

HP Network Node Manager i Software

Windows® および Linux オペレーティングシステム用

ソフトウェアバージョン : NNMi 10.00

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

ドキュメントリリース日 : 2014 年 5 月
ソフトウェアリリース日 : 2014 年 5 月



ご注意

保証について

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

ここに記載されている情報は、予告なく変更されることがあります。

権利制限について

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、HP 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。

著作権について

© Copyright 2008–2014 Hewlett-Packard Development Company, L.P.

商標に関する通知

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

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

Microsoft® および Windows® は Microsoft Corporation の米国内での登録商標です。

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

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

UNIX® は The Open Group の登録商標です。

Oracle テクノロジーの制限された権限に関する通知

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 社のライセンス契約に規定された制約を受けるものとします。それ以外の場合は、連邦調達規則に従って供給されたプログラムは、「制限されたコンピューターソフトウェア」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。

謝辞

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

この製品には、Indiana University Extreme!Lab で開発されたソフトウェアが含まれています。
(<http://www.extreme.indiana.edu>)

使用可能な製品ドキュメント

このガイドに加え、次のドキュメントが NNMi について利用できます。

- **HP Network Node Manager i Software** ドキュメント一覧 — HP マニュアル Web サイト上にあります。このファイルを使用して、このバージョンの NNMi の NNMi ドキュメントセットにある追加や改訂を調べることができます。リンクをクリックして、HP マニュアル Web サイト上のドキュメントにアクセスします。
- **NNMi インストールガイド** — これは対話型ドキュメントで、NNMi 製品メディアで入手できます。詳細については、製品メディアの `nnmi_interactive_installation_ja_README.txt` ファイルを参照してください。
- 『**HP Network Node Manager i Software アップグレードリファレンス**』 — HP マニュアル Web サイトから入手できます。
- **HP Network Node Manager i Software** リリースノート — 製品メディアおよび NNMi 管理サーバーから入手できます。
- **HP Network Node Manager i Software** システムおよびデバイス対応マトリックス — 製品メディアおよび NNMi 管理サーバーから入手できます。
- 『**HP Network Node Manager iSPI Network Engineering Toolset 計画とインストールガイド**』(HP Network Node Manager iSPI Network Engineering Toolset Planning and Installation Guide) — NNM iSPI NET 診断サーバー製品メディアにあります。

最近の更新を確認する場合、または最新のドキュメントを使用しているか確認する場合は、以下をご覧ください。

<http://h20230.www2.hp.com/selfsolve/manuals>

このサイトを利用するには、HP Passport への登録とサインインが必要です。HP Passport ID を登録するには、以下にアクセスします。

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

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

製品のサポートサービスに登録すると、最新版を入手できます。詳細については、HP 営業担当者にお問い合わせください。

サポート

次の HP ソフトウェアサポートオンライン Web サイトを参照してください。

www.hp.com/go/hpsoftwaresupport

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

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

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

一部を除き、サポートのご利用には、HP Passport ユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HP Passport ユーザー ID のご登録は、以下の URL で行ってください。

