Hewlett Packard Enterprise

# HPE Network Node Manager i Software

ソフトウェアバージョン: 10.20

## HPE Network Node Manager i Software—HPE Business Service Management/Universal CMDB トポロジ統合ガイド

およびNNMiとOMiの統合情報

ドキュメントのリリース日 : 2016年7月
ソフトウェアのリリース日 : 2016年7月

# ご注意

## 保証

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。HPE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。

## 制限付き権利

機密コンピューターソフトウェアこれらを所有、使用、または複製するには、HPEが提供する有効なライセンスが必要です。FAR 12.211および12.212に準拠し、商用コンピューターソフトウェア、コンピューターソフトウェアドキュメント、および商用アイテムの技術データは、ベンダーの標準商用ライセンスの下、米国政府にライセンスされています。

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

Oracleライセンスの全文は、NNMiの製品DVDにあるlicense-agreementsのディレクトリを参照してください。

## 著作権



## 商標について

Adobe®は、Adobe Systems Incorporatedの商標です。

Appleは、米国および他の国々で登録されたApple Computer, Inc.の商標です。

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

Google™は、Google Inc.の登録商標です。

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

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

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

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

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

sFlowは、InMon Corpの登録商標です。

UNIX®はThe Open Groupの登録商標です。

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

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

# マニュアル更新

このドキュメントのタイトルページには、次の識別情報が含まれています。

- ソフトウェアーバージョン番号。ソフトウェアーのバージョンを示します。
- ドキュメントリリース日。ドキュメントが更新されるたびに変更されます。
- ソフトウェアリリース日。ソフトウェアのこのバージョンのリリース日を示します。

最近の更新を確認するか、ドキュメントの最新版を使用していることを確認するには、https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword= を参照してください。

このサイトでは、HPパスポートのアカウントが必要です。HPパスポートのアカウントがない場合は、HPパスポートのサインインページで [**アカウントを作成してください** ] ボタンをクリックしてください。

## サポート

HPEソフトウェアサポートWebサイトには、次のアドレスからアクセスしてください。**https://softwaresupport.hpe.com**

このWebサイトでは、製品、サービス、およびHPEソフトウェアが提供するサポートに関する詳細と連絡先の情報を提供します。

HPEソフトウェアサポートでは、お客様にセルフソルブ機能を提供しています。すばやく効率的な方法で、お客様のビジネス管理に必要な対話型テクニカルサポートツールにアクセスできます。サポートの大切なお客様として、サポートWebサイトで次の操作が可能です。

- 興味のあるナレッジドキュメントの検索
- サポート事例と改善要求の送信と追跡
- ソフトウェアーパッチのダウンロード
- サポート契約の管理
- HPEサポートの問合せ先の検索
- 利用可能なサービスに関する情報のレビュー
- 他のソフトウェアーユーザーとの情報交換
- ソフトウェアートレーニングの調査と登録

ほとんどのサポートエリアでは、HPパスポートのユーザーとして登録してサインインする必要があります。また、多くのエリアではサポート契約も必要です。HPパスポートのIDを登録するには、**https://softwaresupport.hpe.com** にアクセスし、[**HPパスポートに登録**] をクリックしてください。

アクセスレベルの詳細については、次のURLにアクセスしてください。
**https://softwaresupport.hpe.com/web/softwaresupport/access-levels**

# 目次

# 概要

HPE Business Service Management (BSM) プラットフォームは、本番アプリケーションの可用性の管理、システムのパフォーマンスモニタリング、インフラストラクチャーのパフォーマンスモニタリング、および障害が発生した場合の積極的な解決に使用するツールです。

BSMのご購入については、HP営業担当者にお問い合わせください。

このガイドで説明する手順に従って、NNMiをHPE Operations Manager i (OMi) と統合することもできます。

この章では、NNMiとBSM/OMi間で使用できる統合を紹介します。内容は以下のとおりです。

- 「NNMiをHPE BSM Operations ManagementまたはOMiと統合する方法の比較」(7ページ)
- 「HPE NNMi–HPE BSM Operations Management統合」(10ページ)
- 「HPOMおよびHPE BSM Operations Managementと統合されるNNMi」(10ページ)
- 「BSMのNNMiの視覚化」(11ページ)

# NNMiをHPE BSM Operations ManagementまたはOMiと統合する方法の比較

「表 1: NNMiとBSM Operations Management/OMiおよびHPOMの統合の比較」(7ページ)に、HPE NNMi—HPE BSM Operations Management統合とHPE NNMi—HPOM統合の比較を示します。

NNMiとBSM Operations Managementの統合の詳細については、「HPE NNMi–HPE BSM Operations Management統合」(10ページ)を参照してください。

NNMiとHPOMの統合の詳細については、『HP Network Node Manager i Software—HP Operations Manager 統合ガイド』を参照してください。

**表 1: NNMiとBSM Operations Management/OMiおよびHPOMの統合の比較**

| 比較項目 | BSM Connectorとの直接統合 | HPOMを介した間接統合 |
|---|---|---|
| 説明テキスト | イベントに説明テキストを含めることはできません。説明テキストを使用できるようにするには、ユーザー定義の説明をURLとして起動するツールを作成します。(このツールの外部ドキュメントを作成する必要があります。)<br><br>BSMが自動モニタリングコンポーネントとともにインストールされている場合、以下の手順を実行できます。<br>1. トラップ条件を表示するSNMPトラップポリシーに、ヘルプテキストが含まれていることを確認します。<br>2. 以下のいずれかのコマンドを使用して、SNMPトラップポリシーをインポートします。 | イベントに説明テキストを含めることができます。 |

**表1: NNMiとBSM Operations Management/OMiおよびHPOMの統合の比較 (続き)**

| 比較項目 | BSM Connectorとの直接統合 | HPOMを介した間接統合 |
|---|---|---|
| | Windowsの場合:<br>• <BSM_Root_Directory>\opr\bin\ConfigExchange.bat -username <username> -password <password> uploadOM -input <policy header file><br>または<br>• <BSM_Root_Directory>\opr\bin\ConfigExchange.bat -username <username> -password <password> -uploadOM -input <dir in which the policy header file is located><br>• 説明:<br>• <username> は、BSMユーザー名です。<br>• <password> は、BSMユーザーのパスワードです。<br>Linuxの場合:<br>• <BSM_Root_Directory>\opr\bin\ConfigExchange -username <username> -password <password> uploadOM -input <policy header file><br>または<br>• <BSM_Root_Directory>\opr\bin\ConfigExchange -username <username> -password <password> -uploadOM -input <dir in which the policy header file is located><br>• 説明:<br>• <username> は、BSMユーザー名です。<br>• <password> は、BSMユーザーのパスワードです。<br>BSM ConnectorのOMエージェントのSNMPトラップポリシーが、BSMサーバーにインポートされます。<br>「HPE NNMi—HPE BSM Operations | |

**表1: NNMiとBSM Operations Management/OMiおよびHPOMの統合の比較 (続き)**

| 比較項目 | BSM Connectorとの直接統合 | HPOMを介した間接統合 |
|---|---|---|
| | ManagementまたはOMi統合の使用法」(41ページ)も参照してください。 | |
| アクション | イベントにオペレーターが起動するアクションまたは自動アクションを含めることができます。これらの目的に対応するツールを作成できます。 | イベントにオペレーターが起動するアクション、自動アクション、またはその両方を含めることができます。 |
| NNMi管理サーバー監視 | BSM Connectorは、イベントフォワーダーとしてのみ機能します。NNMi管理サーバーは監視されません。 | HP Operations AgentおよびポリシーでNNMi管理サーバーを完全に監視することができます。 |
| ポリシー管理 | 複数のNNMi管理サーバーがある環境の場合、NNMi管理サーバーと関連付けられているBSM Connector間でポリシーを手動で交換する必要があります。 | HPE NNMi—HPOM統合のエージェント実装の場合: 複数のNNMi管理サーバーがある環境の場合、NNMiから転送されるイベントのポリシーをHPOMで中央管理できます。 |
| ライセンスコスト | BSM Connectorにはライセンスがないため、ライセンスコストはかかりません。 | HP Operations Agentライセンスでは、NNMi管理サーバーごとにコストが追加されます。 |
| 通信 | BSMでイベントのライフサイクル状態が[解決済み]に変わると、BSM Connectorを介してイベントソースに同期できます。 | • HPE NNMi—HPOM統合のエージェント実装は1方向です。<br>• HPE NNMi—HPOM統合のWebサービス実装では、双方向のイベント処理が可能です。 |

# HPE NNMi–HPE BSM Operations Management統合

HPE NNMi—HPE BSM Operations Management統合では、NNMi管理イベントのインシデントをSNMPv2cトラップとしてBSM Connectorに転送します。BSM Connectorは、NNMiトラップをフィルターし、HPE BSM Operations Managementイベントブラウザーに転送します。アダプタの設定により、どのBSM Operations Managementイベントブラウザーが転送インシデントを受信するかが決まります。Event Management Foundationライセンスがある場合、NNMiイベントはOperations Managementイベントブラウザーに表示されます。Operations ManagementイベントブラウザーからNNMiコンソールにアクセスすることもできます。

HPE NNMi—HPE BSM Operations Management統合で、NNMiが受信するSNMPトラップをBSM Connectorに転送することもできます。

BSM ConnectorはNNMi管理サーバー上にインストールする必要があります。

BSM ConnectorをNNMi管理サーバーにインストールした後で、次のコマンドを実行する必要があります。

Windowsの場合 : **%nnminstalldir%\lbin\changeUser.ovpl**

Linuxの場合 : **/opt/OV/lbin/changeUser.ovpl**

NNMiイベントで、対応するヘルスインジケータが定義されている場合、これらのヘルスインジケータは、BSMアプリケーションの関連するCIのステータス ([サービス稼働状態] や [サービスレベル管理] など) に影響します。

推奨されているようにNorthbound転送を有効にする (`nnmopcexport.ovpl`に`-omi_hi`オプションを使用する) と、HPE BSM Operations Managementイベントブラウザーで表示できるイベントにヘルスインジケータを含めることができます。NNMi-BSMトポロジ同期を有効にした場合、イベントはBSM RTSMインベントリのCIと対応付けられます。詳細については、「ヘルスインジケータ」(41ページ)を参照してください。

詳細については、「HPE NNMi—HPE BSM Operations Management/OMi統合」(34ページ)を参照してください。

# HPE NNMi–OMi統合

NNMiとOMiは、NNMiとHPE BSM Operations Managementの統合と同じ方法で統合できます。

# HPOMおよびHPE BSM Operations Managementと統合されるNNMi

HPOMアクティブメッセージブラウザーおよびBSM Operations Managementイベントブラウザーにインシデントを表示するには、任意の順序で以下の両方を実行します。

- 『HP Network Node Manager i Software - HP Operations Manager統合ガイド』の「HP NNMi—HPOM統合 (エージェント実装)」セクションの説明に従って、HPE NNMi—HPOM統合のエージェント実装を設定します。
- 『BSM - Operations Manager統合ガイド』の説明に従って、BSM Operations ManagementイベントブラウザーとHPOMの統合を設定します。

# BSMのNNMiの視覚化

NNMiとBSMの両方が実行されている環境の場合、2つの製品を適切に統合すると、BSM内で以下の視覚化されたNNMiデータにアクセスできます。

- BSMのMyBSMポータルのNNMiコンポーネント。詳細については、「MyBSMポータル」(52ページ)を参照してください。
- OMiのマイワークスペースポータルのNNMiコンポーネント。
- BSM Operations Managementイベントブラウザーおよび OMiイベントブラウザーのイベントから起動されるNNMiコンソールビュー。詳細については、「HPE NNMi—HPE BSM Operations ManagementまたはOMi統合の使用法」(41ページ)を参照してください。

# HP Universal CMDBとのトポロジ統合

NNMi 10.00以降では、HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合の方法 (この章で説明) を使用することをお勧めします。

HP Universal Configuration Management Database (UCMDB) ソフトウェアには、以下の利点があります。

- 設定および資産管理
- アプリケーションとサポート対象ハードウェア、サーバー、ネットワークインフラストラクチャ間の関係を追跡します。
- 影響モデル化を使用し、変更が行われる前に、インフラストラクチャとアプリケーションに対する変更の徐々に進行する効果を示します。
- 検出された変更履歴によって、実際に計画済みの変更または未計画の変更を追跡します。
- 既存のリポジトリの認識によって、環境の信頼できる共有ビューを得ます。

HPOMiBusiness Service Management (BSM) ソフトウェアでは、本番アプリケーションの可用性の管理、システムのパフォーマンスモニタリング、インフラストラクチャのパフォーマンスモニタリング、および障害が発生した場合の積極的な解決に使用するツールやUCMDBと同じ利点の一部を得られます。

NNMiトポロジをBSMおよびUCMDBに統合する2つの方法のメリットとデメリットについては、『「NNMiとBSM/UMCDBの統合方法の比較」(66ページ).』を参照してください。

BSM、OMiまたはHP UCMDBのご購入については、HP営業担当者にお問い合わせください。

この章には、以下のトピックがあります。



# HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合

HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合では、NNMiトポロジをBSM/OMi Run-time Service Model (RTSM) またはUCMDBデータベースに入力します。NNMiトポロジの各デバイスおよびデバイスコンポーネントは、RTSMまたはUCMDBの設定項目 (CI) として保存されます。BSMまたはUCMDBユーザーおよび統合アプ

リケーションでは、NNMi管理対象レイヤー2ネットワークデバイスとBSM/UCMDB検出対象サーバーおよびホスト元アプリケーションなどの関係を表示できます。

また、統合により、NNMiデータベースに入力されたCIの識別子が保存されます。NNMi管理対象デバイスのCIは以下のように使用します。

- MyBSMポータルのNNMiコンポーネント。詳細については、「MyBSMポータル」(52ページ)を参照してください。
- BSM Real User Monitor (RUM) から使用可能なパスヘルスビュー。詳細については、「HTTPS接続の設定」(54ページ)を参照してください。
- HPE NNMi—HPOM統合のエージェント実装を使用してBSM Connectorを指定することで、HP NNMi–HP BSM Operations Management統合でNNMi管理対象デバイスに関するインシデントがBSM CIと関連付けられます。詳細については、「設定項目のID」(41ページ)を参照してください。
- HPE NNMi—HPOM統合のエージェント実装を使用して、NNMi管理サーバーのHPOMエージェントを指定することで、NNMi管理対象デバイスに関するインシデントをBSM CIに関連付けることができます。詳細については、『HP Network Node Manager i Software-HP Operations Manager統合ガイド』の「設定項目のID」セクションを参照してください。
- RTSMまたはUCMDBによって管理される包括的な関係により、NNMiオペレーターは、サポートされるほかのデバイスおよびアプリケーションでネットワークアクセススイッチインフラストラクチャの障害の影響を確認できます。NNMiオペレーターは、NNMiのインシデントまたはノードを選択し、影響を受けるCIの要求を入力します。

# 値

HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合によって、NNMiはネットワークインフラストラクチャデバイスのステータスと関係情報の信頼できるソースとして使用できるようになります。このトポロジ情報をRTSMまたはUCMDBデータベースに提供することで、統合で変更管理アクティビティ、影響分析、およびイベント報告を実行できるようになり、BSMまたはUCMDBとのその他の統合が可能になります。

# 統合製品

この章の情報は、以下の製品に当てはまります。

- BSMまたはOMi
- UCMDB

  **ヒント:** サポートされるバージョンは、NNMi対応マトリックスにリストされています。

- NNMi 10.20

NNMiとBSM/OMiまたはUCMDBは、別々のコンピューターにインストールする必要があります。NNMi管理サーバーとBSM/OMiゲートウェイサーバーまたはUCMDBサーバーで使用するオペレーティングシステムは、同じでも、異なっていても構いません。

サポートされているハードウェアプラットフォームおよびオペレーティングシステムの最新情報については、すべての製品の対応マトリックスを参照してください。

# ドキュメント

この章では、BSMまたはUCMDBと通信するようにNNMiを設定する方法について説明します。

BSMのドキュメントスイートでは、BSMの機能について詳しく説明しています。UCMDBのドキュメントスイートでは、UCMDBの特徴と機能について詳しく説明しています。ドキュメントスイートは関連製品メディアに含まれています。

# HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合の有効化

**注意:** UCMDBでは、従来の統合方法でNNMiからトポロジデータを取得できます。NNMiでは、この従来の方法やこの章で説明する方法を使用してUCMDBと同時に統合することはできません。従来のUCMDB統合でこのNNMi管理サーバーからデータを取得するように設定されている場合は、その設定を無効にしてからHPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合を有効にしてください。両方のデータベースでNNMiの情報が必要である場合は、以下を両方とも任意の順序で実行してください。

- この章の説明に従って、HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合を設定します。
- UCMDB製品メディアに収録されている『UCMDB データフロー管理ガイド』の説明に従ってBSMとUCMDBの統合を設定します。このマニュアルは、UCMDB製品用の以下のURLから入手することもできます。
  https://softwaresupport.hp.com

**ヒント:** 説明責任と監査を向上させるために、新しいRTSMユーザーを作成して使用します。この統合で作成または更新されたCIでは、`Created By`属性と`Updated By`属性が設定されます。統合で別のユーザーを使用すると、これらの属性はより一般的な`UCMDB:User:admin`ではなく、`UCMDB:User:<integration_user>`に設定されます。新しいRTSMユーザー名では、CIのソースを簡単に識別できます。詳細については、「新しいRTSMユーザーの作成」(68ページ)を参照してください。

NNMi管理サーバーで以下の手順を実行して、NNMiとBSM/OMiまたはUCMDB間の接続を設定します。

1. 前提条件:BSM/OMiまたはUCMDBライセンスとNNMiライセンスがインストールされていることを確認します。詳細については、『BSM Platform Administration Guide』の「License Management Overview」または『UCMDB Installation and Configuration Guide』の「Licensing」を参照してください。
2. オプション。インタフェースのRTSMまたはUCMDBモデルを更新し、MACアドレスよりも分かりやすい名前にインタフェース表示ラベルを設定します。
   a. BSMを使用する場合は、BSMまたはUCMDBユーザーインタフェースで [**CIタイプマネージャー**] ページを開きます (**[管理者] > [RTSM管理] > [モデリング] > [CIタイプマネージャー]**)。

      OMiを使用する場合は、OMiユーザーインタフェースで [**CIタイプマネージャー**] ページを開きます (**[管理] > [RTSM管理] > [モデリング] > [CIタイプマネージャー]**)。
   b. [**CIタイプ**] ペインでインタフェースを選択します (**[構成アイテム] > [インフラストラクチャーエレメント] > [ノードエレメント] > [インタフェース]**)。
   c. 編集ペインの [**デフォルトのラベル**] タブの [**CIタイプ属性**] で [**InterfaceName**] を選択します。
   d. [**CIタイプラベルの定義形式**] で、以下のように形式を設定します。

      ```
      interface_name | mac_address
      ```
3. NNMiコンソールで、[**HPE NNMi–HPE BSM/OMi/UCMDBトポロジの統合設定**] フォームを開きます (**[統合モジュールの設定] > [HP BSM/UCMDBトポロジ]**)。
4. [**統合の有効化**] チェックボックスをオンにし、フォームの残りのフィールドに入力できるようにします。

5. NNMi管理サーバーへの接続情報を入力します。これらのフィールドの詳細については、「NNMi管理サーバー接続」(29ページ)を参照してください。
6. BSMゲートウェイサーバーまたはUCMDBサーバーへの接続情報を入力します。これらのフィールドの詳細については、「BSM/OMiゲートウェイサーバーまたはUCMDBサーバー接続」(30ページ)を参照してください。
7. オプション: 統合から管理対象外のCIと未接続インタフェースを除外する場合は、[**管理対象オブジェクトのみを同期する**] を選択します。
8. オプション: トポロジ同期に含めるCIタイプをより詳細に制御するには、[**その他のオプション**] ボタンを選択します。これらのフィールドの詳細については、「設定項目トポロジフィルター」(31ページ)を参照してください。
9. オプション: BSMで管理するNNMiノードを説明する情報を入力します。これらのフィールドの詳細については、「ノードトポロジフィルター」(31ページ)を参照してください。
10. オプション: [**トポロジ同期間隔 (時間)**] を調整し、完全なトポロジ同期間の間隔を増やします。

    HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合では、CIやCIの関係が変更されるたびにRTSMまたはUCMDBデータベースが継続的に更新されます。ただし、ネットワーク通信の問題や一時的にBSM/OMiまたはUCMDBが使用できなくなることが原因で一部の動的更新が行われない可能性があります。このため、統合では完全なトポロジ同期がデフォルトで24時間ごとに実行されます。ノードCIが5000を超える大規模なインストールの場合、同期間隔を48時間、72時間またはそれ以上に増やすことをお勧めします。
11. [***ルールのバンドル名***] を入力します。これにより、NNMiノードから [**BSM/UCMDBで影響を受けるCIを検出**] 統合アクションを実行するときに影響を受けるCIの特定に使用される一連のルールが定義されます。BSM、OMi、およびUCMDBの影響分析マネージャーでは、一連のルールグループが保持されています。

