ

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。

メモ:

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.hpe.com で入 手できる『Step- by-Step Guide to IncidentManagement』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、HPE Operations Manager (HPE 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「オペレーター用のヘルプ」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。

Net	work Node Manager i	77	イル <mark>(</mark> F	F)	۲a	(V)) ツ	ール <mark>(T)</mark>	アクション(c)	ヘルプ <mark>(H)</mark>							
	ダッシュボード		E 40 +	472.1-1	(2.2)												
مع _{رہ}	インシテントの管理	里子	₹ 4 .★	BH .X	1.72	7 JF	*										
	田 重要な未解決インシデント	S			0	1		Ъ 🗎									
	田 未割り当ての重要な未解決インシデント	重大	優先	51	▼最行	复の第	性日時	割り当て先	ソースノード	ソースオブジェクト	カテ	77	発生	相関	テナント	メッセージ	
	目前の未解決インシデント	8	5 📮	2	15/11	/26 1	0:40:05		10.161.4.3	10.161.4.3	*		Ъ	₽ <u>¥</u> 4	デフォルト	ノード停止中	
		8	5	5	15/11	/16 1	6:33:27		core6509-1	VI16	*	949 6-0	۵	Þ <u>⊼</u> 4	デフォルト	インタフェース停止中	
		8	5 📮	ē,	15/11	/16 1	6:33:27		core6509-1	VI60	*		۵	₽ <u>¥</u> 4	デフォルト	インタフェース停止中	
		8	5	5	15/11	/16 1	6:33:27		core6509-1	√161	*		ъ	₽ <u>⊼</u> 4	デフォルト	インタフェース停止中	
		8	5 📮	5	15/11	/16 1	6:33:27		core6509-1	VI62	*		ъ	₽ <u>¥</u> 4	デフォルト	インタフェース停止中	
		8	5	5	15/11	/16 1	6:33:27		core6509-1	Gi9/42	*		ъ	₽ <u>⊼</u> 4	デフォルト	インタフェース停止中	
		8	5	5	15/11	/16 1	6:33:27		core6509-1	VI17	*		Ъ.	₽ <u>⊼</u> 4	デフォルト	インタフェース停止中	
		8	5	5	15/11	/06 1	1:25:46		core6509-2	VI1	*		1	₽ <u>⊼</u> 4	デフォルト	インタフェース停止中	
	3	€新	日時:	15/1	1/30 0	4:16:1	11 午後								合	it:8	選択済み: <mark>0</mark>
																	-
*	トポロジマップ	•	分析														

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。

Network Node Manager i	ファイル(F)	E	ב−(V)	ツール(T) アクション	(c) ヘルブ	(H)						
山 ダッシュボード												
ℴ≁ インシテントの管理												
🛔 トポロジマップ	C 🛅	C	17 h	Ъ 🗎								
	አ ም-ቆ አ ና	デバネ	5前	ホスト名	管理アドレス	システムのロケーショ	デバイスのプロファイ	SNN				
- 囲 正常域にないノードセンサー	V	🏙 n	nemphis-p1	memphis-p1.% up a 80.0	46.70.20 1422	Memphis, TN	cisco7206	~				
正常域にない物理センサー	8	<u>?</u> n	npls2950-2	mpls2950-2.1c			VMware Virtual Mac					
田 正常域にないシャーシ	<u>A</u>	👯 ip	ov6_vlan5_sw	16.78.56.20	16.78.56.20	FTC	ciscoCat37xxStack	~				
■ 正常域にないカード	8	🤔 с	at2950	cat2950.fc.usa.hp.com			VMware Virtual Mac					
Ⅲ 正常域にない インタフェース	8	<u></u> c	isco2522	cisco2522.fc.usa.hp.com			VMware Virtual Mac					
■ 正常域にないノード	Δ.	‡ c	isco4k2	cisco4k2.fc.usa.hp.com	16.78.56.126	5 upper east compu	cisco4500	~				
■ 正常域にない SNMPエージェント	Δ	site ip	ov6-vlan5-sw3	ipv6-vlan5-sw3.fc.usa.h	16.78.56.18	building 6 North LIT	hp3500-24G-PoEyl	~				
Ⅲ 応答のないアドレス	8	2 5	uecon9	5uecon9.fc.usa.hp.com	16.78.56.95	Secure Console Ser	lantronixSCS3200	~				
# インタフェースのパフォーマンス	8	<u>?</u> h	p2626-1	hp2626-1.fc.usa.hp.com			VMware Virtual Mac					
ヨシャーシ冗長グループ	Ā		apervillepe1	napervillepe1 fc usa hp	16 78 56 21	801 S Washington	cisco2821	7				
Ⅲ カード冗長グループ	-	÷ "		· -· · · ·				Ť				

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「オペレーター用のヘルプ」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、<u>ここ</u>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 10.20

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:



[©] Copyright 2015 Hewlett Packard Enterprise Development LP.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。Hewlett Packard Enterprise 製品とサービスの保証は、当該製品、およびサービスに付随する明示的 な保証文によってのみ規定されるものとします。ここに記載された情報は追加の保証をなすものではありません。 Hewlett Packard Enterprise 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。