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

アクセスレベルに関する詳細については、以下の URL で確認してください。

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

2014 年 5 月

目次

NNMi と HP BSM Operations Management を統合する方法の比較.....	9
HP NNMi-HP BSM Operations Management 統合.....	12
HPOM および HP BSM Operations Management と統合される NNMi	13
BSM の NNMi の視覚化.....	13
HP NNMi-HP BSM/UCMDB トポロジ統合.....	16
値.....	16
統合製品.....	16
ドキュメント.....	17
トポロジを UCMDB システムと同期するための HP NNMi と HP BSM/USMCDB の統合の有効化.....	17
HP NNMi-HP BSM/UCMDB トポロジ統合の有効化.....	20
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.....	22
[BSM/UCMDB で影響を受ける CI を検出]機能の有効化.....	22
HP NNMi-HP BSM/UCMDB トポロジ統合の使用法.....	25
統合が提供する追加の NNMi 機能.....	27
NNMi コンソールからの BSM または UCMDB 影響分析の実行.....	27
HP NNMi-HP BSM/UCMDB トポロジ統合設定の変更.....	28
HP NNMi-HP BSM/UCMDB トポロジ統合の無効化.....	28
HP NNMi-HP BSM/UCMDB トポロジ統合のトラブルシューティング.....	28
BSM ユーザーインターフェースでインターフェースラベルが MAC アドレスとして表示される.....	28
RTSM の管理対象ノードで CI が重複する.....	29
アプリケーションフェイルオーバーと HP NNMi-HP BSM/UCMDB トポロジ統合.....	29
HP NNMi-HP BSM/UCMDB [トポロジの統合設定]フォームのリファレンス.....	29
NNMi 管理サーバー接続.....	29
BSM ゲートウェイサーバーまたは UCMDB サーバー接続.....	30
設定項目トポロジフィルター.....	31
ノードトポロジフィルター.....	32
HP NNMi-HP UCMDB 統合.....	35
値.....	36
統合製品.....	36
ドキュメント.....	36
HP NNMi-HP UCMDB 統合の使用法.....	37
HP NNMi と HP UCMDB 間のシングルサインオンの設定.....	37
HP NNMi-HP BSM Operations Management 統合.....	39
値.....	40
統合製品.....	40
ドキュメント.....	41

HP NNMi—HP BSM Operations Management 統合の有効化.....	41
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	44
HP NNMi—HP BSM Operations Management 統合の使用法.....	45
設定項目の ID	46
ヘルスインジケータ	46
デフォルトのポリシー条件	46
ポリシー条件のカスタマイズ.....	47
詳細情報.....	48
HP NNMi—HP BSM Operations Management 統合の変更	48
新規 NNMi トラップの SNMP トラップポリシー条件の更新	48
設定パラメーターの変更	49
HP NNMi—HP BSM Operations Management 統合の無効化.....	50
HP NNMi—HP BSM Operations Management 統合のトラブルシューティング	50
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.....	50
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	53
NNMi[—HPOM Agent デスティネーション] フォームリファレンス (BSM Operations Management 統合).....	53
BSM Connector 接続.....	54
BSM Operations Management 統合コンテンツ.....	54
BSM Connector 転送先のステータス情報.....	56
MyBSM ポータル	59
MyBSM で使用できる NNMi コンポーネント	60
MyBSM の NNMi コンポーネントの表示.....	60
NNMi と BSM または UCMDB 間のシングルサインオンの設定	61
BSM への SSL 接続の設定.....	62
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	66
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	67
NNMi データへのドリルダウンの設定	68
BSM からの NNMi の視覚化の有効化	68

HP Business Service Management 概要

HP 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。

この章では、NNMi と BSM 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 と HP BSM Operations Management を統合する方法の比較](#) ページ 9
- [HP NNMi—HP BSM Operations Management 統合](#) ページ 12
- [HPOM および HP BSM Operations Management と統合される NNMi](#) ページ 13
- [BSM の NNMi の視覚化](#) ページ 13

NNMi と HP BSM Operations Management を統合する方法の比較

表 1 に、HP NNMi—HP BSM Operations Management 統合と HP 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、[HP NNMi—HP BSM Operations Management 統合](#) ページ 12 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 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	<p>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。)</p> <p>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。</p> <ol style="list-style-type: none"> 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。 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。 <p>Windows の場合：</p> <ul style="list-style-type: none"> — <BSM_Root_Directory>%opr%\bin%\ConfigExchange.bat -username <username> -password <password> uploadOM -input <policy header file> <p>または</p> <ul style="list-style-type: none"> — <BSM_Root_Directory>%opr%\bin%\ConfigExchange.bat -username <username> -password <password> -uploadOM -input <dir in which the policy header file is located> <p>Linux の場合：</p> <ul style="list-style-type: none"> — <BSM_Root_Directory>%opr%\bin%\ConfigExchange -username <username> -password <password> uploadOM -input <policy header file> <p>または</p> <ul style="list-style-type: none"> — <BSM_Root_Directory>%opr%\bin%\ConfigExchange -username <username> -password <password> -uploadOM -input <dir in which the policy header file is located> <p>BSM Connector OM Agent 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。</p> <p>HP NNMi—HP BSM Operations Management 統合の有効化 ページ 41 も参照してください。</p>	<p>イベントに説明テキストを含めることができます。</p>