    これらのルールにより、選択したノードが停止中になるなどのネットワークイベントの影響を受ける可能性のあるCIを判別できます。統合によって使用されるデフォルトのルールグループはNNMiです。

    [**ルールの重大度レベル**] を入力することもできます。これにより、ルールを適用するときの影響分析トリガーの重大度が決まります。
12. フォームの下部にある [**送信**] をクリックします。

    新しいウィンドウにステータスメッセージが表示されます。NNMi管理サーバーへの接続に問題があることを示すメッセージが表示されたら、[**戻る**] をクリックして、エラーメッセージを参考に値を調整してください。

    > **注:** NNMi管理サーバーに接続できず、証明書に問題があると推測される場合は、『NNMi 10.20デプロイメントリファレンス』の「NNMiでの証明書の使用」を参照してください。

13. 同じ初期化ストリング値を使用して、BSM、OMi、またはUCMDBとNNMiの両方でシングルサインオンが設定されていることを確認します。

    UCMDBの初期化ストリング値の設定については、『HP Universal CMDBデプロイメント・ガイド』のConfiguration ManagerとUCMDB間のLW-SSOの有効化に関するセクションを参照してください。

    NNMiの初期化ストリング値の設定については、「HTTPS接続の設定」(54ページ)を参照してください。
14. BSMまたはOMiでNNMiデータを表示するには、「BSMまたはOMiからのNNMiの視覚化の有効化」(65ページ)に示した手順を実行します。
15. BSMを使用する場合は、「MyBSMで使用できるNNMiコンポーネント」(52ページ)や「NNMiへのドリルダウンが可能なエンドユーザー管理レポート」(63ページ)の説明に従って、MyBSMおよびEUMでNNMiデータを表示できます。

    OMiを使用する場合は、マイワークスペースからNNMiデータを表示できます。

    BSMまたはOMiの影響分析ルールの詳細については、BSMコンソールヘルプかOMiオンラインヘルプの **[RTSMガイド] > [モデリング] > [モデリング] > [影響分析マネージャー]** またはUCMDBコンソールヘルプの **[モデリング] > [モデリング] > [影響分析マネージャー]** を参照してください。

# NNMiとBSM、OMi、またはUCMDB間のシングルサインオンの設定

シングルサインオンは、同一の初期化ストリング値を使用し、共通のネットワークドメイン名を共有するすべてのHPエンタープライズアプリケーションで使用できます。

あるユーザーがHP NNMiとHP Business Service Management (HP BSM) でまったく同じユーザー名を使用している場合、そのユーザーはNNMiにログオンしなくても、MyBSMポータルにログオンして、HP NNMiポートレットを表示できます。このシングルサインオン機能では、2つの製品間のユーザー名をマッピングしますが、パスワードはマッピングしません。MyBSMとHP NNMiのログオンパスワードが異なる場合があるためです。また、ユーザーロールもマッピングしないため、ユーザーは各アプリケーションで異なる権限を有することができます。たとえば、あるユーザーが、HP BSMでは通常の権限、HP NNMiでは管理者権限を有する場合があります。

シングルサインオンの詳細については、『NNMiデプロイメントリファレンス』の「NNMiとシングルサインオン (SSO) の使用」を参照してください。

HP BSMまたはOMiからNNMiへのシングルサインオンアクセスを設定するには、両方のアプリケーションで同じ初期化ストリングが使用されていることを確認します。アプリケーションから別のアプリケーションにストリングをコピーして使用できます。使用する初期化ストリングを選択するときは、やり取りするすべてのアプリケーションを考慮します。必要に応じて、他のアプリケーションの初期化ストリング設定も更新します。

### NNMi初期化ストリング

以下のようにして、NNMi初期化ストリングを特定します。

1. テキストエディターで以下のファイルを開きます。
   - Windowsの場合: `%NNM_PROPS%\nms-ui.properties`
   - Linuxの場合: `$NNM_PROPS/nms-ui.properties`
2. ファイルから、以下のようなセクションを特定します。

   ```
   com.hp.nms.ui.sso.isEnabled =
   ```
3. `com.hp.nms.ui.sso.isEnabled`プロパティが`true`に設定されていることを確認します。
4. ストリング`initString`を検索します。

   初期化ストリングは、`initString`パラメーターの値です。引用符は含みません。

   たとえば、`nms-ui.properties`ファイルに以下のテキストが含まれているとします。

   ```
   initString=E091F3BA8AE47032B3B35F1D40F704B4
   ```

   この場合、以下が初期化ストリングです。

   ```
   E091F3BA8AE47032B3B35F1D40F704B4
   ```

   このストリングをコピーします。
5. 「ファイルから、以下のようなセクションを特定します。」(16ページ)に示されている`initString`パラメーターの値を変更する場合、以下のコマンドを実行します。

   ```
   nnmsso.ovpl -reload
   ```

### BSM初期化ストリング

以下のようにして、BSM初期化ストリングを特定します。

1. BSMコンソールで、**[管理] > [プラットフォーム] > [ユーザと権限] > [認証管理]** の順に移動します。
2. [シングル サインオン構成] セクションの [**設定**] をクリックします。シングル サインオン構成 ウィザードが表示されます。
3. シングル サインオン構成 ウィザードで、次のように行います。
   - [**Lightweight**] を選択します。
   - [トークン作成キー] ボックスに、「ファイルから、以下のようなセクションを特定します。」(16ページ)でコピーしたinitStringパラメーターの値を入力します。
   - シングル サインオン構成 ウィザードで他の設定を行うには、BSMオンラインヘルプの指示に従ってください。

### OMi初期化ストリング

以下のようにして、OMi初期化ストリングを特定します。

1. OMiコンソールで、**[管理] > [ユーザ] > [認証管理]** の順に移動します。
2. [シングル サインオン構成] セクションの [**設定**] をクリックします。シングル サインオン構成 ウィザードが表示されます。
3. シングル サインオン構成 ウィザードで、次のように行います。
   - [**Lightweight**] を選択します。
   - [トークン作成キー] ボックスに、「ファイルから、以下のようなセクションを特定します。」(16ページ)でコピーしたinitStringパラメーターの値を入力します。
   - シングル サインオン構成 ウィザードで他の設定を行うには、OMiオンラインヘルプの指示に従ってください。

# SNMPエージェントのソース文字エンコードを正しく行うためのNNMiの設定

UCMDBとBSM/OMiトポロジでのノード調整は、多くの場合、異なるデータプロバイダーから提供される値の文字列照合に依存します。場合によっては、NNMiがBSM/OMi/UCMDBに送信する値の最後にnullバイトが含まれることがあります。[インタフェースの説明] の値はその一例です。

これにより、他のデータプロバイダーから提供されたデータと完全一致しなくなり、オブジェクト調整で問題が発生します。[インタフェースの説明] の値にこれらの文字が含まれるのは、NNMiがSNMPエージェントからのOCTET STRING値をデフォルトでUTF-8文字でエンコードするのに対し、SNMPエージェントはISO-8859-1文字エンコードなどの他の文字エンコードでデータを戻すためです。

SNMP OCTET STRINGデータは、nms-jboss.propertiesファイルのcom.hp.nnm.sourceEncodingプロパティで定義された文字エンコードに基づいて解釈されます。

SNMPエージェントの場合に予期されるソース文字エンコードが正しく行われるようにNNMiを設定するには、nms-jboss.propertiesファイルで文字セットエンコードの設定を行う必要があります。

たとえば、com.hp.nnm.sourceEncodingのプロパティ値をISO-8859-1,
UTF-8に設定し、以下のようにSNMP OCTET STRINGデータを正しく解釈します。

1. nms-jboss.propertiesファイルを開きます。
   Windowsの場合：%NNM_PROPS%\nms-jboss.properties
   Linuxの場合：$NNM_PROPS/nms-jboss.properties
2. 以下の行を含むテキストブロックを探します。
   #!com.hp.nnm.sourceEncoding=UTF-8
3. 行を以下のように編集します。
   com.hp.nnm.sourceEncoding=ISO-8859-1, UTF-8

**注：** ISO 8859-1は、ソース文字エンコードが競合する可能性があるー例にすぎません。ソースエンコードでは、異なる環境では異なる値にすることが必要になる場合もあります。

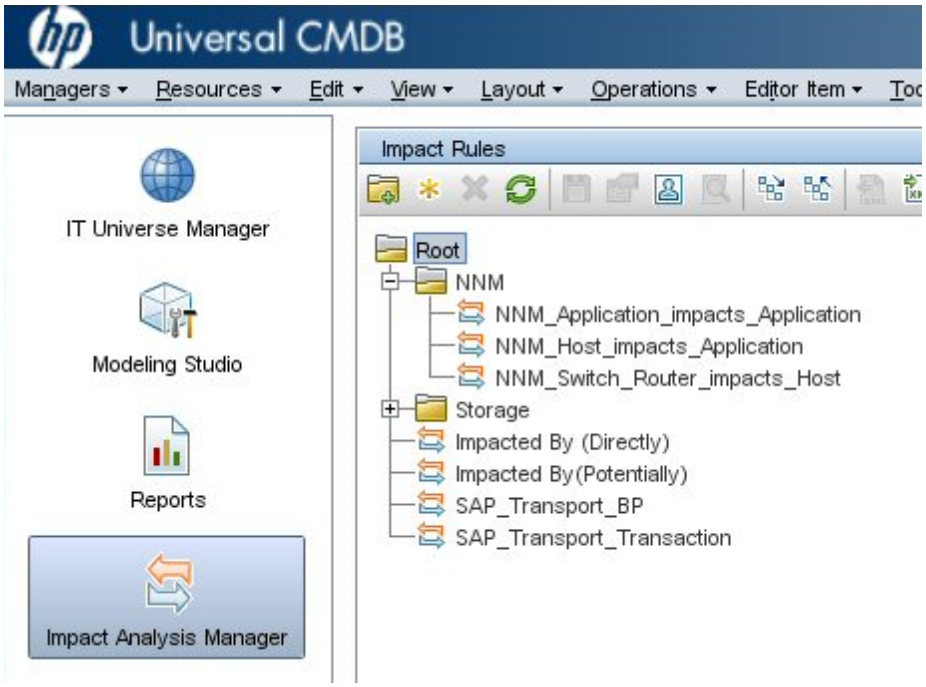
詳細については、『NNMiデプロイメントリファレンス』の「NNMiの文字セットエンコードの設定」を参照してください。

# BSM/OMi/UCMDBで影響を受けるCIを検出する機能の有効化

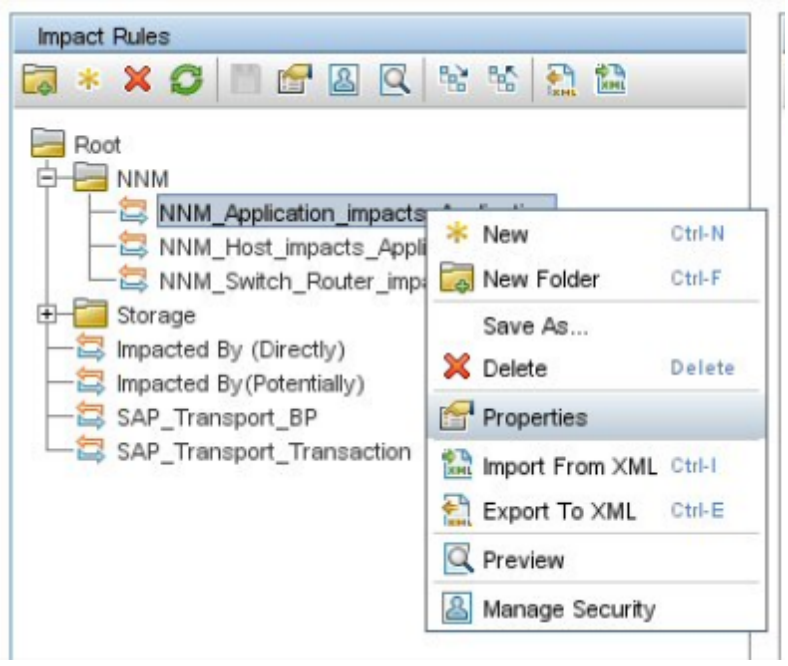
NNMi-BSM統合での[**BSM/UCMDBで影響を受けるCIを検出**]機能を有効にするには、以下のように[**影響分析マネージャー**]を使用して、NNMiによって提供されるルールをNNMiルールバンドルに追加する必要があります。

**注**:NNMi-BSM統合を有効にするときにデフォルトの[**NNMi**]ルールバンドルを選択し、以下の手順の説明に従って[**影響分析マネージャー**]を使用して提供されるルールをNNMiルールバンドルに追加しないと、CIのセットが空になります。

1. [**影響分析マネージャー**]をクリックします。
2. [**影響ルール**]ペインで、[**Root/NNM**]フォルダーに移動します。

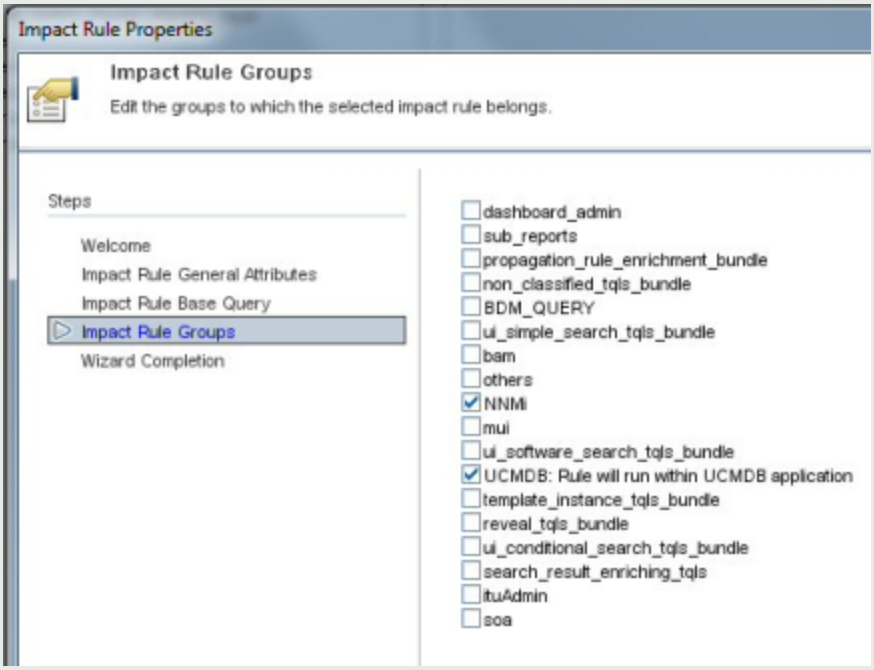



3. リストにあるルールごとに、以下の手順を実行します。
   a. ルールを右クリックし、[**プロパティ**] を選択します。




   b. [**プロパティ**] ウィザードで、[**次へ**] をクリックします。
   c. [**影響ルールグループ**] に移動します。
   d. [**NNMi**] をクリックします。

**ヒント:** [**NNMi**] ルールバンドルが表示されない場合は、まず「HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合の有効化」(14ページ)の説明に従ってNNMi-BSM統合を有効にしてください。




# HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合の使用法

HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合により、BSM RTSMまたはUCMDBデータベースに以下のCIタイプが入力されます。

- InfrastructureElement > Node

  NNMiトポロジのノード。「ノードトポロジフィルター」(31ページ)に記載されているようにノードを制限できます。
- InfrastructureElement > NodeElement > Interface

  統合によってデータが入力されるノードCIに関連付けられたインタフェース。
- InfrastructureElement > NetworkEntity > IpAddress

  統合によってBSM、OMi、またはUCMDBにデータが入力されるノードCIに関連付けられたインタフェースのIPアドレス。
- InfrastructureElement > NodeElement > HardwareBoard

  統合によってBSMまたはUCMDBにデータが入力されるノードCIに関連付けられたカード。

  **注:** HP NNMi–HP UCMDB統合では、これらのシャーシ要素がホストポートとしてUCMDB/RTSMにレポートされます。RTSM/UCMDBには、これらのシャーシ要素がハードウェアボードとして表示されます。これは、NNMiのシャーシ要素とUCMDB/RTSMのCIのシャーシを区別するために行われます。
- InfrastructureElement > NodeElement > PhysicalPort

統合によってBSMまたはUCMDBにデータが入力されるノードCIに関連付けられたポート。

- InfrastructureElement > NetworkEntity > IpSubnet

  NNMiトポロジのすべてのサブネット。明示的に除外されない限り、すべてのサブネットがRTSMまたはUCMDBデータベースに提供されます。これにより、NNMiトポロジからノードIPアドレスCIが作成されるときにIPアドレスの関係で使用できるようになります。統合からのCIタイプの除外については、「設定項目トポロジフィルター」(31ページ)を参照してください。
- InfrastructureElement > NetworkEntity > Layer2Connection

  統合がノードCIとしてBSMに入力する接続エンドを少なくとも2つ持つNNMi Leyer 2接続。
- InfrastructureElement > NetworkEntity > Vlan

  統合によってBSM、OMi、またはUCMDBにポートCIとして入力されるポートを1つ持つNNMi VLAN。

BSM/OMi RTSMで作成されたCIごとに、統合によってNNMiデータベースにRTSM識別子またはUCMDBグローバルIDが保存されます。

**ヒント:** デフォルトでは、NNMiはエンドノードを検出しません。NNMiの検出とモニタリングの設定を更新し、BSM、OMi、またはUCMDBで確認する必要があるエンドノードが含まれるようにしてください。

**ベストプラクティス: NodeRole**属性を使用して、ネットワークデバイスのロールの変更を追跡します。たとえば、デバイスロールがswitchからswitch-routerに変わることがあります。スイッチ、ルーター、サーバーなどのデバイスは、すべてNode CIタイプとして定義されます。デバイスタイプは、Node CIの**NodeRole**属性によって識別されます。**NodeRole**属性は、以下の1つ以上の値に設定されます。

- `hub`
- `load_balancer`
- `printer`
- `router`
- `server`
- `lan_switch`
- `voice_gateway`
- `desktop`

**ヒント:** 1つのノードに複数のノードロールを割り当てることができます。NNMiは、ノードの[**デバイスのカテゴリ**]とノードの機能を使用して、どの**NodeRoles**を設定するかを判断します。

ノードにIP転送機能 (com.hp.nnm.capability、node.ipforwarding) がある場合、NNMiは**NodeRole**を`router`に設定します。ノードにスイッチング機能 (com.hp.nnm.capbility.node、node.lan_switching) がある場合、NNMiは**NodeRole**を`lan_switch`に設定します。

以下の表に、NNMiの**デバイスカテゴリ**と**NodeRole**属性のマッピングを示します。

| NNMiのデバイスカテゴリ | NodeRole属性 |
|---|---|
| ハブ | hub |

| NNMiのデバイスカテゴリ | NodeRole属性 |
|---|---|
| LoadBalancer | load_balancer |
| プリンター | printer |
| ルーター | router |
| サーバー | server |
| スイッチ | lan_switch |
| Switch_Router | router、lan_switch |
| ボイスゲートウェイ | voice_gateway |
| ワークステーション | desktop |

NNMi-BSM/OMiトポロジ統合では、以下の関係が作成されます。

- Membership: **IpSubnet > IpAddress**
- Membership: **Layer2Connection > Interface**
- Composition: **Node > Interface**
- Containment: **Node > IpAddress**
- Composition:**Node > HardwareBoard**
- Composition:**HardwareBoard > HardwareBoard**
- Composition:**HardwareBoard > PhysicalPort**
- Realization: **PhysicalPort > Interface**

NNMiの属性と各CIタイプの対応するCI属性のマッピングについては、「NNMi - CI属性のマッピング」(69ページ)を参照してください。

HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合は、一方向通信でNNMi情報と更新をBSM/OMi RTSMまたはUCMDBデータベースに転送します。NNMiは、BSM CI情報の使用方法を認識していないか管理していないため、統合は、ある一定の期間更新されていないCIを削除する上で、BSM/OMi CIのエージング設定に依存します。

**ヒント:** CIライフサイクルについては (エージングメカニズムの有効化および実行の手順を含む)、BSMヘルプまたはUCMDBヘルプの「CIライフサイクルおよびエージングメカニズム」を参照してください。これらの情報は、BSMコンソールの**[RTSMガイド] > [RTSM管理] > [管理] > [CIライフサイクルおよびエージングメカニズム]**にあります。これらの情報は、UCMDBコンソールの**[管理] > [管理] > [CIライフサイクルおよびエージングメカニズム]** にあります。

ほかの製品がBSMまたはUCMDBと統合すると、HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合によって、それらの製品はNNMiのトポロジ情報を使用できるようになります。

# ネットワークトポロジビュー

BSMのネットワークトポロジビューは、NNMi – UCMDB履歴統合の方法で動作するように設計されています。これは、TQLには**Net Device** CIタイプや**Computer** CIタイプが含まれますが、NNMi - BSMトポロジ統合ではノー

ドが**Node** CIとしてのみ作成されるので、**NodeRole**属性を設定して、デバイスタイプをサーバーやスイッチなどとして識別するためです。

本番環境でビューが更新されるまでに、NNMiによって入力されるネットワークトポロジで動作するようにこれらを簡単に変更できます。以下のセクションでは、RTSM、サービス稼働状態およびOperations Managementでモデリングに合わせてビューを変更する方法について説明します。

# レイヤー2トポロジビュー

以下の2つの図は、NNMiのレイヤー2近隣接続ビューの結果と、BSMの対応するNNMiに基づくレイヤー2ビューの結果の比較です。3番目の図は、NNMi – UCMDB履歴統合の方法を使用したUCMDBのNNMiに基づくレイヤー2ビューを示しており、結果が同じになっています。

**図1: NNMiのレイヤー2近隣接続ビュー**

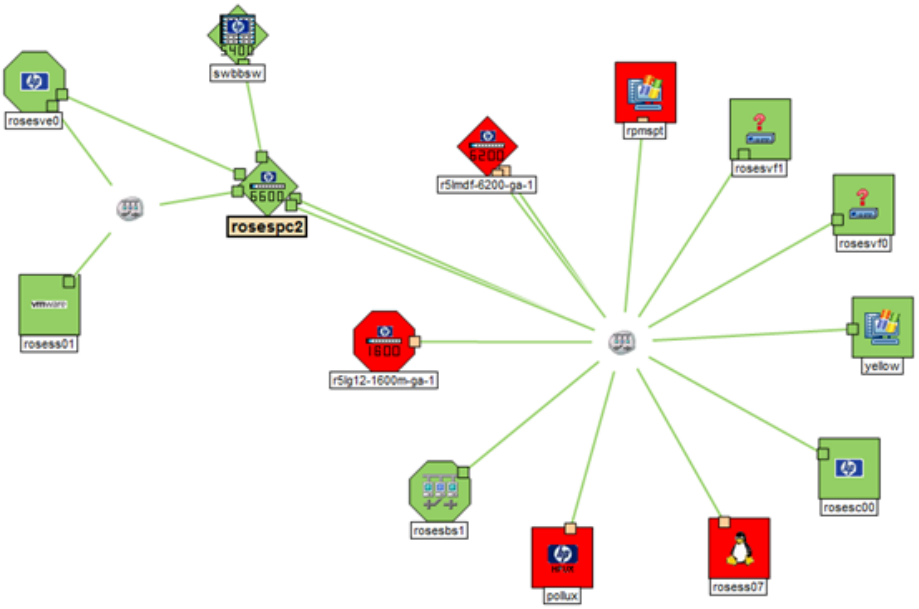


**図2: BSMのNNMiに基づくレイヤー2ビュー**

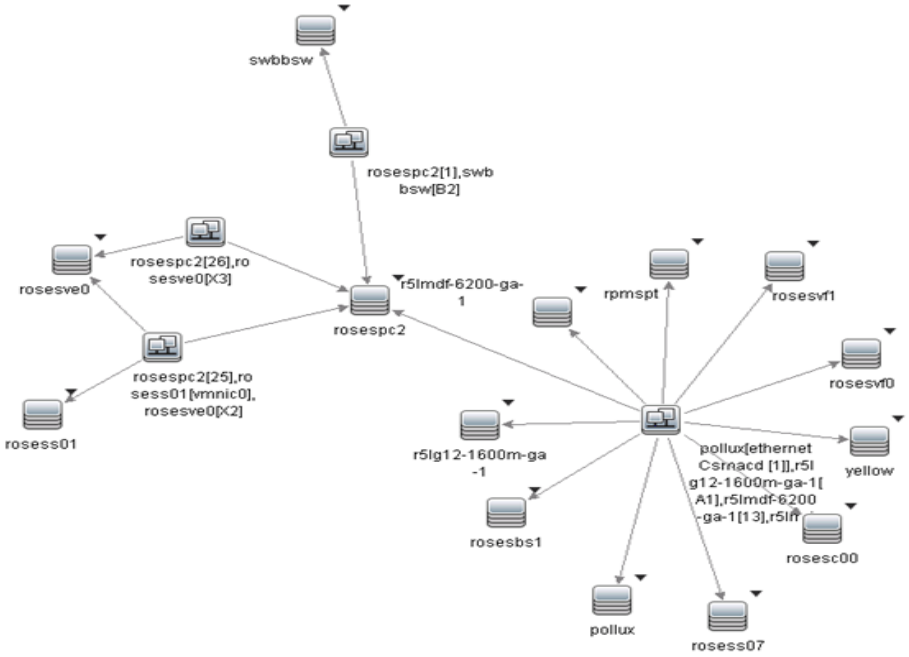
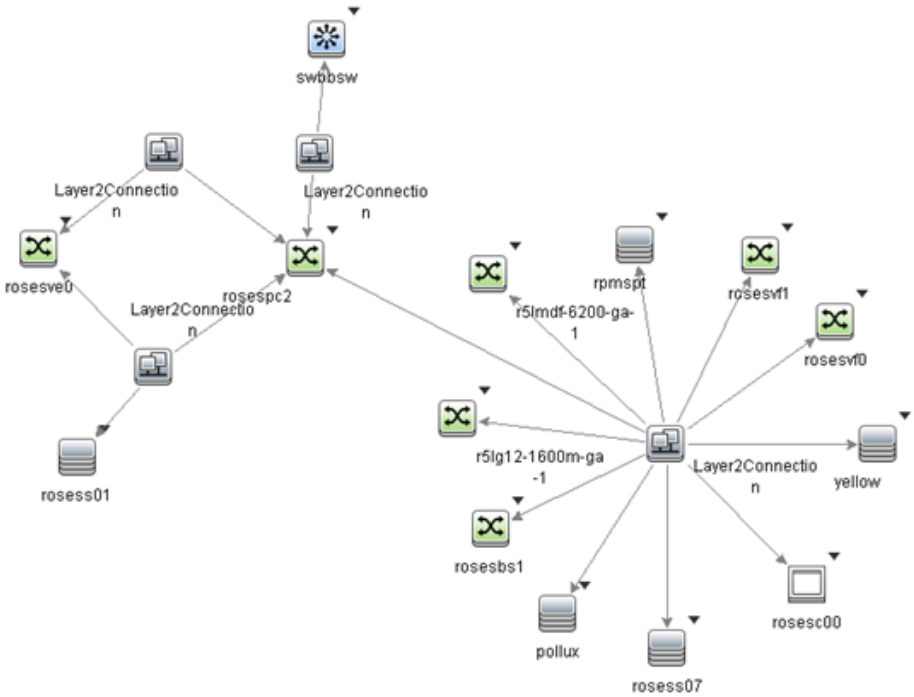



**図3: UCMDBのNNMiに基づくレイヤー2ビュー**




このタイプのビュー (NNMiに基づくレイヤー2) は、主にTBECルールの基盤として使用する場合や、ビューセレクタでOMiイベントをフィルターする場合に便利です。サービス稼働状態での使用には適していません。ネットワークデバイスを含むビューを作成する場合の推奨事項については、「サービス稼働状態ビュー」(26ページ)セクション

を参照してください。ただし、サービス稼働状態でこのビューを表示する場合、ビュー定義プロパティを変更して、バンドルを [**Service_Health**] に設定する必要があります。

OMiイベントをフィルターするためにビュー セレクタで使用されるビューの場合、ネットワークイベントが関連付けられたすべてのCIを含めることができます。NNMiイベントは、**Node**、**Interface**、**Layer 2 Connection**または**IP Address**CIタイプに解決されるため、**IPアドレス**をビューに追加できます。以下の2つの図は、**OBA1**ビジネスアプリケーションに関連付けられたネットワーク要素を含むビューの例を示しています。

**図 4: ビジネスアプリケーションに適用されるレイヤー2トポロジの例**

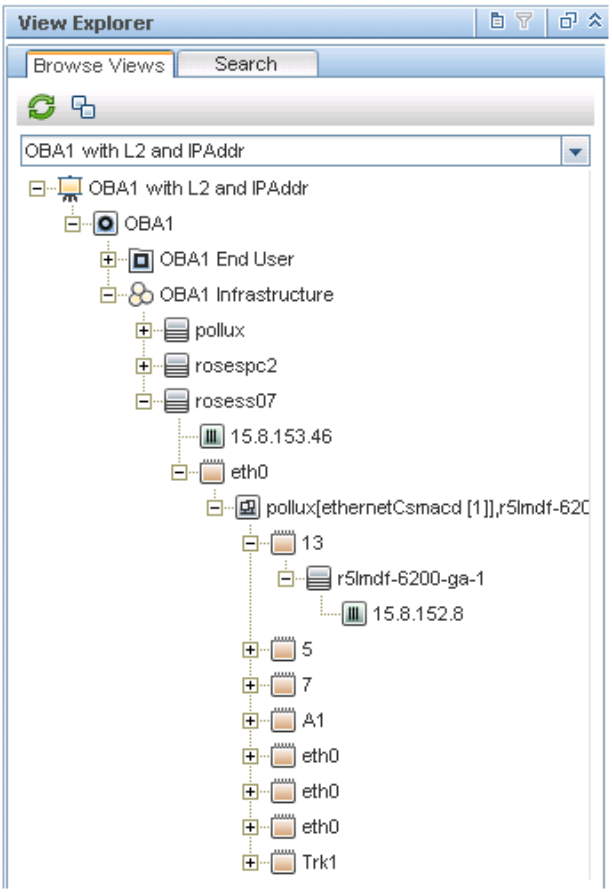
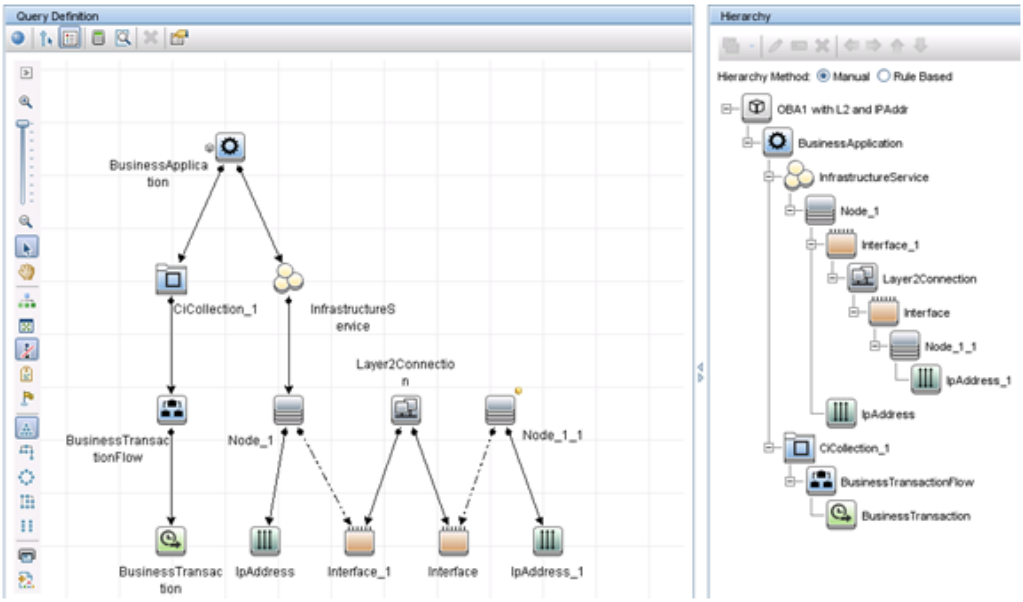


**図5: ビュー定義:**

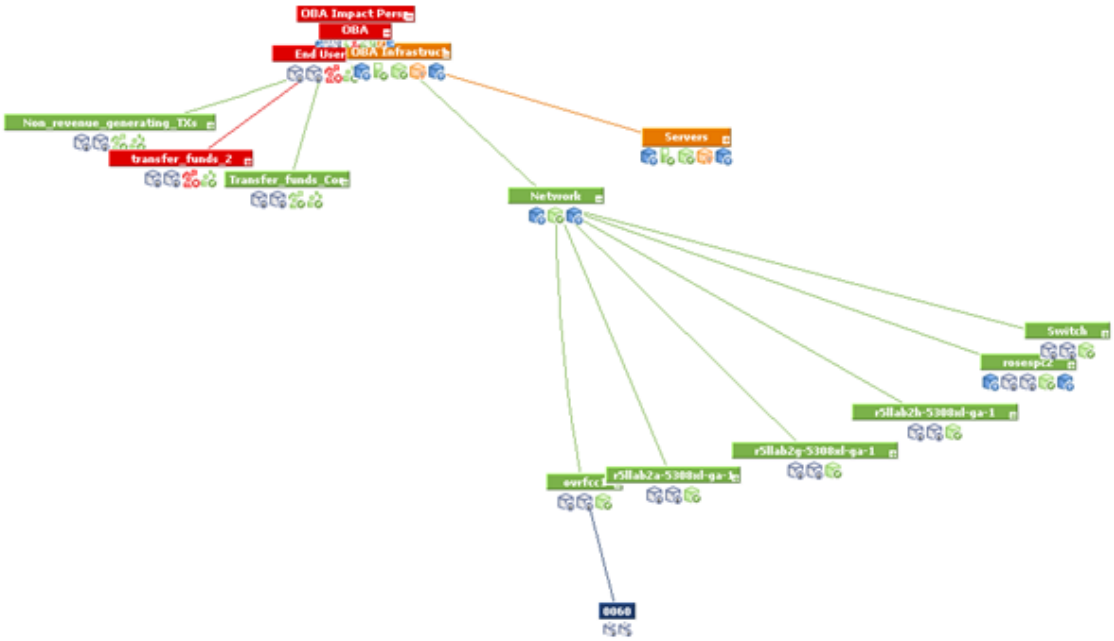



# サービス稼働状態ビュー

従来のネットワークトポロジをサービス稼働状態で表示するのは簡単ではありません。**ノード -> インタフェース -> レイヤー2の接続 -> インタフェース -> ノード**の関係は無意味です。これは、たとえば、レイヤー2の接続とインタフェース間に影響関係 (KPIステータスの伝播) がないためです。

サービス稼働状態ビューにネットワークデバイスを含める必要がある場合、従来のネットワークトポロジを再現するのではなくフラット構造で表示することをお勧めします。インタフェースとノード間に影響関係があるため、場合によっては以下の例のように**ネットワーク**としてグループ化し、**ノード -> インタフェース**を含むビューを作成することも1つの方法です。

**図6: トップビュー:**




## OMi状況パースペクティブ

OMi状況パースペクティブの[**状況トップビュー**]には、選択したイベントの関連CIに基づいてビューが表示されます。デフォルトのビューは、CIの**ビューマッピング**によって決まります。

状況パースペクティブで使用されるデフォルトのビューマッピングは、ノードCIおよびインタフェースCIでは機能しません。

ノードCIの場合、デフォルトの**ビューマッピング**はありません。OMi状況パースペクティブを使用する場合、そのようなビューを定義できます。

インタフェースCITの場合、NetworkInterface_InfrastructureとSystems_Infrastructureのデフォルトのビューマッピングは、Computer CIによって異なります。そのため、NNMiから入力されるノードの場合、これらのビューは失敗します。Computer CIではなくNode CIを使用するように**NetworkInterface_Infrastructure**ビューを変更できます。

# 統合で提供される追加のNNMi機能

HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合では、RTSMまたはUCMDB影響分析マネージャーにアクセスして、ネットワークの機能停止の影響を受ける可能性のあるCIを判別できます。

## NNMiコンソールからのBSM、OMi、またはUCMDB影響分析の実行

HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合では、NNMiコンソールからBSMまたはUCMDBへのリンクが提供されます。

HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合を有効にすると、以下の項目がNNMiコンソールのノードの[**アクション**]メニューに追加されます。

**BSMで影響を受けるCIを検出** — [**HP NNMi-HP BSM/UCMDBトポロジの統合設定**] フォームで設定された重大度のトリガー値でルールグループが適用された後に、BSMまたはUCMDB影響分析マネージャーから返されるCIのリストが表示されます。追加のCIの詳細については、リストされている、影響を受けるCIのいずれかから [**BSMのOpen CI**] を選択し、BSMコンソールまたはUCMDBコンソールでCIの詳細を起動できます。

# HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合設定の変更

1. NNMiコンソールで、[**HP NNMi-HP BSM/UCMDBトポロジの統合設定**] フォームを開きます ([**統合モジュールの設定**] > [**HP BSMトポロジ**])。
2. 該当するように値を変更します。このフォームのフィールドの詳細については、「[HPE NNMi–HPE BSM/OMi/UCMDBトポロジの統合設定] フォームのリファレンス」(29ページ)を参照してください。
3. フォームの上部にある [**統合の有効化**] チェックボックスがオンであることを確認し、フォームの下部にある [**送信**] をクリックします。

**注:** 変更はただちに有効になります。

# HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合の無効化

1. NNMiコンソールで、[**HP NNMi-HP BSM/UCMDBトポロジの統合設定**] フォームを開きます ([**統合モジュールの設定**] > [**HP BSMトポロジ**])。
2. フォームの上部にある [**統合の有効化**] チェックボックスをオフにし、フォームの下部にある [**送信**] をクリックします。統合URLアクションはもう使用できません。

**注:** 変更はただちに有効になります。

# HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合のトラブルシューティング

このセクションでは以下の内容について説明します。



RTSMへの接続に関するトラブルシューティングについては、BSMドキュメントスイートを参照してください。

## BSMユーザーインタフェースでインタフェースラベルがMACアドレスとして表示される

RTSMまたはUCMDBモデルでは、インタフェースラベルとしてインタフェース名よりもMACアドレスがデフォルトで優先されます。BSMコンソールまたはUCMDBコンソールでインタフェース名を表示するには、BSMまたはOMiのコン

ソールかUCMDBコンソールでインタフェースモデルを編集します。

## RTSMの管理対象ノードでCIが重複する

HP Operations ManagerもRTSMと同期している場合は、RTSMの管理対象ノードで重複したCIが表示されることがあります。HPOMで検出されるノードはCIタイプコンピューターであり、NNM iSPI NETで検出されるノードはCIタイプノードです。この重複による製品のパフォーマンスへの影響はありません。

# アプリケーションフェイルオーバーとHPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合

NNMi管理サーバーがNNMiアプリケーションフェイルオーバーに参加する場合、HPE NNMi–HPE BSM/OMi/UCMDBトポロジは、フェイルオーバーの発生後、新しいNNMi管理サーバーホスト名で続行されます。統合のユーザーにフェイルオーバーを意識させないようにしてください。

統合では、BSM/OMiサーバーの自動フェイルオーバーはサポートされません。

# [HPE NNMi–HPE BSM/OMi/UCMDBトポロジの統合設定]フォームのリファレンス

[**HP NNMi-HP BSM/UCMDBトポロジの統合設定**]フォームには、NNMiとBSM、OMi、またはUCMDB間の通信を設定するためのパラメーターが含まれています。このフォームは、[**統合モジュールの設定**]ワークスペースから使用できます。

> **注:** 管理者ロールのNNMiユーザーのみが[**HP NNMi-HP BSM/UCMDBトポロジの統合設定**]フォームにアクセスできます。

[**HP NNMi-HP BSM/UCMDBトポロジの統合設定**]フォームは、以下の領域に関する情報を収集します。

- 「NNMi管理サーバー接続」(29ページ)
- 「BSM/OMiゲートウェイサーバーまたはUCMDBサーバー接続」(30ページ)
- 「ノードトポロジフィルター」(31ページ)

統合設定に変更を適用するには、[**HP NNMi-HP BSM/UCMDBトポロジの統合設定**]フォームの値を更新し、[**送信**]をクリックします。

## NNMi管理サーバー接続

「表2: NNMi管理サーバー情報」(30ページ)に、NNMi管理サーバーへの接続パラメーターを示します。これはNNMiコンソールを開くために使用したのと同じ情報です。これらの値の多くを決定するには、NNMiコンソールセッションを起動するURLを調べます。NNMi管理者と協力し、設定フォームのこのセクションに適切な値を決定します。