表 1 NNMi と BSM Operations Management 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
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 エージェントおよびポリシーで 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 管理サーバーの BSM Connector 間でポリシーを手動で交換する必要があります。	HP 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 エージェントライセンスでは、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。	<ul style="list-style-type: none"> • HP NNMi—HPOM 統合のエージェント実装は 1 方向です。 • HP 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。

HP NNMi—HP BSM Operations Management 統合

HP NNMi—HP 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 NNMi 管理サーバーの BSM Connector に転送します。BSM Connector は、NNMi トラップをフィルターし、それを HP BSM Operations Management イベントブラウザーに転送します。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。

HP NNMi—HP 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。

NNMi イベントで、対応するヘルスインジケーターが定義されている場合、これらのヘルスインジケーターは、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、HP 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ー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ー ページ 46 を参照してください。

詳細については、HP NNMi—HP BSM Operations Management 統合 ページ 39 を参照してください。

HPOM および HP 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および BSM Operations Management イベントブラウザに NNMi 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、HP 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』(BSM - Operations Manager Integration Guide) の説明に従って、BSM Operations Management イベントブラウザとの HPOM 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。

- 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 ページ 59](#) を参照してください。
- BSM Operations Management イベントブラウザ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、[HP NNMi—HP BSM Operations Management 統合の使用法 ページ 45](#) を参照してください。

HP Business Service Management およ び HP Universal CMDB

NNMi 10.00 以降では、HP NNMi-HP BSM/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ー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ー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。

HP Business 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、『HP NNMi - HP BSM トポロジ統合のベストプラクティス』(HP NNMi - HP BSM Topology Integration Best Practices) を参照してください。

BSM 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。

- [HP NNMi-HP BSM/UCMDB トポロジ統合](#)
- [Enabling the HP NNMi-HP BSM/UCMDB Integration to Synchronize Topology to the UCMDB System](#)
- [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](#)
- [HP NNMi-HP BSM/UCMDB トポロジ統合の使用法](#)
- [HP NNMi-HP BSM/UCMDB トポロジ統合設定の変更](#)
- [HP NNMi-HP BSM/UCMDB トポロジ統合の無効化](#)
- [HP NNMi-HP BSM/UCMDB トポロジ統合のトラブルシューティング](#)
- [アプリケーションフェイルオーバーと HP NNMi-HP BSM/UCMDB トポロジ統合](#)
- [HP NNMi-HP BSM/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 トポロジ統合

HP NNMi–HP BSM/UCMDB トポロジ統合では、NNMi トポロジを **BSM 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。
- BSM Real User Monitor (RUM) から使用可能なパスヘルスビュー。
- HP NNMi–HPOM 統合のエージェント実装を使用して **BSM Connector** を指し示すことで、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 ページ 46](#) を参照してください。
- HP 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 エージェントを指し示すことで、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ー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

HP NNMi–HP BSM/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ー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
- UCMDB



サポートされるバージョンは、NNMi システムとデバイス対応マトリックスにリストされています。

- NNMi 10.00

NNMi と BSM 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 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。