**表2: NNMi管理サーバー情報**

| フィールド | 説明 |
|---|---|
| NNMi SSLの有効化 | 接続プロトコル指定。<br>• HTTPSを使用するようにNNMiコンソールが設定されている場合は、[**NNMi SSLの有効化**] チェックボックスをオンにします。<br>• HTTPを使用するようにNNMiコンソールが設定されている場合は、[**NNMi SSLの有効化**] チェックボックスをオフにします。<br>統合では、この指定に基づいてNNMiコンソールに接続するポートが選択されます。 |
| NNMiホスト | NNMi管理サーバーの正式な完全修飾ドメイン名。このフィールドは読み取り専用です。 |
| NNMiユーザー | NNMi Webサービスに接続するためのユーザー名。このユーザーは、NNMi AdministratorまたはWeb Service Clientのロールを持っている必要があります。 |
| NNMiパスワード | 指定のNNMiユーザーのパスワード。 |

# BSM/OMiゲートウェイサーバーまたはUCMDBサーバー接続

「表3: BSMゲートウェイサーバー情報」(30ページ)に、BSM/OMiゲートウェイサーバーまたはUCMDBサーバーに接続してBSM RTSMまたはUCMDBデータベースと通信するためのパラメーターを示します。BSM、OMi、またはUCMDB管理者と協力し、設定のこのセクションに適切な値を決定します。

**注:** 設定フォームのBSMへの参照は、BSMゲートウェイサーバー、OMiゲートウェイサーバー、またはUCMDBサーバーのいずれかに適用されます。

**表3: BSMゲートウェイサーバー情報**

| BSM/OMiゲートウェイサーバーまたはUCMDBサーバーのパラメーター | 説明 |
|---|---|
| BSM SSL有効化 | BSM、OMi、またはUCMDBに接続するための接続プロトコルの指定。<br>• HTTPSを使用するようにBSM、OMi、またはUCMDBが設定されている場合は、[**BSM SSLの有効化**] チェックボックスをオンにします。<br>• HTTPを使用するようにBSM、OMi、またはUCMDBが設定されている場合は、[**BSM SSLの有効化**] チェックボックスをオフにします。<br>• NNMi管理サーバーに接続できず、証明書に問題があると推測される場合は、『NNMi 10.20デプロイメントリファレンス』の「NNMiでの証明書の使用」を参照してください。 |
| BSMホスト | BSMゲートウェイサーバー、OMiゲートウェイサーバー、またはUCMDBサーバーの完全修飾ドメイン名。 |
| BSMポート | BSMまたはUCMDBに接続するためのポート。 |

**表3: BSMゲートウェイサーバー情報 (続き)**

| BSM/OMiゲートウェイサーバーまたはUCMDBサーバーのパラメーター | 説明 |
|---|---|
| | デフォルトのBSM設定を使用する場合は、デフォルトのhttpポート (BSMの場合は80、UCMDBの場合は8080) を使用します。<br>BSMおよびUCMDBのデフォルトのhttpsポートは443です。 |
| BSM RTSMユーザー | BSM RTSMまたはUCMDB管理者のユーザー名。 |
| BSM RTSMパスワード | BSM RTSMまたはUCMDB管理者のパスワード。<br>BSM RTSM管理者は、BSM管理者ではなく内部RTSMのRTSM管理者です。BSM管理者は、管理者ロールを使用してRTSMユーザーを設定する必要があります。詳細については、「新しいRTSMユーザーの作成」(68ページ)を参照してください。 |

# 設定項目トポロジフィルター

HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合では、デフォルトでノードに関する情報およびその他のいくつかのNNMiトポロジ項目に関する情報 (IPサブネット、インタフェース、IPアドレス、カード、ポート、レイヤー2接続、VLANなど) が入力されます。次のセクションで説明する [ノードトポロジフィルター] フィールドを使用して、入力される一連のノードを設定します。ほかのCIタイプの場合、[**HP NNMi-HP BSM/UCMDBトポロジの統合設定**] フォームの [**その他のオプション**] ボタンを選択し、RTSMまたはUCMDBデータベースに入力しないCIタイプを選択解除します。たとえば、トポロジの何千もの未接続インタフェースをNNMiでモニタリングしている場合があります。この情報をRTSMまたはUCMDBデータベースに入力すると、同期時間が長くなり、マップが複雑になる可能性があります。この情報がRTSMまたはUCMDBデータベースで必要ない場合、統合から除外しても問題ありません。

一部のCIタイプはその他のCIタイプの存在に依存しています。たとえば、VLANでは、関連するポートを認識している必要があります。このため、一部のCIタイプは、必要な依存CIタイプが選択されていないと選択できません。

# ノードトポロジフィルター

デフォルトでは、HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合により、NNMiトポロジ内のすべてのノードとノードのサブコンポーネント (省略可能) に関する情報がBSMまたはUCMDBに伝達されます。BSM内のNNMiノードトポロジ情報のサブセットのみを統合が管理するようにする必要がある場合は、このセクションの説明に従って、ノードグループ (省略可能) を1つまたは両方指定します。

以下の例は、NNMiトポロジ情報のフィルタリングを説明しています。

- 限定フィルター — NNMiで、すべてのNNMiノードがBSM RTSMまたはUCMDBデータベースに含まれるように明示的に定義したノードグループを1つ作成します。この方法では、ネットワークトポロジに関する専門性の高い知識が必要です。

  たとえば、以下のデバイスの種類を含むBSM-Topologyというノードグループを作成したとします。

  - 管理対象環境のアプリケーションサーバー
  - アプリケーションサーバーを接続するルーターとスイッチ

この場合、ノードグループ(この例ではBSM_Topology)をトポロジフィルターノードグループとして指定します。追加の接続ノードグループを指定しないでください。

統合は、指定されたトポロジフィルターノードグループ(この例ではBSM_Topology)のすべてのノードに関する情報を転送し、NNMiトポロジ内のほかのすべてのノードを無視します。

- 追加フィルター—NNMiで、モニタリング対象ネットワークのコアインフラストラクチャを定義するノードグループを指定(または作成)し、そのエンドノードを定義する別のノードグループを作成します。

  たとえば、以下のNNMiノードグループを作成したとします。

  - ネットワーキングインフラストラクチャデバイスノードグループとその他の主要接続デバイスを含むBSM_Coreグループ
  - 管理対象ネットワークのアプリケーションサーバーを含むBSM_End_Nodesグループ

  この場合、最初のグループ(この例ではBSM_Core)をトポロジフィルターノードグループとして指定します。また、2つ目のノードグループ(この例ではBSM_End_Nodes)を追加の接続ノードグループとして指定します。

  統合は、トポロジフィルターノードグループ(この例ではBSM_Core)のすべてのノードに関する情報を転送します。次に、追加の接続ノードグループ(この例ではBSM_End_Nodes)の各ノードを以下のように調べます。

  - ノードがトポロジフィルターノードグループの1つ以上のノードに接続されている場合、統合はそのノードに関する情報をBSM、OMi、またはUCMDBに転送します。
  - ノードがトポロジフィルターノードグループのノードに接続されていない場合、統合はそのノードを無視します。

「表4: ノードトポロジフィルターの情報」(32ページ)は、ノードトポロジフィルターを指定するためのオプションパラメーターをリストし、これらのパラメーターに入力する値を説明しています。

**表4: ノードトポロジフィルターの情報**

| ノードトポロジフィルターのパラメーター | 説明 |
|---|---|
| トポロジフィルターノードグループ | BSMに挿入する一連のプライマリノードを含むNNMiノードグループ。統合により、このノードグループのすべてのノードに関する情報がRTSMまたはUCMDBデータベースに入力されます。<br>NNMiで[**ノードグループ**]フォームの[**名前**]フィールドに記述されているとおりに(引用符または追加文字は含みません)ノードグループの名前を入力します。<br>トポロジフィルターノードグループを指定しない場合、HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合により、NNMiトポロジ内のすべてのノードとインタフェースがRTSMまたはUCMDBデータベースに入力されます。この場合、統合は、[**追加接続ノードグループ**]フィールドの値を無視します。 |
| 追加接続ノードグループ | BSMまたはUCMDBに入力する追加ノードのヒントを含むNNMiノードグループ。統合により、このノードグループの中から、トポロジフィルターノードグループ内の1つ以上のノードに接続された(NNMiトポロジ内の)ノードのみに関する情報がRTSMまたはUCMDBデータベースに入力されます。<br>NNMiで[**ノードグループ**]フォームの[**名前**]フィールドに記述されているとおりに(引用符または追加文字は含みません)ノードグループの名前を入力します。<br>トポロジフィルターノードグループを指定し、さらに追加接続ノードグループを指定した場合、HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合は、トポロジフィルターノー |

**表4: ノードトポロジフィルターの情報 (続き)**

| ノードトポロジフィルターのパラメーター | 説明 |
| --- | --- |
| | ドグループのノードとインタフェースに関する情報と追加接続ノードグループの接続ノードに関する情報を転送します。<br><br>トポロジフィルターノードグループを指定し、追加接続ノードグループを指定しない場合、HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合は、トポロジフィルターノードグループのノードとインタフェースに関する情報のみを転送します。<br><br>トポロジフィルターノードグループを指定しない場合、HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合により、NNMiトポロジ内のすべてのノードとインタフェースがRTSMに入力されます。この場合、統合は、[**追加接続ノードグループ**]フィールドの値を無視します。 |

# HPE BSM Operations ManagementおよびOMi

HPE Business Service Management (BSM) プラットフォームおよびOMiのOperations Managementには、包括的なイベント管理、先を見越したパフォーマンス監視、および管理オペレーティングシステム、ミドルウェア、およびアプリケーションインフラストラクチャを対象とした自動アラート、レポート、およびグラフ作成機能が備わっています。HPE NNMi—HPE BSM Operations Management/OMiは広範囲のソースから1つのビューにイベントを統合します。

BSMやOMiのご購入については、HP営業担当者にお問い合わせください。

この章には、以下のトピックがあります。



# HPE NNMi—HPE BSM Operations Management/OMi統合

HPE NNMi—HPE BSM Operations Management/OMi統合では、NNMi管理イベントのインシデントをSNMPv2cトラップとしてBSM Connectorに転送します。BSM Connectorは、NNMiトラップをフィルターし、HPE BSM Operations Managementイベントブラウザーに転送します。アダプタの設定により、どのBSM Operations Managementイベントブラウザーが転送インシデントを受信するかが決まります。

HPE NNMi—HPE BSM Operations Management/OMi統合で、NNMiが受信するSNMPトラップをBSM Connectorに転送することもできます。

BSM ConnectorはNNMi管理サーバー上に存在する必要があります。

HPE NNMi—HPE BSM Operations Management/OMi統合では、BSM Operations ManagementまたはOMiのイベントブラウザーからNNMiコンソールにアクセスできます。

**ヒント:** この章では、NNMiと、BSM Operations ManagementまたはOMiのイベントブラウザーとの間の直接統合について説明します。NNMiとBSM Operations Managementを統合する方法の比較については、「NNMiをHPE BSM Operations ManagementまたはOMiと統合する方法の比較」(7ページ)を参照してください。

HPE NNMi—HPE BSM Operations Management統合は、NNMi Northboundインタフェースの特定の実装です。これについては『NNMiデプロイメントリファレンス』の「NNMi Northboundインタフェース」の章で説明されています。

HPE NNMi—HPE BSM Operations Management/OMi統合は以下のコンポーネントで構成されます。

- nnmi-hpomエージェント統合モジュール
- nnmopcexport.ovplツール

# 値

HPE NNMi—HPE BSM Operations Management/OMi統合では、ネットワーク管理、システム管理、およびアプリケーション管理の各ドメインのイベントをBSM Operations ManagementまたはOMiのイベントブラウザーで統合できるため、BSM Operations ManagementまたはOMiのイベントブラウザーユーザーは潜在的なネットワーク問題を検出および調査できます。

統合の主要な機能は以下のとおりです。

- NNMiからBSM Connectorへの自動インシデント転送。転送されたインシデントはBSM Operations ManagementまたはOMiのイベントブラウザーに表示されます。
- BSM Operations ManagementまたはOMiのイベントブラウザーからNNMiコンソールへのアクセス。
  - 選択したイベントのコンテキストでNNMiの [**インシデント**] フォームを開きます。
  - 選択したイベントおよびノードのコンテキストでNNMiビュー (たとえば、レイヤー2の近隣接続ビュー) を開きます。
  - 選択したイベントおよびノードのコンテキストでNNMiツール (たとえば、ステータスポーリング) を起動します。

# 統合製品

この章の情報は、以下の製品に当てはまります。

- HP Operations Managementライセンスを含むBSM

  または

  HP Operations Manager i (OMi)

  > **ヒント:** サポートされるバージョンは、NNMi対応マトリックスにリストされています。

- NNMi 10.20 (WindowsまたはLinuxオペレーティングシステムのみ)

NNMiとBSM/OMiは、別々のコンピューターにインストールする必要があります。NNMi管理サーバーとBSM/OMiサーバーのコンピューターで使用するオペレーティングシステムは、同じでも、異なっていても構いません。

BSM Connectorは、NNMiのインストール後にインストールする必要があります。BSM ConnectorはNNMi管理サーバー上に存在する必要があります。NNMiとBSM Connector間のレイテンシが高くなるといったネットワークの問題を避けるために、BSM ConnectorはNNMi管理サーバーコンピューターにインストールすることをお勧めします。

サポートされているハードウェアプラットフォームおよびオペレーティングシステムの最新情報については、すべての製品の対応マトリックスを参照してください。

# ドキュメント

この章では、BSM Operations ManagementまたはOMiのイベントブラウザーと通信するようにNNMiを設定する方法について説明します。

BSMドキュメントでは、BSM Operations Managementイベントブラウザーから NNMiコンソールにアクセスするBSM Connectorとアプリケーションのインストール方法と使用方法を説明します。

- BSMアプリケーション管理ガイド
- BSM Connector Installation and Upgrade Guide
- BSM Connector User Guide
- BSM Connector Help
- BSM Operations Management Extensibility Guide

OMiドキュメントでは、OMiイベントブラウザーからNNMiコンソールにアクセスするBSM Connectorとアプリケーションのインストール方法と使用方法を説明します。

- OMiユーザーガイド
- OMi管理ガイド
- OMi拡張性ガイド

BSM ConnectorをNNMi管理サーバーにインストールした後で、次のコマンドを実行する必要があります。

Windowsの場合 : **%nnminstalldir%\lbin\changeUser.ovpl**

Linuxの場合 : **/opt/OV/lbin/changeUser.ovpl**

# HPE NNMi—HPE BSM Operations Management/OMi統合の有効化

HPE NNMi—HPE BSM Operations Management/OMi統合を有効にする手順は、経験のあるBSM Connectorユーザーが実行することを推奨します。

**注 :** NNMiをHPE Business Service Management (BSM)トポロジデータベースと統合すると、HPE NNMi—HPE BSM Operations Management/OMi統合では、NNMi管理対象デバイスに関するインシデントをBSM設定項目 (CI) に関連付けることができます。この情報は、標準のNNMi Northboundインタフェースでは使用できません。詳細については、「設定項目のID」(41ページ)を参照してください。

HPE NNMi—HPE BSM Operations Management/OMi統合を有効にするには、以下の手順を実行します。

1. NNMi管理サーバーで、NNMiが転送するトラップのSNMPトラップポリシーファイルを生成します。
   a. NNMiサービスが実行中であることを確認します。

      ```
      ovstatus -c
      ```

      すべてのNNMiサービスで、[実行中] 状態が表示されます。
   b. 以下のコマンドを入力して、SNMPトラップポリシーファイルを生成します。

      ```
      nnmopcexport.ovpl -u <username> -p <password> \
      -template "NNMi Management Events" -application "NNMi" \
      -omi_policy -omi_hi
      ```

      **<username>** と **<password>** の値は管理者ロールを付与されたNNMiコンソールユーザーに対応します。

      このコマンドにより、現在のディレクトリにファイルが2つ作成されます。

      - <UUID>_dataファイルはSNMPトラップポリシーファイルです。<UUID> はユニバーサルに一意なIDです。

- <UUID>_header.xmlファイルは、BSM Connectorに対して<UUID>_dataファイルを示します。

**注意:** これらの出力ファイルの名前を変更すると、BSM Connectorで使用不能になります。

SNMPトラップポリシーファイルには、各管理イベントのポリシー条件と現在のNNMiインシデント設定でのSNMPトラップ設定が含まれています。このコマンドの出力のカスタマイズについては、nnmopcexport.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。

デフォルトのポリシー条件および条件のカスタマイズの詳細については、「HPE NNMi—HPE BSM Operations ManagementまたはOMi統合の使用法」(41ページ)を参照してください。

c. NNMiの重大度情報を転送する場合 (「オプション。(HP Operations Agent 11.12以降の場合のみ) さらに、NNMiの重大度をBSMに転送するようにエージェントを設定します。」(38ページ)を実行する場合)、以下のコマンドを実行します。

Windowsの場合:

a. **findstr /V SEVERITY** <UUID>**_data > <UUID>_data_new**

b. **robocopy /mov** <UUID>**_data_new** <UUID>**_data**

Linuxの場合:

a. **grep -v SEVERITY** <UUID>**_data > <UUID>_data_new**

b. **mv** <UUID>**_data_new** <UUID>**_data**

2. BSM Connectorをインストールおよび設定します。

**注:** BSM ConnectorをNNMi管理サーバーにインストールした後で、次のコマンドを実行する必要があります。

Windowsの場合: **%nnminstalldir%\lbin\changeUser.ovpl**

Linuxの場合: **/opt/OV/lbin/changeUser.ovpl**

a. NNMi管理サーバーまたは別のサーバーで、『BSM Connector Installation and Upgrade Guide』の説明に従って、BSM Connectorをインストールします。

b. BSM/OMiで、『BSMアプリケーション管理ガイド』または『OMi管理ガイド』の説明に従って、BSM/OMiとのBSM Connector統合を設定します。

**ヒント:** HPOMのHP Operations AgentとBSM Connectorを1つのシステムで同時に実行できます。詳細については、『BSM Connector User Guide』を参照してください。

c. BSM Connectorユーザーインタフェースを使用して、この手順の「NNMi管理サーバーで、NNMiが転送するトラップのSNMPトラップポリシーファイルを生成します。」(36ページ)で作成したヘッダーファイルとポリシーファイルをインポートします。

詳細については、『BSM Connector Help』の「Working with BSM Connector」>「Policy Management」>「How to Import Policies」を参照してください。

d. BSM Connectorユーザーインタフェースを使用して、新しいポリシーをアクティブにします。

詳細については、『BSM Connector Help』の「Working with BSM Connector」>「Policy Management」>「How to Activate and Deactivate Policies」を参照してください。

3. NNMiとBSM Connectorとの間のSNMP通信に使用可能なポートを指定します。

BSM Connectorは、NNMiがこのポートに転送するSNMPトラップをこのポートで待機します。統合を有効化する間、この手順の「BSM Connectorがインストールされているサーバーで、以下のコマンドを入力することにより、BSM Connector内部のエージェントでNNMiからSNMPトラップを受信するカスタムポートを設定します。」(38ページ) (BSM Connector用) と「NNMi管理サーバーで、BSM ConnectorへのNNMiインシデント転送を設定します。」(38ページ) (NNMi用) の両方でこのポート番号を使用します。

**ヒント:** SNMP通信ポートは、インストール後にBSM Connector設定ウィザードで指定した、Apache TomcatサーバーのHTTP/HTTPSポートとは異なります。

BSM ConnectorをNNMi管理サーバーにインストールする場合、このポート番号は、NNMiがSNMPトラップを受信するときのポートとは別にする必要があります。以下のように使用可能なポートを特定します。

a. NNMi管理サーバーから、**nnmtrapconfig.ovpl -showProp**コマンドを実行します。コマンド出力で、`trapPort`の現在の値を探します。通常、この値は162です。これは、SNMPトラップを受信する標準的なUDPポートです。NNMiとBSM Connectorとの間でSNMP通信を設定するときには、この`trapPort`の値を使用しないでください。

b. NNMiとBSM Connectorとの間のSNMP通信を設定するためのポートを選択します。`trapPort`の値に似たポート番号を使用することを推奨します。たとえば、ポート162が使用可能でなければ、ポート5162で試してください。

c. NNMi管理サーバーから**netstat -a**コマンドを実行し、その出力から「NNMiとBSM Connectorとの間のSNMP通信を設定するためのポートを選択します。trapPortの値に似たポート番号を使用することを推奨します。たとえば、ポート162が使用可能でなければ、ポート5162で試してください。」(38ページ)で選択したポートを検索します。出力でそのポート番号が見つからない場合は、BSM Connectorで使用できると考えられます。

4. BSM Connectorがインストールされているサーバーで、以下のコマンドを入力することにより、BSM Connector内部のエージェントでNNMiからSNMPトラップを受信するカスタムポートを設定します。

   a. エージェントを設定します。

      HP Operations Agent 11.00以降を使用している場合:

      ```
      ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> \
      -set SNMP_SESSION_MODE NETSNMP
      ```

      11.00より古いバージョンのHP Operations Agentを使用している場合:

      ```
      ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> \
      -set SNMP_SESSION_MODE NNM_LIBS
      ```

   b. オプション。(HP Operations Agent 11.12以降の場合のみ) さらに、NNMiの重大度をBSMに転送するようにエージェントを設定します。

      ```
      ovconfchg -ns eaagt.integration.nnm -set OPC_SNMP_SET_SEVERITY TRUE
      ```

      **注:** HP Operations Agent 11.12以降を使用している場合にのみ、NNMiインシデントの重大度をBSM Operations Managementに転送できます。これよりも低いバージョンのHP Operations Agentを使用している場合は、この手順をスキップします。

   c. エージェントを再起動します。

      ```
      ovc -restart opctrapi
      ```

   `<custom_port>`には、この手順の「NNMiとBSM Connectorとの間のSNMP通信に使用可能なポートを指定します。」(37ページ)で指定したポートを使用します。

5. NNMi管理サーバーで、BSM ConnectorへのNNMiインシデント転送を設定します。

a. NNMiコンソールで、[**NNMi–HPOMの統合選択**] フォーム ([**統合モジュールの設定**] > [**HPOM**]) を開きます。

b. [**HPOMエージェントの実装**] をクリックして、次に [**新規作成**] をクリックします。

(使用可能な転送先を選択してある場合、[**リセット**] をクリックして、[**新規作成**] ボタンを使用可能にしてください。)

c. [**NNMi–HPOMエージェントデスティネーション**] フォームで、[**有効にする**] チェックボックスをオンにして、フォームの残りのフィールドを使用可能にします。

d. BSM Connectorへの接続情報を入力します。トラップ送信先ポートは、この手順の「NNMiとBSM Connectorとの間のSNMP通信に使用可能なポートを指定します。」(37ページ)で指定したポートです。

これらのフィールドの詳細については、「BSM Connector接続」(48ページ)を参照してください。

e. 送信オプションを指定します。[**NNMiコンソールアクセス**] フィールドから [**HTTP**] オプションを選択します。

これらのフィールドの詳細については、「BSM Operations ManagementまたはOMi統合コンテンツ」(49ページ)を参照してください。

f. フォームの下部にある [**送信**] をクリックします。

新しいウィンドウにステータスメッセージが表示されます。設定に問題があることを示すメッセージが表示されたら、[**戻る**] をクリックして、エラーメッセージを参考に値を調整してください。

6. オプション。BSMゲートウェイサーバーで説明テキストを使用可能にするには、以下の手順を実行します。

BSM/OMiはMonitoring Automationと一緒にインストールされている必要があります。

a. トラップ条件を表示するSNMPトラップポリシーに、ヘルプテキストが含まれていることを確認します。

b. 以下のいずれかのコマンドを使用して、SNMPトラップポリシーをインポートします。

- Windowsの場合:

```
<BSM_Root_Directory>\opr\bin\ConfigExchange.bat -username <BSM_username> -
password <password> -uploadOM -input <policy_header_file>
```

または

```
<BSM_Root_Directory>\opr\bin\ConfigExchange.bat -username <BSM_username> -
password <password> -uploadOM -input <directory_containing_policy_header_file>
```

- Linuxの場合:

```
<BSM_Root_Directory>/opr/bin/ConfigExchange -username <BSM_username> -password
<password> -uploadOM -input <policy_header_file>
```

または

```
<BSM_Root_Directory>/opr/bin/ConfigExchange -username <BSM_username> -password
<password> -uploadOM -input <directory_containing_policy_header_file>
```

BSM/OMiユーザーには、BSM RTSMまたはUCMDBの管理者権限が必要です。

BSM ConnectorのエージェントのSNMPトラップポリシーが、BSM/OMiサーバーにインポートされます。

# 対応するBSMイベントの解決後にインシデントを解決するためのNNMiの設定

対応するイベントがHPE BSM Operations Management/OMiで解決した後でNNMiインシデントを自動的に解決するようにNNMiを設定できます。

1. NNMi管理サーバーで次のコマンドを実行します。

   Windowsの場合: **%nnminstalldir%\bin\nmsconfigurebacksync.ovpl**

   Linuxの場合: **/opt/OV/bin/nmsconfigurebacksync.ovpl**

   ユーザー名とパスワードの入力を求められたら、管理者権限のあるNNMiユーザーの資格証明を指定します。
2. Windowsのみ: 以下のコマンドを%ovinstalldir%ディレクトリから実行します。
   **newconfig\HPNmsCommon\scripts\nnm-configure-perl.ovpl -source newconfig\HPNmsCommon\perl\a -target nonOV\perl\a**
3. 次のコマンドを実行して、ombacksyncプロセスを再起動します。

   **ovc -restart ombacksync**
4. NNMi管理サーバーで、**nnmopcexport.ovpl**スクリプトを使用して、新しいトラップの各ポリシーファイルを再生成します。

   既存のポリシーを変更すると、承認中のアラートが検出された時点で、HPE BSM Operations Management/OMiとのインシデントの自動同期を開始する新しいスクリプトがBSM Connectorで検索され、実行されます。

**注意:** NNMiを再インストールする場合は、BSM Connectorを再インストールし、「NNMi管理サーバーで次のコマンドを実行します。」(40ページ)～「NNMi管理サーバーで、nnmopcexport.ovplスクリプトを使用して、新しいトラップの各ポリシーファイルを再生成します。」(40ページ)を繰り返す必要があります。

**注意:** BSM Connectorを再インストールする場合は、「NNMi管理サーバーで次のコマンドを実行します。」(40ページ)および「次のコマンドを実行して、ombacksyncプロセスを再起動します。」(40ページ)を繰り返す必要があります。

5. 以下の手順に従って、ポリシーファイル(*_header.xmlおよび*_data)をBSM Connectorにインポートします。
   a. BSM Connectorユーザーインタフェースのツールバーで、  をクリックします。

      ファイル選択ダイアログボックスが表示されます。
   b. ポリシーファイルに移動し、ポリシーごとにヘッダー(*_header.xml)とデータ(*_data)の両方のファイルを選択します。
   c. [**開く**]をクリックし、インポートプロセスを開始します。

      BSM Connectorにすでに同じポリシーが存在する場合、新しくインポートしたポリシーで置き換えるかどうか尋ねられます。

      インポートしたポリシーがBSM Connectorユーザーインタフェースのポリシーのリストに表示されます。これらのポリシーは、デフォルトでは非アクティブ化されています。

      詳細については、『BSM Connector User Guide』を参照してください。
6. 以下の手順に従って、ポリシーファイルをアクティブ化します。
   a. BSM Connectorユーザーインタフェースのポリシーのリストで、アクティブ化するポリシーを選択します。

      選択したポリシーの少なくとも1つのアクティブ化状態は、[非アクティブ]または[アクティブ化(新規バージョンの再アクティブ化)]になっている必要があります(すでにアクティブ化されたポリシーを選択しても、そのポリシーは無視されて再度アクティブ化されません)。
   b. ツールバーで  をクリックします。アクティブ化状態が[アクティブ化]に変わります。

      詳細については、『BSM Connector User Guide』を参照してください。

# HPE NNMi—HPE BSM Operations ManagementまたはOMi統合の使用法

前のセクションで説明したように、対応するイベントがHPE BSM Operations ManagementまたはOMiで解決した後でNNMiインシデントを自動的に解決するようにNNMiを設定できます。HPE NNMi—HPE BSM Operations ManagementまたはOMi統合では、BSM/OMiとBSM Operations ManagementまたはOMiのイベントブラウザーとの間で、NNMi管理イベントおよびSNMPトラップの双方向フローが備えられています。NNMi SNMPトラップポリシーにより、BSM Operations ManagementまたはOMiのイベントブラウザーでの着信トラップの処理方法と表示方法が決まります。たとえば、トラップカスタム属性の値をイベントタイトルに含めるようにポリシー条件を変更できます。

**注:** NNMiは、BSM Connectorに対して、各管理イベントまたはSNMPトラップのコピーを1つしか送信しません。この動作は、NNM 6.x/7.xとHPOMの統合の動作とは異なります。

転送されたNNMiインシデントをBSM Operations ManagementまたはOMiのイベントブラウザーに表示します。BSM Operations ManagementまたはOMiのイベントブラウザーのメニューコマンドを使用すれば、選択したイベントに合ったNNMiビューにアクセスできます。各イベントに埋め込まれた情報により、このクロスナビゲーションがサポートされます。

- イベント内の`nnmi.server.name`および`nnmi.server.port`カスタム属性により、NNMi管理サーバーが指定されます。
- `nnmi.incident.uuid`カスタム属性により、NNMiデータベース内のインシデントが指定されます。

BSM Operations ManagementまたはOMiのイベントブラウザーでは、送信元のソースオブジェクトが、[**追加情報**] タブの [**オブジェクト**] フィールドと`nnm.source.name`カスタム属性に表示されます。

## 設定項目のID

HPE Business Service Management (BSM)/OMi およびHPE Universal CMDB Software (HPE UCMDB) において、設定項目 (CI) はIT環境にあるコンポーネントをデータベースとして表現したものです。CIは、一連のビジネス、ビジネスプロセス、アプリケーション、サーバーハードウェア、またはサービスです。

NNMiをBSMトポロジデータベースまたはHPE UCMDBと統合すると、NNMiは、NNMiが管理するデバイスのBSMまたはHPE UCMDBとCI情報を共有します。この場合、HPE NNMi—HPE BSM Operations Management統合では、NNMi管理対象デバイスに関するインシデントをBSMまたはHPE UCMDBのCIに関連付けることができます。SNMPトラップポリシー条件により、この関連付けを有効にします。

BSMおよびHPE UCMDBとの統合の詳細については、「HP Universal CMDBとのトポロジ統合」(12ページ)を参照してください。

## ヘルスインジケータ

NNMi SNMPトラップポリシーファイルは、`nnmopcexport.ovpl`に`-omi_hi`オプションを指定して作成されたため、ヘルスインジケータをSNMPトラップポリシーファイルの各標準NNMi管理イベントと関連付けます(ヘルスインジケータのない管理イベントタイプもあります)。ヘルスインジケータは、`EtiHint`カスタム属性で使用できます。

具体的なヘルスインジケータについては、SNMPトラップポリシーファイルを参照してください。

# デフォルトのポリシー条件

デフォルトの統合動作は、ここで説明する統合コンテンツに応じてさまざまです。

- NNMi管理イベントインシデント
  - NNMi SNMPトラップポリシーファイルには、ファイルの生成時にNNMiインシデント設定で定義したすべてのNNMi管理イベント設定の条件が含まれています。
  - NNMi管理イベントから作成されたイベントは、BSM Operations Managementイベントブラウザーに表示されます。
  - これらのトラップには、「設定項目のID」(41ページ)で説明されているCI情報が含まれます。
  - これらのトラップから作成されるイベントには、「ヘルスインジケータ」(41ページ)で説明されているヘルスインジケータが含まれます。
- サードパーティSNMPトラップ
  - NNMi SNMPトラップポリシーファイルには、ファイルの生成時にNNMiインシデント設定で定義したすべてのSNMPトラップ設定の条件が含まれています。
  - サードパーティのトラップから作成されたイベントは、BSM Operations Managementイベントブラウザーに表示されます。
  - これらのトラップには、「設定項目のID」(41ページ)で説明されているCI情報が含まれます。
  - これらのトラップから作成されるイベントに、ヘルスインジケータは含まれていません。
  - 受信したすべてのSNMPトラップを転送するように統合を設定している場合に、BSM Operations ManagementまたはOMiのイベントブラウザーがNNMiが管理するデバイスからSNMPトラップを直接受信すると、BSM Operations ManagementまたはOMiのイベントブラウザーはデバイストラップを受信することになります。NNMiからのSNMPトラップをBSM Operations ManagementまたはOMiのイベントブラウザーが管理対象デバイスから直接受信したトラップと相関させるようにポリシーを設定できます。
- Syslog
  - NNMiは、管理対象デバイスからSyslogを受信して、BSM Connectorに転送します。
- EventLifecycleStateClosedトラップ
  - BSM Connectorは、これらのトラップから作成されたイベントをログに記録します。通常、それらのイベントはBSM Operations ManagementまたはOMiのイベントブラウザーに表示されません。
  - NNMi SNMPトラップポリシーファイルにより、BSM Connectorは、BSM Operations ManagementまたはOMiのイベントブラウザーで解決済みのNNMiインシデントに対応するイベントを承認します。
- LifecycleStateChangeEventトラップ
  - NNMi SNMPトラップポリシーファイルには、これらのトラップを処理する場合の条件は含まれていません。BSM Connectorは、これらのトラップをBSM Operations ManagementまたはOMiのイベントブラウザーに転送しません。
- EventDeletedトラップ

  - NNMi SNMPトラップポリシーファイルには、これらのトラップを処理する場合の条件は含まれていません。BSM Connectorは、これらのトラップをBSM Operations ManagementまたはOMiのイベントブラウザーに転送しません。

- 相関関係通知トラップ
  - BSM Connectorは、これらのトラップから作成されたイベントをログに記録します。それらのイベントは、BSM Operations ManagementまたはOMiのイベントブラウザーに表示されません。
  - BSM Connectorは、NNMi相関トラップを処理して、BSM Operations ManagementまたはOMiのイベントブラウザーでNNMiインシデント相関を複製します。

## ポリシー条件のカスタマイズ

BSM Connectorユーザーインタフェースを使用して、デフォルトのポリシー条件をカスタマイズします。詳細については、『BSM Connector Help』の「Integrating Data With BSM Connector」>「SNMP Trap Policies」>「SNMP Policy User Interface」>「Configuring Rules in SNMP Policies」を参照してください。

## 詳細情報

HPE NNMi—HPE BSM Operations ManagementまたはOMi統合の詳細については、以下のリファレンスを参照してください。

- この統合でBSM Connectorに送信するトラップタイプの説明については、『NNMiデプロイメントリファレンス』の「NNMi Northboundインタフェース」の章にある「NNMi Northboundインタフェースの使用法」セクションを参照してください。
- NNMiがBSM Connectorに送信するトラップの形式については、`hp-nnmi-nbi.mib`ファイルを参照してください。
- HPE NNMi—HPE BSM Operations Management統合の使用法の詳細については、『BSM Operations Management Extensibility Guide』を参照してください。

# HPE NNMi—HPE BSM Operations ManagementまたはOMi統合の変更

このセクションでは以下の内容について説明します。


- 「新規NNMiトラップのSNMPトラップポリシー条件の更新」(43ページ)
- 「設定パラメーターの変更」(44ページ)


## 新規NNMiトラップのSNMPトラップポリシー条件の更新

統合を設定した後に、新しいSNMPトラップインシデント設定をNNMiに追加した場合は、以下の手順を実行します。

1. NNMi管理サーバーで、`nnmopcexport.ovpl`コマンドを使用して新しいトラップのSNMPトラップポリシーファイルを作成します。

   `-template`オプションの場合、既存のSNMPトラップポリシーファイルの名前とは異なる名前を指定します。

   `-omi_policy`オプションと`-omi_hi`オプションを使用します。

ファイルの内容を、特定の作成者またはOIDプレフィックス値に制限します。詳細については、nnmopcexport.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。

2. BSM Connectorユーザーインタフェースを使用して、新しいヘッダーファイルとポリシーファイルをインポートしてアクティブにします。

すべてのNNMi管理イベントとSNMPトラップに対するSNMPトラップポリシーファイルを再作成することもできます。この方法を使用する場合は、BSM Connectorユーザーインタフェースから古いポリシーを削除してください。

**注:** BSM Connectorの設定で、1つのNNMiインシデントについて複数のポリシー条件が含まれる場合は、BSM Operations ManagementまたはOMiのイベントブラウザーにメッセージが表示されます。

## 設定パラメーターの変更

統合設定パラメーターを変更するには、以下の手順を実行します。

1. NNMiコンソールで、[**NNMi–HPOMの統合選択**] フォーム ([**統合モジュールの設定**] > [**HPOM**]) を開きます。
2. [**HPOMエージェントの実装**] をクリックします。
3. 転送先を選択し、[**編集**] をクリックします。
4. 該当するように値を変更します。

   このフォームのフィールドの詳細については、「[NNMi–HPOMエージェントデスティネーション] フォームのリファレンス (BSM Operations Management統合)」(48ページ)を参照してください。
5. フォームの上部にある [**統合の有効化**] チェックボックスがオンであることを確認し、フォームの下部にある [**送信**] をクリックします。

   変更はただちに有効になります。

# HPE NNMi—HPE BSM Operations ManagementまたはOMi統合の無効化

転送先が無効な間は、SNMPトラップはキューイングされません。

BSM ConnectorへのNNMiインシデントの転送を停止するには、以下の手順を実行します。

1. NNMiコンソールで、[**NNMi–HPOMの統合選択**] フォーム ([**統合モジュールの設定**] > [**HPOM**]) を開きます。
2. [**HPOMエージェントの実装**] をクリックします。
3. 転送先を選択し、[**編集**] をクリックします。

   または、[**削除**] をクリックして、選択した転送先の設定をすべて削除します。
4. フォームの上部にある [**統合の有効化**] チェックボックスをオフにし、フォームの下部にある [**送信**] をクリックします。

   変更はただちに有効になります。

必要に応じて、『BSM Connector Help』の説明に従って、SNMPトラップポリシーを非アクティブ化または削除します。

# HPE NNMi—HPE BSM Operations Management統合のトラブルシューティング

このセクションでは以下の内容について説明します。



## BSM Operations Managementイベントブラウザーに転送されたインシデントが表示されない

**ヒント:** 以下の手順の`OVBIN`環境変数は、BSM Connector内部のエージェントの設定で使用するコマンドが格納されている`bin`ディレクトリを参照します。`OVBIN`環境変数のデフォルト値は以下のとおりです。

- Windowsの場合:`<drive>\Program Files (x86)\HP\HP BTO Software\bin`
- Linuxの場合:`/opt/OV/bin`

BSM Operations ManagementイベントブラウザーにNNMiからのインシデントが表示されない場合は、以下の手順を実行します。

1. BSM Connectorがインストールされているサーバーで、エージェント設定を確認します。
   - Windowsの場合:

     **`%OVBIN%\ovconfget eaagt`**

   - Linuxの場合:

     **`$OVBIN/ovconfget eaagt`**

   コマンド出力には、以下の情報が含まれます。
   - Windowsの場合:

     ```
     SNMP_SESSION_MODE=NNM_LIBS
     SNMP_TRAP_PORT=<custom_port>
     ```

   - Linuxの場合:

     ```
     SNMP_SESSION_MODE=NO_TRAPD
     SNMP_TRAP_PORT=<custom_port>
     ```

   `<custom_port>`の値は、162ではなく、[**NNMi–HPOMエージェントデスティネーション**] フォームの [**ポート**] フィールドの値と一致する必要があります。
2. 「BSM Connectorがインストールされているサーバーで、エージェント設定を確認します。」(45ページ)の結果を考慮することでエージェント設定を評価します。
   - エージェント設定が期待通りの場合は、この手順の「BSM Connectorがインストールされているサーバーで、エージェントが実行されていることを確認します。」(46ページ)に進みます。

- SNMP_SESSION_MODEパラメーターが正しく設定されていない場合は、ovconfgetコマンドが期待される結果を返すようになるまで、「BSM Connectorがインストールされているサーバーで、以下のコマンドを入力することにより、BSM Connector内部のエージェントでNNMiからSNMPトラップを受信するカスタムポートを設定します。」(38ページ)を繰り返します。

- <custom_port> の値が162であるか、[**NNMi–HPOMエージェントデスティネーション**] フォームの [**ポート**] フィールドの値と一致していない場合は、予期した結果がovconfgetコマンドから返されるまで、必要に応じて「NNMiとBSM Connectorとの間のSNMP通信に使用可能なポートを指定します。」(37ページ)から「NNMi管理サーバーで、BSM ConnectorへのNNMiインシデント転送を設定します。」(38ページ)を繰り返します。

3. BSM Connectorがインストールされているサーバーで、エージェントが実行されていることを確認します。
   - Windowsの場合:

     **%OVBIN%\opcagt -status**

   - Linuxの場合:

     **$OVBIN/opcagt -status**

   コマンド出力には、以下の例と同様のopctrapiエントリが含まれます。

   ```
   opctrapi  OVO SNMP Trap Interceptor  AGENT,EA  (4971)  Running
   ```

   出力が期待通りでない場合は、エージェントを再起動します。

   **ovc -restart opctrapi**
4. BSM Connectorがインストールされているサーバーで、エージェントが予期されるSNMPトラップポートで待機していることを確認します。
   a. 以下のコマンドを実行します。
      - Windowsの場合: **netstat -an | findstr** <custom_port>
      - Linuxの場合:**netstat -an | grep** <custom_port>

      <custom_port> は、この手順の「BSM Connectorがインストールされているサーバーで、エージェント設定を確認します。」(45ページ)で取得したSNMP_TRAP_PORTの値です。
   b. 出力に状態LISTENINGまたはLISTENが含まれることを確認します。