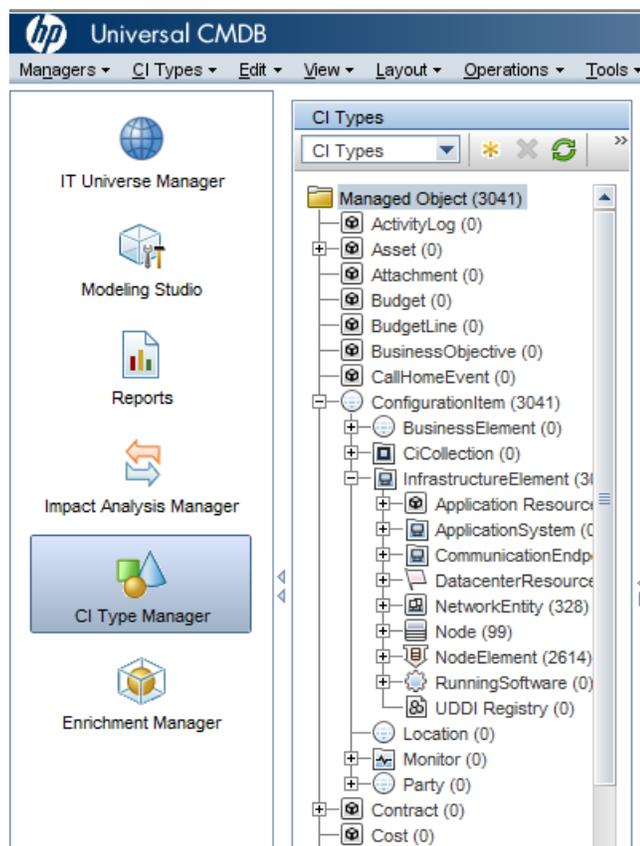
トポロジを UCMDB システムと同期するための HP NNMi と HP BSM/USMCDB の統合の有効化

トポロジを UCMDB システムと同期するには、特定の CI タイプごとに UCMDB の CI タイプモデルの **[monitored by]** 属性を追加して、HP NNMi と HP BSM/USMCDB の統合を有効にする必要があります。

注：この同期は BSM/RTSM には適用されません。

- 1 UCMDB コンソールを開きます。
- 2 **[CI タイプマネージャー]** を選択します。

- 3 [設定項目] > [インフラストラクチャ要素] の順に展開します。



- 4 [ネットワークエンティティ] を選択します。
- 5 [属性] タブに移動します。
- 6 [+] (追加) をクリックします。
- 7 [属性の追加] ダイアログで、以下の値を入力します。
 - a 属性名 : **monitored_by**
 - b 表示名 : **Monitored By**
- 8 [属性タイプ] セクションで、以下の手順を実行します。
 - a [プリミティブ] を選択します。

b [文字列のリスト] を選択します。

The screenshot shows the 'Add Attribute' dialog box with the following configuration:

- Attribute Name: `monitored_by`
- Display Name: `Monitored By`
- Scope: `CMS`
- Attribute Type: `Primitive` (selected), `list of strings` (selected from dropdown)
- Value Size: (empty)
- Default Value: (empty, with a '+' icon for adding)

- 9 [OK] をクリックします。
- 10 [NodeElement] を選択します。
- 11 [属性] タブに移動します。
- 12 [+] (追加) をクリックします。
- 13 [属性の追加] ダイアログで、以下の値を入力します。
 - a 属性名: `monitored_by`
 - b 表示名: `Monitored By`
- 14 [属性タイプ] セクションで、以下の手順を実行します。
 - a [プリミティブ] を選択します。
 - b [文字列のリスト] を選択します。
- 15 [OK] をクリックします。

HP NNMi-HP BSM/UCMDB トポロジ統合の有効化



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が、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 HP NNMi-HP BSM/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 の情報が必要な場合は、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、HP NNMi-HP BSM/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。UCMDB 製品のこのマニュアルは、次の URL から入手することもできます。
<http://h20230.www2.hp.com/selfsolve/manuals>