      出力が期待通りでない場合は、エージェントを再起動します。

      **ovc -restart opctrapi**
5. BSM Connectorがインストールされているサーバーで、NNMiのSNMPトラップポリシーファイルがNNMi管理サーバーのBSM Connectorに配備されていることを確認します。
   - Windowsの場合:

     **%OVBIN%\ovpolicy -list**

   - Linuxの場合:

     **$OVBIN/ovpolicy -list**

   コマンド出力には、以下の例と同様のエントリが含まれます。

   ```
   Type     Name                         Status     Version
   ------------------------------------------------------------
   trapi    "NNMi Management Events"   enabled    0001.0000
   ```

[Name] フィールドの値は、「NNMi管理サーバーで、NNMiが転送するトラップのSNMPトラップポリシーファイルを生成します。」(36ページ)でnnmopcexport.ovplに指定する-templateオプションから得られるSNMPトラップポリシーファイルの名前です。

6. BSM Connectorがインストールされているサーバーで、エージェントログファイルにエラーが記録されていないかを確認します。ログファイルは、以下の場所にあります。
   - Windowsの場合：%ovdatadir%\log\System.txt
   - Linuxの場合：/var/opt/OV/log/System.txt
7. BSM Connectorがトラップを受信していることを確認します。
   a. BSM ConnectorがBSM Operations Managementイベントブラウザーにイベントを送信できることを確認します。これを行うには、BSMCポリシー管理UIを使用して、単純なopen message interfaceポリシーを作成します。ポリシーの [**オプション**] タブで、[**一致しないイベントをアクティブブラウザーに転送する**] が有効になっている必要があります。この新しいopen message interfaceポリシーを**保存およびアクティブ化**します。このopen message interfaceポリシーをアクティブ化すると、opcmsgコマンドを使用して、BSM Operations Managementイベントブラウザーにイベントを送信できます。
   b. BSM Connectorのトレースを有効にして、トラップがBSM Connectorに到着するかどうかを判断します。これを行うため、適切なSNMPポリシーの [オプション] タブで、着信トラップイベントをログに記録するポリシーを設定する場合があります。これらのイベントは、以下のログファイルのローカルノードにログ記録されます。
      - Windowsの場合：%ovdatadir%\log\OpC\opcmsglg
      - Linuxの場合：/var/opt/OV/log/OpC/opcmsglg
8. NNMiがBSM Connectorに管理イベントを転送していることを確認します。

   詳細については、『NNMiデプロイメントリファレンス』の「NNMi Northboundインタフェース」の章にある「NNMi Northboundインタフェースのトラブルシューティング」セクションを参照してください。

# BSM Operations Managementイベントブラウザーに転送されたインシデントの一部だけが表示される

BSM Operations Managementイベントブラウザーに1つ以上のNNMiインシデントが表示されない場合は、以下の手順を実行します。

1. NNMi管理サーバーで、SNMPトラップポリシーによってトラップが抑制されないことを確認します。
2. BSMサーバーで、BSM Operations Managerが実行されていることを確認します。

   **注：** Windows BSMサーバーには、BSMサーバーのステータスが表示されているWebページがあります。[**スタート**] > [**すべてのプログラム**] > [**HP Business Service Management**] > [**管理**] > [**HP Business Service Managementのステータス**] メニューを使用してステータスを表示します。

   BSMサーバーがシャットダウンすると、BSM Connectorは受信したトラップをキューイングします。BSM Connectorは、BSM Operations Managementイベントブラウザーが使用可能になると、キューイングされたトラップを転送します。

   BSM Connectorがシャットダウンすると、転送されたトラップは失われます。NNMiはトラップを再送しません。
3. NNMi管理サーバーで、NNMiプロセスが実行されていることを確認します。

   ```
   ovstatus -c
   ```

   シャットダウン中にNNMiに送信されたトラップは失われます。

# [NNMi–HPOMエージェントデスティネーション] フォームのリファレンス (BSM Operations Management統合)

[**NNMi–HPOMエージェントデスティネーション**] フォームには、NNMiとBSM Connectorの間の通信を設定するためのパラメーターが含まれています。このフォームは、[**統合モジュールの設定**] ワークスペースから使用できます。([**NNMi–HPOMの統合選択**] フォームで、[**HPOMエージェントの実装**] をクリックします。[**新規作成**] をクリックするか、転送先を選択してから、[**編集**] をクリックします。)

**注:** [**NNMi–HPOMエージェントデスティネーション**] フォームにアクセスできるのは、管理者ロールを持つNNMiユーザーのみです。

[**NNMi–HPOMエージェントデスティネーション**] フォームでは、以下の領域の情報を収集します。

- 「BSM Connector接続」(48ページ)
- 「BSM Operations ManagementまたはOMi統合コンテンツ」(49ページ)
- 「BSM Connector転送先のステータス情報」(51ページ)

統合設定への変更を適用するには、[**NNMi–HPOMエージェントデスティネーション**] フォームの値を更新して、[**送信**] をクリックします。

## BSM Connector接続

「表5: BSM Connectorの接続情報」(48ページ)に、BSM Connectorへの接続設定用パラメーターを示します。

**表5: BSM Connectorの接続情報**

| フィールド | 説明 |
|---|---|
| ホスト | NNMi管理サーバーの完全修飾ドメイン名 (推奨) またはIPアドレス。この管理サーバーは、BSM ConnectorがNNMiからSNMPトラップを受信するシステムです。<br>統合は、以下のBSM Connectorホストの識別方法をサポートしています。<br>• **NNMi FQDN**<br>NNMiは、BSM Connectorへの接続を管理します。[**ホスト**] フィールドは読み取り専用になります。<br>これがデフォルトの推奨設定です。<br>• **ループバックを使用**<br>このオプションは使用しないでください。<br>• **その他**<br>このオプションは使用しないでください。<br>**注:** NNMi管理サーバーがNNMiアプリケーションフェイルオーバーに参加する場合は、『NNMiデプロイメントリファレンス』の「NNMi Northboundインタフェース」の章にある「アプリケーションフェイルオーバーとNNMi Northboundインタフェース」を参照してください。 |

**表5: BSM Connectorの接続情報 (続き)**

| フィールド | 説明 |
|---|---|
| ポート | BSM ConnectorがSNMPトラップを受信するUDPポート。<br>BSM Connector固有のポート番号を入力します。この値は、「NNMiとBSM Connectorとの間のSNMP通信に使用可能なポートを指定します。」(37ページ)で指定したポートです。<br>ポートを決定するには、BSM Connectorがインストールされているサーバーで **ovconfget eaagt**コマンドを実行します。トラップポートは、SNMP_TRAP_PORT変数の値です。<br>**注:** このポート番号は、NNMiコンソールの [**通信の設定**] フォームの [**SNMPポート**] フィールドで設定した、NNMiがSNMPトラップを受信するためのポートと別にする必要があります。 |
| コミュニティ文字列 | トラップを受信するBSM Connectorの読み取り専用コミュニティ文字列。<br>HPE NNMi—HPE BSM Operations Management統合では、デフォルト値publicを使用します。 |

# BSM Operations ManagementまたはOMi統合コンテンツ

「表6: BSM Operations Management統合コンテンツ設定情報」(49ページ)に、NNMiがBSM Connectorに送信するコンテンツを設定するためのパラメーターを示します。

**表6: BSM Operations Management統合コンテンツ設定情報**

| フィールド | 説明 |
|---|---|
| インシデント | インシデント転送の送信オプション。<br>• **管理**<br>NNMiは、NNMiで生成された管理イベントのみをBSM Connectorに転送します。<br>• **サードパーティSNMPトラップ**<br>NNMiは、NNMiが管理対象デバイスから受信したSNMPトラップのみをBSM Connectorに転送します。<br>• **Syslog**<br>NNMiは、NNMiが生成した管理イベントとNNMiが管理対象デバイスから受信したSNMPトラップの両方をBSM Connectorに転送します。<br>これがデフォルト設定です。<br>詳細については、『NNMiデプロイメントリファレンス』の「NNMi Northboundインタフェース」の章を参照してください。 |
| ライフサイクル状態の変化 | インシデント変更通知の送信オプション。<br>• **解決済みに変化**<br>NNMiは、ライフサイクル状態が [解決済み] に変化したインシデントごとに、インシデント解決済みトラップをBSM Connectorに送信します。<br>これがデフォルト設定です。 |

**表6: BSM Operations Management統合コンテンツ設定情報 (続き)**

| フィールド | 説明 |
|---|---|
| | • **状態が変化した**<br>NNMiは、ライフサイクル状態が[進行中]、[完了]、または[解決済み]に変化したインシデントごとに、インシデントのライフサイクル状態変化トラップをBSM Connectorに送信します。<br>• **両方**<br>NNMiは、ライフサイクル状態が[解決済み]に変化したインシデントごとに、インシデント解決済みトラップをBSM Connectorに送信します。また、この統合は、ライフサイクル状態が[進行中]、[完了]、または[解決済み]に変化したインシデントごとに、インシデントのライフサイクル状態変化トラップをBSM Connectorに送信します。<br>**注:** この場合、インシデントが[解決済み]ライフサイクル状態に変化するたびに、インシデント解決済みトラップとインシデントライフサイクル状態変更トラップの2つの通知トラップが統合によって送信されます。 |
| 相関処理 | インシデント相関処理の送信オプション。<br>• **なし**<br>NNMiは、NNMiの因果関係分析によるインシデント相関処理結果をBSM Connectorに通知しません。<br>これがデフォルト設定です。<br>• **単一**<br>NNMiは、NNMi因果関係分析で判明した親子インシデント相関関係ごとにトラップを1つ送信します。<br>• **グループ**<br>NNMiは、親インシデントに相関するすべての子インシデントをリストした相関処理ごとに、トラップを1つ送信します。<br>**メモ**: BSMでイベントの相関処理も行う場合はこの値を選択することをお勧めします。 |
| 削除 | インシデント削除の送信オプション。<br>• **送信しない**<br>NNMiは、インシデントがNNMiで削除されてもBSM Connectorに通知しません。<br>これがデフォルト設定です。<br>• **送信**<br>NNMiは、インシデントがNNMiで削除されるたびに削除トラップをBSM Connectorに送信します。 |
| NNMiコンソールアクセス | BSM Operations ManagementまたはOMiのイベントブラウザーからNNMiコンソールにアクセスするための、URL内での接続プロトコルの指定。NNMiがBSM Connectorに送信するトラップのNmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2) には、NNMi URLが含まれます。<br>統合には、NNMiコンソールへのHTTP接続が必要であるため、[**HTTP**] オプションを選択します。 |
| インシデントフィルター | BSM Connectorに送信されたイベントを統合でフィルターするときのオブジェクトID (OID) のリスト。各フィルターエントリは、有効な数値OID (たとえ |

**表6: BSM Operations Management統合コンテンツ設定情報 (続き)**

| フィールド | 説明 |
|---|---|
| | ば、.1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9) またはOIDプレフィックス (たとえば、.1.3.6.1.6.3.1.1.5.*) にすることができます。<br>次のいずれかのオプションを選択します。<br>• **なし**<br>NNMiは、すべてのイベントをBSM Connectorに送信します。<br>これがデフォルト設定です。<br>• **含む**<br>NNMiは、フィルターで識別されたOIDと一致する特定のイベントのみを送信します。<br>• **除外する**<br>NNMiは、フィルターで識別されたOIDと一致する特定のイベントを除くすべてのイベントを送信します。<br>インシデントフィルターを指定します。<br>• フィルターエントリを追加するには、下側のテキストボックスにテキストを入力してから、[**追加**] をクリックします。<br>• フィルターエントリを削除するには、上側のボックスのリストからエントリを選択して、[**削除**] をクリックします。 |

# BSM Connector転送先のステータス情報

「表7: BSM Connector転送先のステータス情報」(51ページ)に、BSM Connectorに使用する読み取り専用のステータス情報を示します。この情報は、統合が現在機能しているか確認する場合に役立ちます。

**表7: BSM Connector転送先のステータス情報**

| フィールド | 説明 |
|---|---|
| トラップ先IPアドレス | BSM Connectorの転送先ホスト名の解決先となるIPアドレス。<br>この値は、この転送先に固有の値です。 |
| アップタイム (秒) | Northboundコンポーネントが最後に起動されてからの時間 (秒)。NNMiがBSM Connectorに送信するトラップのsysUptimeフィールド (1.3.6.1.2.1.1.3.0) には、この値が含まれます。<br>この値は、NNMi Northboundインタフェースを使用するすべての統合に対して同じです。最新の値を表示するには、リフレッシュするか、フォームを閉じて再び開いてください。 |
| NNMi URL | NNMiコンソールに接続するためのURL。NNMiがBSM Connectorに送信するトラップのNmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2) には、この値が含まれます。<br>この値は、このノースバウンド転送先に固有です。 |

# NNMiの視覚化

HPE Business Service Management (BSM) プラットフォームおよびOMiは、本番アプリケーションの可用性の管理、システムのパフォーマンスモニタリング、インフラストラクチャのパフォーマンスモニタリング、および障害が発生した場合の積極的な解決に使用するツールです。

BSMやOMiのご購入については、HP営業担当者にお問い合わせください。

この章には、以下のトピックがあります。



BSM Operations Managementイベントブラウザーのイベントから起動されるNNMiコンソールビューについては、「HPE NNMi—HPE BSM Operations ManagementまたはOMi統合の使用法」(41ページ)を参照してください。

# MyBSMポータル

MyBSMは、HPソフトウェアポートフォリオでデータを表示するためのポータルベースのダッシュボード環境です。MyBSMポータルでは、一連のポータルページおよびポートレットが提供され、ユーザー固有のビジネスタスクに関する情報が表示されます。

MyBSM管理者は、特定のユーザーまたはユーザーグループが求めるコンポーネントを含むページを設定します。MyBSMワークスペースでは、異なるBSMアプリケーションおよびレポート間でスムーズなやり取りが可能です。

**注:** 複数のNNMiインスタンスを1つのBSMと統合する場合、制限が1つあります。イベント統合およびトポロジ統合が期待どおりに機能していても、MyBSMポータルのその他のNNMiコンポーネントの機能を考慮する必要があります。これらのNNMiコンポーネントは「MyBSMで使用できるNNMiコンポーネント」(52ページ)で説明されています。MyBSM統合のみの場合、単一の(BSMに事前設定された)NNMiインスタンスとの通信に制限されます。

NNMiコンポーネントにアクセスするには、適切なライセンスをインストールしておく必要があります。NNMiコンポーネントはNNMi管理サーバーとの接続を設定した場合のみ表示されます([**管理者**] > [**プラットフォーム**] > [**セットアップとメンテナンス**] > [**インフラストラクチャ設定**] > [**ファウンデーション**] > [**他のアプリケーションとの統合**] > [**HP NNM**])。

## MyBSMで使用できるNNMiコンポーネント

BSMコンポーネントギャラリには、以下のNNMiコンポーネントが含まれます。

- 重要な未解決インシデント

  ネットワークオペレーターにとって最も重要で、緊急な対処を要することが多いインシデントが表示されます。
- レイヤー2の近隣接続ビュー

  選択したデバイス、およびそのデバイスから指定したホップ数内にあるコネクターデバイスのマップビューが表示されます。このビューは、デバイス間のスイッチの接続性を理解するのに役立ちます。

- レイヤー3の近隣接続ビュー

  選択したデバイス、およびそのデバイスから指定したホップ数内にあるコネクターデバイスのマップビューが表示されます。このビューは、デバイス間のルーターの接続性を理解するのに役立ちます。
- MPLS VPNインベントリ

  これは、MPLSネットワークで提供されるサービスを使用してサイトがどのように接続されているのかを示すエンタープライズカスタマービューです。
- 全体のネットワークヘルス(ノードグループの概要)

  親ノードグループのないすべての(トップレベルの)ノードグループを含むマップが表示されます。
- 全体のネットワークヘルス

  ネットワークのルーターの接続性のノードグループマップが表示されます。
- パスビュー

  選択したノード間のパスビューが表示されます。
- ルーター冗長グループインベントリ

  NNMi管理者が作成した使用可能なルーター冗長グループが表示されます。各ルーター冗長グループは、情報パケットが目的の宛先に確実に到達するように、1つまたは複数の仮想IPアドレスを使用する2つ以上のルーターのセットです。

## MyBSMのNNMiコンポーネントの表示

MyBSMでNNMiコンポーネントを表示するには、以下の手順を実行します。

1. 「BSMまたはOMiからのNNMiの視覚化の有効化」(65ページ)の説明に従って、BSMからNNMiへの接続を設定します(まだ行っていない場合)。
2. 「NNMiとBSM、OMi、またはUCMDB間のシングルサインオンの設定」(16ページ)の説明に従って、BSMとNNMi間のシングルサインオンを有効にします(まだ行っていない場合)。
3. 「HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合の有効化」(14ページ)の説明に従って、トポロジ情報をRTSMまたはUCMDBに直接プッシュするようにNNMiを設定します(まだ行っていない場合)。

   **注:** NNMiがトポロジ情報をUCMDBにプッシュするように設定している場合、UCMDB製品メディアに収録されている『UCMDB データフロー管理ガイド』を使用して、必要なCIおよび関係がUCMDBからBSMにプッシュされることを確認してください。このマニュアルは、UCMDB製品用の以下のURLから入手することもできます。
   http://h20230.www2.hp.com/selfsolve/manuals
4. NNMiコンポーネントをMyBSMポータルに追加します。
   a. ユーザー定義のMyBSMページ内で、[**コンポーネントギャラリ**]を開きます。
   b. いずれかのNNMiコンポーネントを選択し、ページに追加します。

   詳細については、『HP BSM Using MyBSM Guide』の「How to Create Your MyBSM Workspace」を参照してください。

# OMiのマイワークスペース

OMi 10.00(およびそれ以降)では、マイワークスペースがMyBSMと同等の機能を提供します。NNMiと統合することで、OMiのマイワークスペースにMyBSMと同じNNMiコンポーネントが表示されます。

# HTTPS接続の設定

BSMまたはOMiへのSSL接続を設定するには、このトピックで説明する手順を実行します。

NNMi 10.20では、PKCS #12形式のkeystoreファイルとtruststoreファイルにより、より強固で安全な証明書スキームが導入されます。すべての新しいインストールでは、PKCS #12形式に基づく証明書スキームがデフォルトで有効です。NNMiを旧バージョンからアップグレードしたシステムでは、証明書管理が古いスキームになっていることがあります。

PKCS #12形式の証明書を使用した設定手順については、「nnm-key.p12ファイルによる設定」を参照してください。

古い形式の証明書を使用した設定手順については、「nnm.keystoreファイルによる設定」を参照してください。

### nnm-key.p12ファイルによる設定

1. BSMまたはOMiのゲートウェイサーバーのコマンドウィンドウで、以下のディレクトリに変更します。
   - Windowsの場合: `<drive>:\HPBSM\JRE64\bin`
   - Linuxの場合: `/opt/HP/BSM/JRE64/bin`
2. 自己署名証明書を使用する場合は、次のコマンドを実行して、新しい2048ビット証明書を生成する必要があります。
   - Windowsの場合:
     **keytool -genkey -keyalg rsa -keysize 2048 -alias** <alias_name> **-keystore** <Install_Dir>**\odb\conf\security\server.keystore -validity "7200" -dname** <distinguished_name>
   - Linuxの場合:
     **./keytool -genkey -keyalg rsa -keysize 2048 -alias** <alias_name> **-keystore** <Install_Dir>**/odb/conf/security/server.keystore -validity "7200" -dname** <distinguished_name>

     この場合、<Install_Dir> はBSMまたはOMiをインストールしたディレクトリ、<distinguished_name> はゲートウェイサーバーの識別名です。
3. CA署名証明書を使用する場合は、以下の手順に従って、証明書署名要求 (CSR) ファイルを送信します。
   a. 以下のコマンドを実行します。
      - Windowsの場合:
        **keytool -keystore** <Install_Dir>**\odb\conf\security\server.keystore -certreq -storepass hppass -alias** <alias_name> **-filename** <cert_file_name>
      - Linuxの場合:
        ./**keytool -keystore** <Install_Dir>**/odb/conf/security/server.keystore -certreq -storepass hppass -alias** <alias_name> **-filename <cert_file_name>**

        この例の、<Install_Dir> はBSMまたはOMiをインストールしたディレクトリ、<cert_file_name> は証明書ファイルの名前、<alias_name> はCA署名証明書のエイリアス名です。

   b. CA署名機関にCSRを送信します (CA署名機関が証明書ファイルに署名して返します)。
4. 手順5のコマンドを実行しますが、`server.truststore`を`server.keystore`の代わりに使用します。

- Windowsの場合:
  **keytool.exe -import -alias <NNMi_FQDN>.selfsigned -keystore <drive>:\HPBSM\odb\conf\security\server.truststore -storepass hppass -trustcacerts -file <drive>:\bsm_temp\nnmicert**

- Linuxの場合:
  **keytool -import -alias <NNMi_FQDN>.selfsigned -keystore /opt/HP/BSM/odb/conf/security/server.truststore -storepass hppass -trustcacerts -file /bsm_tmp/nnmicert**

「Trust this certificate?」という質問に対しては、必ず「yes」と答えます。以下のプログラム一覧は、このコマンドを実行した後の表示例です。

```
Owner: CN=hpbsm_server.example.com
Issuer: CN=hpbsm_server.example.com
Serial number: 4d525d0e
Valid from: Wed Feb 09 11:23:26 EET 2011 until:Fri Jan 16 11:23:26 EET 2111
Certificate fingerprints:
     MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
     SHA1: 42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
     Signature algorithm name: SHA1withRSA
     Version: 1
Trust this certificate?[no]: yes
Certificate was added to keystore
```

5. NNMi証明書をJREに追加するには、以下のコマンドを実行します。

   - Windowsの場合:
     **keytool.exe -import -alias <NNMi_FQDN>.selfsigned -keystore <drive>:\HPBSM\JRE\lib\security\cacerts -storepass changeit -trustcacerts -file <drive>:\bsm_temp\nnmicert**

   - Linuxの場合:
     **keytool -import -alias <NNMi_FQDN>.selfsigned -keystore /opt/HP/BSM/JRE/lib/security/cacerts -storepass changeit -trustcacerts -file /bsm_tmp/nnmicert**

   「Trust this certificate?」という質問に対しては、必ず「yes」と答えます。以下のプログラム一覧は、このコマンドを実行した後の表示例です。

   ```
   Owner: CN=hpbsm_server.example.com
   Issuer: CN=hpbsm_server.example.com
   Serial number: 4d525d0e
   Valid from: Wed Feb 09 11:23:26 EET 2011 until:Fri Jan 16 11:23:26 EET 2111
   Certificate fingerprints:
        MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
        SHA1: 42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
        Signature algorithm name: SHA1withRSA
        Version: 1
   Trust this certificate?[no]: yes
   Certificate was added to keystore
   ```

6. NNMi証明書をJRE64に追加するには、以下のコマンドを実行します。

- Windowsの場合:
  **keytool.exe -import -alias <NNMi_FQDN>.selfsigned -keystore <drive>:\HPBSM\JRE64\lib\security\cacerts -storepass changeit -trustcacerts -file <drive>:\bsm_temp\nnmicert**
- Linuxの場合:
  **keytool -import -alias <NNMi_FQDN>.selfsigned -keystore /opt/HP/BSM/JRE64/lib/security/cacerts -storepass changeit -trustcacerts -file /bsm_tmp/nnmicert**

「Trust this certificate?」という質問に対しては、必ず「yes」と答えます。以下のプログラム一覧は、このコマンドを実行した後の表示例です。

```
Owner: CN=hpbsm_server.example.com
Issuer: CN=hpbsm_server.example.com
Serial number: 4d525d0e
Valid from: Wed Feb 09 11:23:26 EET 2011 until:Fri Jan 16 11:23:26 EET 2111
Certificate fingerprints:
     MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
     SHA1: 42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
     Signature algorithm name: SHA1withRSA
     Version: 1
Trust this certificate?[no]: yes
Certificate was added to keystore
```

7. BSMまたはOMiの証明書をNNMi管理サーバーにインポートするには、以下の手順を実行します。
   a. BSMまたはOMiのゲートウェイサーバーで以下のコマンドを実行します。
      - Windowsの場合:
        **keytool.exe -export -alias hpcert -file <path>\keystore -keystore** <drive>**:\HPBSM\odb\conf\security\server.keystore -storepass hppass**
      - Linuxの場合:
        **keytool.exe -export -alias hpcert -file <path>/keystore -keystore /opt/HP/BSM/odb/conf/security/server.keystore -storepass hppass**

      コマンドの実行が終了すると、BSMまたはOMiのキーストア証明書は、指定したkeystoreファイルに保存されます。
   b. BSMまたはOMiのゲートウェイサーバーで以下のコマンドを実行します。
      - Windowsの場合:
        **keytool.exe -export -alias clientcert -file <path>\truststore -keystore <drive>:\HPBSM\odb\conf\security\server.truststore -storepass hppass**
      - Linuxの場合:
        **keytool -export -alias clientcert -file <path>/truststore -keystore /opt/HP/BSM/odb/conf/security/server.truststore -storepass hppass**

      コマンドの実行が終了すると、BSMまたはOMiのトラストストア証明書は、指定したtruststoreファイルに保存されます。
   c. 手順bで作成したtruststoreファイルをNNMi管理サーバーの一時ディレクトリにコピーします。残りのコマンドでは、これらのファイルはNNMi管理サーバーの以下の場所に存在しているものとして表示され

ます。

- Windowsの場合:
  <drive>:\nnmi_temp\keystore
  <drive>:\nnmi_temp\truststore,
- Linuxの場合:
  /nnmi_tmp/keystore
  /nnmi_tmp/truststore

d. トラストストアファイルをマージするには、NNMi管理サーバーで以下のコマンドを実行します。

- Windowsの場合:
  **%nnminstalldir%\bin\nnmkeytool.ovpl -import -alias hpcert -keystore %NnmDataDir%\shared\nnm\certificates\nnm-key.p12 -storetype PKCS12 -storepass nnmkeypass -file <drive>:\nnmi_temp\keystore**
- Linuxの場合:
  **/opt/OV/bin/nnmkeytool.ovpl -import -alias hpcert -keystore $NnmDataDir/shared/nnm/certificates/nnm.keystore -storetype PKCS12 -storepass nnmkeypass -file /nnmi_tmp/keystore**

e. BSMまたはOMiで1つ以上の認証機関 (CA) 署名証明書を使用している場合のみこの手順を実行してください (自己署名証明書でない場合)。CAルート証明書およびCA中間証明書をNNMiトラストストアにインポートします。

各CA証明書を別々にインポートします。たとえば、CAルート証明書と1つのCA中間証明書をインポートするには、NNMi管理サーバーで以下のコマンドを実行します。

- Windowsの場合:
  **%nnminstalldir%\bin\nnmkeytool.ovpl -import -alias <bsm_ca_root_cert> -keystore %NnmDataDir%\shared\nnm\certificates\nnm-trust.p12 -storetype PKCS12 -storepass ovpass -file <drive>:\temp\keystore**
- **/opt/OV/bin/nnmkeytool.ovpl -alias <bsm_ca_intermediate_cert> -keystore $NnmDataDir/shared/nnm/certificates/nnm-trust.p12 -storetype PKCS12 -storepass ovpass -file /tmp/keystore**
- Linuxの場合:
  **/opt/OV/bin/nnmkeytool.ovpl -import -alias <bsm_ca_intermediate_cert> -keystore %NnmDataDir%\shared\nnm\certificates\ nnm-trust.p12 -storetype PKCS12 -storepass ovpass -file <drive>:\temp\keystore**
- **/opt/OV/bin/nnmkeytool.ovpl -import -alias <bsm_ca_intermediate_cert> -keystore $NnmDataDir/shared/nnm/certificates/nnm-trust.p12 -storetype PKCS12 -storepass ovpass -file /tmp/keystore**

8. オプション: NNMi管理サーバーで、以下のコマンドを以下の順序で実行します。
   a. **ovstop**
   b. **ovstart**
9. オプション: NNMi管理サーバーとBSMサーバーかOMiゲートウェイサーバーの両方で、以下のコマンドを実行します。出力を比較して、両方のサーバーにキーストア証明書が存在することを確認します。

- NNMi管理サーバー:
  - Windowsの場合: **%nnminstalldir%\bin\nnmkeytool.ovpl -list -keystore %NnmDataDir%\shared\nnm\certificates\nnm-key.p12 -storetype PKCS12 -storepass nnmkeypass -v**

    - Linuxの場合: **/opt/OV/bin/nnmkeytool.ovpl -list -keystore /var/opt/OV/shared/nnm/certificates/nnm-key.p12 -storetype PKCS12 -storepass nnmkeypass -v**

- BSMまたはOMiゲートウェイサーバー:
    - Windowsの場合: **keytool.exe -list -keystore <drive>:\HPBSM\odb\conf\security\server.keystore -storepass hppass -v**
    - Linuxの場合: **keytool -list -keystore /opt/HP/BSM/odb/conf/security/server.keystore -storepass hppass -v**

10. 証明書がまだ有効であることを確認するために、日付の範囲をチェックします。

### nnm.keystoreファイルによる設定

1. 以下のコマンドを使用して、nnm.keystoreファイルからNNMiの証明書をエクスポートします。
    - Windowsの場合:
      **%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -export -alias <NNMi_FQDN>.selfsigned -file <drive>:\temp\nnmicert -keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore -storepass nnmkeypass**

      **注:** keytool.exeコマンドに完全なパスを入力する場合、このコマンドを実行すると、コマンド文字列に存在する予期せぬスペースが原因でコマンドのエラーが表示されることがあります。これを解決するには、パスとkeytool.exeコマンドを引用符で囲みます。たとえば、コマンドのエラーを回避するには「C:\Program Files (x86)\HP\HP BTO Software\nonOV\jdk\hpsw\bin\keytool.exe」を使用してください。

    - Linuxの場合:
      **$NnmInstallDir/nonOV/jdk/hpsw/bin/keytool -export -alias <NNMi_FQDN>.selfsigned -file /tmp/nnmicert -keystore $NnmDataDir/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass**

2. 「Certificate stored in file <**path_and_cert_file**>」というメッセージが表示されることを確認します。
3. 「HTTPS接続の設定」(54ページ)で作成したNNMi証明書ファイルをBSMまたはOMiゲートウェイサーバーの一時ディレクトリにコピーします。残りのコマンドでは、このファイルはBSMまたはOMiのゲートウェイサーバーの以下の場所に存在しているものとして表示されます。
    - Windowsの場合: <drive>:\bsm_temp\nnmicert
    - Linuxの場合: /bsm_tmp/nnmicert
4. BSMまたはOMiのゲートウェイサーバーのコマンドウィンドウで、以下のディレクトリに変更します。
    - Windowsの場合: <drive>:\HPBSM\JRE64\bin
    - Linuxの場合: /opt/HP/BSM/JRE64/bin
5. 以下のコマンドを実行します。

- Windowsの場合:
  **keytool.exe -import -alias <NNMi_FQDN>.selfsigned -keystore <drive>:\HPBSM\odb\conf\security\server.keystore -storepass hppass -trustcacerts -file <drive>:\bsm_temp\nnmicert**

- Linuxの場合:
  **keytool -import -alias <NNMi_FQDN>.selfsigned -keystore /opt/HP/BSM/odb/conf/security/server.keystore -storepass hppass -trustcacerts -file /bsm_tmp/nnmicert**

「Trust this certificate?」という質問に対しては、必ず「yes」と答えます。以下のプログラム一覧は、このコマンドを実行した後の表示例です。

```
Owner: CN=hpbsm_server.example.com
Issuer: CN=hpbsm_server.example.com
Serial number: 4d525d0e
   Valid from: Wed Feb 09 11:23:26 EET 2011 until:Fri Jan 16 11:23:26 EET 2111
Certificate fingerprints:
     MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
     SHA1: 42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
     Signature algorithm name: SHA1withRSA
     Version: 1
Trust this certificate?[no]:yes
Certificate was added to keystore
```

6. 手順5のコマンドを実行しますが、server.truststoreをserver.keystoreの代わりに使用します。
   - Windowsの場合:
     **keytool.exe -import -alias <NNMi_FQDN>.selfsigned -keystore <drive>:\HPBSM\odb\conf\security\server.truststore -storepass hppass -trustcacerts -file <drive>:\bsm_temp\nnmicert**

   - Linuxの場合:
     **keytool -import -alias <NNMi_FQDN>.selfsigned -keystore /opt/HP/BSM/odb/conf/security/server.truststore -storepass hppass -trustcacerts -file /bsm_tmp/nnmicert**

   「Trust this certificate?」という質問に対しては、必ず「yes」と答えます。以下のプログラム一覧は、このコマンドを実行した後の表示例です。

   ```
   Owner: CN=hpbsm_server.example.com
   Issuer: CN=hpbsm_server.example.com
   Serial number: 4d525d0e
   Valid from: Wed Feb 09 11:23:26 EET 2011 until:Fri Jan 16 11:23:26 EET 2111
   Certificate fingerprints:
        MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
        SHA1: 42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
        Signature algorithm name: SHA1withRSA
        Version: 1
   Trust this certificate?[no]: yes
   Certificate was added to keystore
   ```

7. NNMi証明書をJREに追加するには、以下のコマンドを実行します。

- Windowsの場合:
  **keytool.exe -import -alias <NNMi_FQDN>.selfsigned -keystore <drive>:\HPBSM\JRE\lib\security\cacerts -storepass changeit -trustcacerts -file <drive>:\bsm_temp\nnmicert**

- Linuxの場合:
  **keytool -import -alias <NNMi_FQDN>.selfsigned -keystore /opt/HP/BSM/JRE/lib/security/cacerts -storepass changeit -trustcacerts -file /bsm_tmp/nnmicert**

「Trust this certificate?」という質問に対しては、必ず「yes」と答えます。以下のプログラム一覧は、このコマンドを実行した後の表示例です。

```
Owner: CN=hpbsm_server.example.com
Issuer: CN=hpbsm_server.example.com
Serial number: 4d525d0e
Valid from: Wed Feb 09 11:23:26 EET 2011 until:Fri Jan 16 11:23:26 EET 2111
Certificate fingerprints:
     MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
     SHA1: 42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
     Signature algorithm name: SHA1withRSA
     Version: 1
Trust this certificate?[no]: yes
Certificate was added to keystore
```

8. NNMi証明書をJRE64に追加するには、以下のコマンドを実行します。
   - Windowsの場合:
     **keytool.exe -import -alias <NNMi_FQDN>.selfsigned -keystore <drive>:\HPBSM\JRE64\lib\security\cacerts -storepass changeit -trustcacerts -file <drive>:\bsm_temp\nnmicert**
   - Linuxの場合:
     **keytool -import -alias <NNMi_FQDN>.selfsigned -keystore /opt/HP/BSM/JRE64/lib/security/cacerts -storepass changeit -trustcacerts -file /bsm_tmp/nnmicert**

   「Trust this certificate?」という質問に対しては、必ず「yes」と答えます。以下のプログラム一覧は、このコマンドを実行した後の表示例です。

   ```
   Owner: CN=hpbsm_server.example.com
   Issuer: CN=hpbsm_server.example.com
   Serial number: 4d525d0e
   Valid from: Wed Feb 09 11:23:26 EET 2011 until:Fri Jan 16 11:23:26 EET 2111
   Certificate fingerprints:
        MD5: C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
        SHA1: 42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
        Signature algorithm name: SHA1withRSA
        Version: 1
   Trust this certificate?[no]: yes
   Certificate was added to keystore
   ```

9. BSMまたはOMiの証明書をNNMi管理サーバーにインポートするには、以下の手順を実行します。

a. BSMまたはOMiのゲートウェイサーバーで以下のコマンドを実行します。
   - Windowsの場合:
     **keytool.exe -export -alias hpcert -file <path>\keystore**
     **-keystore** <drive>**:\HPBSM\odb\conf\security\server.keystore**
     **-storepass hppass**
   - Linuxの場合:
     **keytool.exe -export -alias hpcert -file <path>/keystore**
     **-keystore /opt/HP/BSM/odb/conf/security/server.keystore**
     **-storepass hppass**

   コマンドの実行が終了すると、BSMまたはOMiのキーストア証明書は、指定したkeystoreファイルに保存されます。

b. BSMまたはOMiのゲートウェイサーバーで以下のコマンドを実行します。
   - Windowsの場合:
     **keytool.exe -export -alias clientcert -file <path>\truststore**
     **-keystore <drive>:\HPBSM\odb\conf\security\server.truststore**
     **-storepass hppass**
   - Linuxの場合:
     **keytool -export -alias clientcert -file <path>/truststore**
     **-keystore /opt/HP/BSM/odb/conf/security/server.truststore**
     **-storepass hppass**

   コマンドの実行が終了すると、BSMまたはOMiのトラストストア証明書は、指定したtruststoreファイルに保存されます。

c. 「BSMまたはOMiのゲートウェイサーバーで以下のコマンドを実行します。」(61ページ)で作成したkeystoreファイルおよび「BSMまたはOMiのゲートウェイサーバーで以下のコマンドを実行します。」(61ページ)で作成したtruststoreファイルをNNMi管理サーバーの一時ディレクトリにコピーします。残りのコマンドでは、これらのファイルはNNMi管理サーバーの以下の場所に存在しているものとして表示されます。
   - Windowsの場合:
     <drive>:\nnmi_temp\keystore
     <drive>:\nnmi_temp\truststore,
   - Linuxの場合:
     /nnmi_tmp/keystore
     /nnmi_tmp/truststore

d. キーストア証明書をマージするには、NNMi管理サーバーで以下のコマンドを実行します。
   - Windowsの場合:
     **keytool.exe -import -alias hpcert -keystore**
     **%NnmDataDir%\shared\nnm\certificates\nnm.keystore**
     **-storepass nnmkeypass -file <drive>:\nnmi_temp\keystore**
   - Linuxの場合:
     **keytool -import -alias hpcert -keystore**
     **$NnmDataDir/shared/nnm/certificates/nnm.keystore**
     **-storepass nnmkeypass -file /nnmi_tmp/keystore**

e. トラストストア証明書をマージするには、NNMi管理サーバーで以下のコマンドを実行します。
   - Windowsの場合:
     **keytool.exe -import -alias clientcert -keystore**
     **%NnmDataDir%\shared\nnm\certificates\nnm.truststore**
     **-storepass ovpass -file <drive>:\nnmi_temp\truststore**

- Linuxの場合:
  **keytool -import -alias clientcert -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass -file /nnmi_tmp/truststore**

f. BSMまたはOMiで自己署名証明書を使用している場合のみこの手順を実行してください(認証機関(CA)署名証明書でない場合)。BSMまたはOMiのキーストア証明書をNNMiトラストストアにマージするには、NNMi管理サーバーで以下のコマンドを実行します。

- Windowsの場合:
  **keytool.exe -import -alias <bsm_selfsigned_cert> -keystore %NnmDataDir%\shared\nnm\certificates\nnm.truststore -storepass ovpass -file <drive>:\temp\keystore**
- Linuxの場合:
  **keytool -import -alias <bsm_selfsigned_cert> -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass -file /tmp/keystore**

g. BSMまたはOMiで1つ以上の認証機関(CA)署名証明書を使用している場合のみこの手順を実行してください(自己署名証明書でない場合)。CAルート証明書およびCA中間証明書をNNMiトラストストアにインポートします。

各CA証明書を別々にインポートします。たとえば、CAルート証明書と1つのCA中間証明書をインポートするには、NNMi管理サーバーで以下のコマンドを実行します。

- Windowsの場合:
  **keytool.exe -import -alias <bsm_ca_root_cert> -keystore %NnmDataDir%\shared\nnm\certificates\nnm.truststore -storepass ovpass -file <drive>:\temp\keystore**
- **keytool.exe -import -alias <bsm_ca_intermediate_cert> -keystore %NnmDataDir%\shared\nnm\certificates\nnm.truststore -storepass ovpass -file <drive>:\temp\keystore**
- Linuxの場合:
  **keytool -import -alias <bsm_ca_root_cert> -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass -file /tmp/keystore**
- **keytool -import -alias <bsm_ca_intermediate_cert> -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass -file /tmp/keystore**

10. オプション: NNMi管理サーバーで、以下のコマンドを以下の順序で実行します。
    a. **ovstop**
    b. **ovstart**
11. オプション: NNMi管理サーバーとBSMサーバーかOMiゲートウェイサーバーの両方で、以下のコマンドを実行します。出力を比較して、両方のサーバーにキーストア証明書が存在することを確認します。
    - NNMi管理サーバー:
      - Windowsの場合: **keytool.exe -list -keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore -storepass nnmkeypass**
      - Linuxの場合: **keytool -list -keystore $NnmDataDir/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass**

- BSMまたはOMiゲートウェイサーバー:
  - Windowsの場合: **keytool.exe -list -keystore <drive>:\HPBSM\odb\conf\security\server.keystore -storepass hppass**
  - Linuxの場合: **keytool -list -keystore /opt/HP/BSM/odb/conf/security/server.keystore -storepass hppass**

12. オプション: NNMi管理サーバーとBSMサーバーかOMiゲートウェイサーバーの両方で、以下のコマンドを実行します。出力を比較して、両方のサーバーにトラストストア証明書が存在することを確認します。
    - NNMi管理サーバー:

      証明書を読み取り可能な形式で印刷するには、-vオプションを使用します。このオプションには証明書が有効な日付の範囲が含まれます。
      - Windowsの場合: **keytool.exe -list -keystore %NnmDataDir%\shared\nnm\certificates\nnm.truststore -storepass ovpass -v**
      - Linuxの場合: **keytool -list -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass -v**
    - BSMゲートウェイサーバー:
      - Windowsの場合: **keytool.exe -list -keystore <drive>:\HPBSM\odb\conf\security\server.truststore -storepass hppass -v**
      - Linuxの場合: **keytool -list -keystore /opt/HP/BSM/odb/conf/security/server.truststore -storepass hppass -v**
13. 証明書がまだ有効であることを確認するために、日付の範囲をチェックします。

# BSMエンドユーザー管理レポートから使用できるNNMiデータ

NNMi管理サーバーにリンクを設定しておけば、BSMユーザーは、一部のエンドユーザー管理レポートからNNMiデータにドリルダウンできます。NNMiでは、ソース(クライアント)マシンとデスティネーション(サーバー)マシン間のパスビュー(trace route)情報を表示できます。これにより、ネットワークの問題の根本原因や共通ネットワークの問題を特定しやすくなります。

また、BSMユーザーは、URLツールを使用してNNMiコンソールを起動し、NNMiの受信イベントをさらに分析することもできます。

## NNMiへのドリルダウンが可能なエンドユーザー管理レポート

「表8: NNMiへのドリルダウンが可能なエンドユーザー管理レポート」(64ページ)に、NNMiデータにドリルダウンできるエンドユーザー管理レポートを示します。「表8: NNMiへのドリルダウンが可能なエンドユーザー管理レポート」(64ページ)には、trace routeデータが表示される関連するソースマシンおよびデスティネーションマシンも記載されています。レポートタイプの詳細については、『BSMユーザ・ガイド』の「分析レポート」を参照してください。

**表8: NNMiへのドリルダウンが可能なエンドユーザー管理レポート**

| エンドユーザー管理レポート | ソースマシンとデスティネーションマシン |
|---|---|
| 経過時間ごとのアクションレポート | ソースIPアドレスとデスティネーションIPアドレス、および選択したアクションで最悪のネットワーク時間。複数のアクションがフィルターに含まれている場合、最初のアクションが使用されます。 |
| アクションの未処理データレポート | ソースIPアドレスとデスティネーションIPアドレス、および選択したアクションで最悪のネットワーク時間。 |
| RUMアクションの概要レポート | ソースIPアドレスとデスティネーションIPアドレス、および選択したアクションで最悪のネットワーク時間。 |
| 時間経過ごとのRUMエンドユーザーグループレポート | 要求/応答のソースIPアドレスとデスティネーションIPアドレス、および選択したアプリケーションで最悪のネットワーク時間。複数のエンドユーザーグループがフィルターに含まれている場合、最初のエンドユーザーグループが使用されます。<br><br>**注:** レポートがTCPアプリケーション、またはTCPデータを伴うWebアプリケーション用に生成されるときのみ、このレポートからNNMiにドリルダウンできます。 |
| RUMエンドユーザーグループの概要レポート | 要求/応答のソースIPアドレスとデスティネーションIPアドレス、および選択したアプリケーションで最悪のネットワーク時間。<br><br>**注:** このレポートからNNMiにドリルダウンするには、生成されるレポートがTCPアプリケーションまたはTCPデータを伴うWebアプリケーションのレポートである必要があります。 |
| RUM層の概要レポート | 要求/応答のソースIPアドレスとデスティネーションIPアドレス、および選択したアプリケーションで最悪のネットワーク時間。 |
| RUMトランザクションの概要レポート | ソースIPアドレスとデスティネーションIPアドレス、および選択したトランザクションで最悪のネットワーク時間。 |
| セッション詳細レポート | アクションサーバーとセッションクライアントのIPアドレス。 |
| 経過時間ごとの層レポート | 要求/応答のソースIPアドレスとデスティネーションIPアドレス、および選択したアプリケーションで最悪のネットワーク時間。 |
| 経過時間ごとのトランザクションレポート | ソースIPアドレスとデスティネーションIPアドレス、および選択したトランザクションで最悪のネットワーク時間。複数のトランザクションがフィルターに含まれている場合、最初のトランザクションが使用されます。 |

# NNMiデータへのドリルダウンの設定

エンドユーザー管理レポートからNNMiデータにドリルダウンできるようにするには、以下の手順を実行します。

1. 「BSMまたはOMiからのNNMiの視覚化の有効化」(65ページ)の説明に従って、BSMからNNMiへの接続を設定します (まだ行っていない場合)。
2. 「NNMiとBSM、OMi、またはUCMDB間のシングルサインオンの設定」(16ページ)の説明に従って、BSMとNNMi間のシングルサインオンを有効にします (まだ行っていない場合)。
3. 「HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合の有効化」(14ページ)の説明に従って、トポロジ情報をRTSMにプッシュするようにNNMiに設定します (まだ行っていない場合)。
4. オプション。BSMサーバーで、HPOprInfインフラストラクチャコンテンツパックをインストールして設定します。

   詳細については、『BSM Operations Management Extensibility Guide』を参照してください。

# BSMまたはOMiからのNNMiの視覚化の有効化

BSMからNNMiへの接続を設定して以下のデータを表示します。

- MyBSMのNNMiコンポーネント
- NNMiコンポーネント (OMiのマイワークスペース)
- エンドユーザー管理レポートからNNMiへのドリルダウン

BSMまたはOMiからNNMiへの接続を設定するには、以下の手順を実行します。

1. BSMの場合: BSMユーザーインタフェースで [**インフラストラクチャ設定**] ページを開きます (**[管理者] > [プラットフォーム] > [セットアップとメンテナンス] > [インフラストラクチャ設定]**)。

   OMiの場合: OMiユーザーインタフェースで [**インフラストラクチャ設定**] ページを開きます (**[管理] > [セットアップとメンテナンス] > [インフラストラクチャ設定]**)。
2. [**ファウンデーション**] を選択し、[**他のアプリケーションとの統合**] を選択します。
3. [**HP NNM**] テーブルで、以下のパラメーターを探して変更します。
   - **HP NNM統合URL**: NNMiコンソールにアクセスするためのURL。以下の形式の正しいURLを使用します。

     **<protocol> ://<fully_qualified_domain_name>:<port_number>**

     **<protocol>**はhttpまたはhttpsです。

     **<fully_qualified_domain_name>**は、NNMi管理サーバーの正式な完全修飾ドメイン名 (FQDN) です。

     **<port_number>**は、以下のファイルで指定するNNMiコンソールに接続するためのポートです。
     - Windowsの場合: `%NnmDataDir%\conf\nnm\props\nms-local.properties`
     - Linuxの場合: `$NnmDataDir/conf/nnm/props/nms-local.properties`

     SSL以外の接続では、`nmsas.server.port.web.http` (以前の`jboss.http.port`) の値を使用します。これはデフォルトでは`80`または`8004`です (NNMiがインストールされたときに別のWebサーバーが存在するかどうかで、どちらかが決まります)。

     SSL接続の場合は、`nmsas.server.port.web.https` (以前の`jboss.https.port`) の値 (デフォルトは`443`) を使用します。
   - **HP NNMiユーザー名**: NNMi Webサービスに接続するためのユーザー名。このユーザーは、NNMi AdministratorまたはWeb Service Clientのロールを持っている必要があります。
   - **HP NNMiユーザーパスワード**: 指定されたNNMiユーザー名のパスワード。

# NNMiとBSM/UMCDBの統合方法の比較

以下の表に、2つの方法の比較の概要を示します。

**表9: NNMiとBSM/UCMDBの統合方法の比較**

| NNMi-BSMトポロジの「プッシュ」統合 | プローブベースの「プル」統合 (「NNMに基づくレイヤー2」の検出ジョブ) |
|---|---|
| NNMiノードグループに基づいて、NNMiからBSMに同期するオブジェクトをフィルターできます。 | 現在、BSMに同期するNNMiオブジェクトをフィルターすることはできません。 |
| 増分検出およびスケジュールされた完全なトポロジ同期を実行します。 | 完全なトポロジ同期のみを実行します。 |
| すべてのNNMiノードをNode CIとして作成します。* | NNMiノードを各種CIタイプ (Router、Switch、Switch Router、Chassis、Computer、ATM Switch、Firewall、Load Balancer、Printer) として作成します。 |
| 他のCI (Interface、IpAddress、IpSubnet、Layer2Connection、HardwareBoard、PhysicalPort) を作成します。 | 他のCIInterface、IpAddress、IpSubnet、Layer2Connection、HardwareBoard+、PhysicalPort+、VLAN +を作成します。 |
| プローブの方法ではなくBSMで入力されるNode CI属性:<br>• Host is Route。<br>• Host is Virtual。<br>• NodeModel。<br>• PrimaryDnsName。 | BSMの方法ではなくプローブで入力されるNode CI属性:<br>• Description (Device Profile Descriptionから入力)<br>BSMの方法で各種値が入力されるNode CI属性:<br>• DiscoveredVendor (BSMの方法のユーザーフレンドリーな形式。例:「hewlettpackard」ではなく「Hewlett-Packard」)。<br>• NodeFamily (BSMの方法のユーザーフレンドリーな形式)。<br>• Host NNM UID。<br>• Host Key。 |
| Layer 2 Connection CI属性表示ラベルは、NNMiで表示されるLayer 2 Connection Nameに設定されます。 | Layer 2 Connection CI属性表示ラベルは、「Layer2Connection」にハードコードされています。<br>プローブで各種属性が入力されるその他のCI:<br>• HardwareBoard CIには、SoftwareVersion属性が含まれます。<br>• PhysicalPort CIには、DuplexSettingおよびPort Name (Nameと同じ値) 属性が含まれます。 |
| レイヤー2ネットワークの標準ビューを簡単に適合できます。 | レイヤー2ネットワークの標準ビュー。 |

+ これらのCIを作成するには、NNMi 9が必要です。

* ノードはNodeRole属性で識別されます。

**注:** UCMDBコンテンツパック9では、大規模なNNMi環境のNNMi統合のサポートが拡張されます。これにより、クエリーごとにNNMiから取得するLayer2Connections、VLAN、Nodeの数を制御できます。

# 新しいRTSMユーザーの作成

HPE NNMi–HPE BSM/OMi/UCMDBトポロジ統合の新しいRTSMユーザーを作成するには、以下の手順を実行します。

1. UCMDBコンソールを開きます。
2. [**セキュリティ**] を選択します。
3. [**ユーザとグループ**] をクリックします。
4. ユーザー名とパスワードを入力します。
5. ロールの関連付けの場合、[**検出と統合の管理**] を選択します。

BSM RTSMユーザーの新しいユーザー名とパスワードおよび [**HPE NNMi–HPE BSM/OMi/UCMDBトポロジの統合設定**] フォームのパスワードを入力します。

# NNMi - CI属性のマッピング

以下の図に、NNMiのオブジェクト属性とBSMまたはOMiの対応するCI属性のマッピングを示します。

**注: Monitored By**属性は、各CIタイプのNNMが含まれるように設定されています。

**表10: NNMiノード - Node CI属性のマッピング**

| NNMiノード属性 | Node CI属性 |
|---|---|
| ホスト名 | • PrimaryDnsName<br>• Name |
| システムの名前 | • SnmpSysName<br>• Name |
| システムのオブジェクトID | SysObjectId |
| システムの連絡先 | DiscoveredContact |
| システムのロケーション | DiscoveredLocation |
| システムの説明 | DiscoveredDescription |
| デバイスモデル | • NodeModel<br>• DiscoveredModel |
| デバイスのベンダー | DiscoveredVendor |
| デバイスのファミリー | NodeFamily |
| ケーパビリティ | NodeRole |
| PartitionID | BiosUuid |
| ケーパビリティ: IP転送 (レイヤー3) | Node Is Route |
| ケーパビリティ:仮想マシン | Node Is Virtual |
| UUID | • Host Key<br>• Host NNM UID |

**表11: NNMiインタフェース - Interface CI属性のマッピング**

| NNMiインタフェース属性 | Interface CI属性 |
|---|---|
| 物理アドレス | MacAddress |

**表11: NNMiインタフェース - Interface CI属性のマッピング (続き)**

| NNMiインタフェース属性 | Interface CI属性 |
|---|---|
| ifName | InterfaceName |
| ifAlias | InterfaceAlias |
| ifDescr | InterfaceDescription |
| ifIndex | InterfaceIndex |
| ifSpeed | InterfaceSpeed |
| ifType | InterfaceType |

**表12: NNMi IPアドレス - IpAddress CIのマッピング**

| NNMi IPアドレス属性 | IpAddress CI属性 |
|---|---|
| アドレス | • IPアドレス<br>• Name<br>• IpAddressType<br>• IpAddressValue |

**表13: NNMi IPサブネット - IpSubnet CI属性のマッピング**

| NNMi IPサブネット属性 | IpSubnet CI属性 |
|---|---|
| プレフィックス | • Name<br>• IpAddressType<br>• IpAddressValue |
| プレフィックス長 | IpPrefixLength |

**表14: NNMiカード - HardwareBoard CI属性のマッピング**

| NNMiカード属性 | HardwareBoard CI属性 |
|---|---|
| 名前 | Name |
| シリアル番号 | SerialNumber |
| ファームウェアバージョン | FirmwareVersion |
| ハードウェアバージョン | HardwareVersion |
| インデックス | BoardIndex |

**表15: NNMiポート - PhysicalPort CI属性のマッピング**

| NNMiポート属性 | PhysicalPort CI属性 |
|---|---|
| 名前 | Name |
| ポートインデックス | PortIndex |

**表16: NNMiレイヤー2接続 - Layer2Connection CI属性のマッピング**

| NNMiレイヤー2接続属性 | Layer2Connection CI属性 |
|---|---|
| 名前 | Name |

**表17: NNMi VLAN - Vlan CI属性のマッピング**

| VLAN属性 | Vlan CI属性 |
|---|---|
| 名前 | VLAN名 |
| VLAN ID | • Vlanid<br>• Name |

# NNMi環境変数

HPE Network Node Manager i Software (NNMi) には、ファイルシステム内の移動やスクリプトの作成に使用できる多数の環境変数があります。

この付録では、以下の内容を記載しています。



# このドキュメントで使用する環境変数

このドキュメントでは、主に以下の2つのNNMi環境変数を使用して、ファイルやディレクトリの場所を参照します。以下に示す変数はデフォルト値です。実際の値は、NNMiのインストール時に行った選択内容によって異なります。

- Windows Serverの場合:
  - `%NnmInstallDir%:<drive>\Program Files (x86)\HP\HP BTO Software`
  - `%NnmDataDir%:<drive>\ProgramData\HP\HP BTO Software`

    **注:** Windowsシステムでは、NNMiのインストールプロセスによってこれらのシステム環境変数が作成されるため、すべてのユーザーがいつでも使用できます。

- Linuxの場合:
  - `$NnmInstallDir:/opt/OV`
  - `$NnmDataDir:/var/opt/OV`

    **注:** Linuxシステムでは、これらの環境変数を使用するには、手動で作成する必要があります。

また、このドキュメントには、NNMi管理サーバーでユーザーログオン設定を行うときに使用するNNMi環境変数も一部掲載されています。これらの変数の形式は`NNM_*`です。NNMi環境変数の詳細リストについては、「他の使用可能な環境変数」(72ページ)を参照してください。

# 他の使用可能な環境変数

NNMi管理者は、いくつかのNNMiファイルの場所に定期的にアクセスします。NNMiには、通常アクセスする場所へ移動するためのさまざまな環境変数を設定するスクリプトが用意されています。

NNMi環境変数の拡張リストをセットアップするには、次の例のようなコマンドを使用します。

- Windowsの場合: `"C:\Program Files (x86)\HP\HP BTO Software\bin\nnm.envvars.bat"`
- Linuxの場合: `. /opt/OV/bin/nnm.envvars.sh`

上記の各OS用のコマンドを実行した後で、「表 18: Windows OSでの環境変数のデフォルトの場所」(Windows)または「表 19: Linux OSでの環境変数のデフォルトの場所」(Linux)で示すNNMi環境変数を使用して、頻繁に使用するNNMiファイルの場所に移動できます。

**表 18: Windows OSでの環境変数のデフォルトの場所**

| 変数 | Windows (例) |
|---|---|
| %NNM_BIN% | C:\Program Files (x86)\HP\HP BTO Software\bin |
| %NNM_CONF% | C:\ProgramData\HP\HP BTO Software\conf |
| %NNM_DATA% | C:\ProgramData\HP\HP BTO Software\ |
| %NNM_DB% | C:\ProgramData\HP\HP BTO Software\shared\nnm\databases |
| %NNM_JAVA% | C:\Program Files (x86)\HP\HP BTO Software\nonOV\jdk\hpsw\bin\java.exe |
| %NNM_JAVA_DIR% | C:\Program Files (x86)\HP\HP BTO Software\java |
| %NNM_JAVA_PATH_SEP% | ; |
| %NNM_JBOSS% | C:\Program Files (x86)\HP\HP BTO Software\nmsas |
| %NNM_JBOSS_DEPLOY% | C:\Program Files (x86)\HP\HP BTO Software\nmsas\server\nms\deploy |
| %NNM_JBOSS_LOG% | C:\ProgramData\HP\HP BTO Software\log\nnm |
| %NNM_JBOSS_SERVERCONF% | C:\Program Files (x86)\HP\HP BTO Software\nmsas\server\nms |
| %NNM_JRE% | C:\Program Files (x86)\HP\HP BTO Software\nonOV\jdk\hpsw |
| %NNM_LOG% | C:\ProgramData\HP\HP BTO Software\log |
| %NNM_LRF% | C:\ProgramData\HP\HP BTO Software\shared\nnm\lrf |
| %NNM_PRIV_LOG% | C:\ProgramData\HP\HP BTO Software\log |
| %NNM_PROPS% | C:\ProgramData\HP\HP BTO Software\shared\nnm\conf\props |
| %NNM_SHARED_CONF% | C:\ProgramData\HP\HP BTO Software\shared\nnm\conf |
| %NNM_SHARE_LOG% | C:\ProgramData\HP\HP BTO Software\log |
| %NNM_SNMP_MIBS% | C:\Program Files (x86)\HP\HP BTO Software\misc\nnm\snmp-mibs |
| %NNM_SUPPORT% | C:\Program Files (x86)\HP\HP BTO Software\support |
| %NNM_TMP% | C:\ProgramData\HP\HP BTO Software\tmp |
| %NNM_USER_SNMP_MIBS% | C:\ProgramData\HP\HP BTO Software\shared\nnm\user-snmp-mibs |
| %NNM_WWW% | C:\ProgramData\HP\HP BTO Software\shared\nnm\www |

**表19: Linux OSでの環境変数のデフォルトの場所**

| 変数 | Linux |
|---|---|
| $NNM_BIN | /opt/OV/bin |
| $NNM_CONF | /var/opt/OV/conf |
| $NNM_DATA | /var/opt/OV |
| $NNM_DB | /var/opt/OV/shared/nnm/databases |
| $NNM_JAVA | /opt/OV/nonOV/jdk/hpsw/bin/java |
| $NNM_JAVA_DIR | /opt/OV/java |
| $NNM_JAVA_PATH_SEP | : |
| $NNM_JBOSS | /opt/OV/nmsas |
| $NNM_JBOSS_DEPLOY | /opt/OV/nmsas/server/nms/deploy |
| $NNM_JBOSS_LOG | /var/opt/OV/log/nnm |
| $NNM_JBOSS_SERVERCONF | /opt/OV/nmsas/server/nms |
| $NNM_JRE | /opt/OV/nonOV/jdk/hpsw |
| $NNM_LOG | /var/opt/OV/log |
| $NNM_LRF | /var/opt/OV/shared/nnm/lrf |
| $NNM_PRIV_LOG | /var/opt/OV/log |
| $NNM_PROPS | /var/opt/OV/shared/nnm/conf/props |
| $NNM_SHARED_CONF | /var/opt/OV/shared/nnm/conf |
| $NNM_SHARE_LOG | /var/opt/OV/log |
| $NNM_SNMP_MIBS | /opt/OV/misc/nnm/snmp-mibs |
| $NNM_SUPPORT | /opt/OV/support |
| $NNM_TMP | /var/opt/OV/tmp |
| $NNM_USER_SNMP_MIBS | /var/opt/OV/shared/nnm/user-snmp-mibs |
| $NNM_WWW | /var/opt/OV/shared/nnm/www |

# フィードバックをお寄せください

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

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

**製品名およびバージョン:**NNMi 10.20

**ドキュメントタイトル:**HPE Network Node Manager i Software—HPE Business Service Management統合ガイド、2016年7月

**フィードバック:**