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

- 1 前提条件: BSM 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 プラットフォーム管理ガイド』の「ライセンス管理の概要」または『UCMDB インストールおよび設定ガイド』の「ライセンス」を参照してください。
- 2 前提条件: トポロジを UCMDB システムと同期するため、特定の CI タイプごとに UCMDB の CI タイプモデルの [monitored by] 属性を追加して統合を有効にしたことを確認してください。「トポロジを UCMDB システムと同期するための HP NNMi と HP BSM/USMCDB の統合の有効化」を参照してください。
- 3 省略可能: 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 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])。
 - 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
```
- 4 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/UCMDB トポロジ])。
- 5 [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。
- 6 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 ページ 29 を参照してください。
- 7 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 ゲートウェイサーバーまたは UCMDB サーバー接続 ページ 30 を参照してください。
- 8 省略可能: 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。

- 9 省略可能：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 ページ 31](#) を参照してください。
- 10 省略可能：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 ページ 32](#) を参照してください。
- 11 省略可能：[**トポロジ同期間隔 (時間)**] を調整し、完全なトポロジ同期間隔を増やします。

HP NNMi-HP BSM/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 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。

- 12 [**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 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。

- 13 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。



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 10.00 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。

- 14 同じ初期化ストリング値を使用して、BSM 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。BSM の初期化ストリング値の設定については、『[BSM プラットフォーム管理ガイド](#)』の「[認証ウィザード \(Authentication Wizard\)](#)」を参照してください。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、[NNMi と BSM または UCMDB 間のシングルサインオンの設定 ページ 61](#) を参照してください。
- 15 BSM で NNMi データを表示したり、MyBSM で NNMi コンポーネントにアクセスしたりするには、[BSM からの NNMi の視覚化の有効化 ページ 68](#) の手順を実行します。
- 16 MyBSM で使用できる NNMi コンポーネント [ページ 60](#) 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 ページ 67](#) の説明に従って、MyBSM および EUM で NNMi データを表示できます。

BSM 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。

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 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/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ている任意の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一例にすぎません。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。

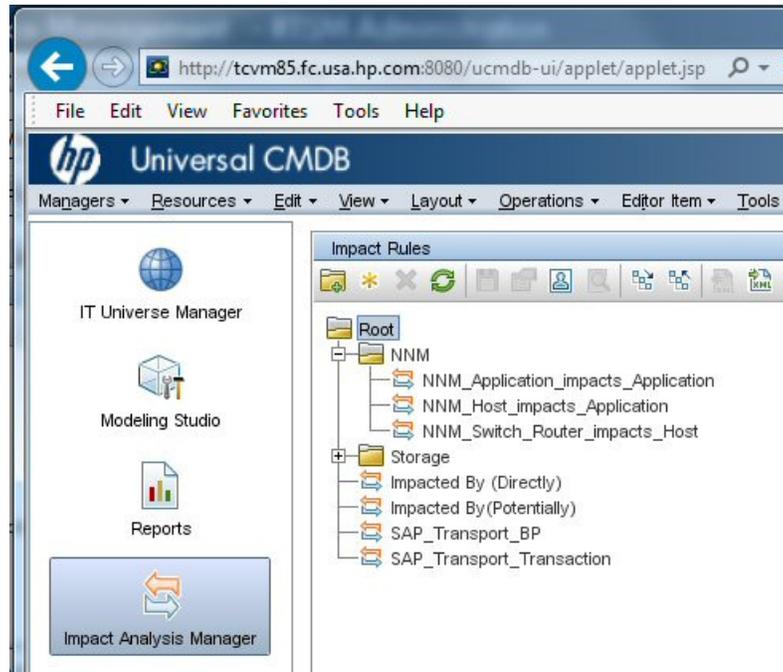
詳細については、『NNMi デプロイメントリファレンス』の「NNMi の文字セットエンコードの設定」を参照してください。

[BSM/UCMDB で影響を受ける CI を検出] 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。

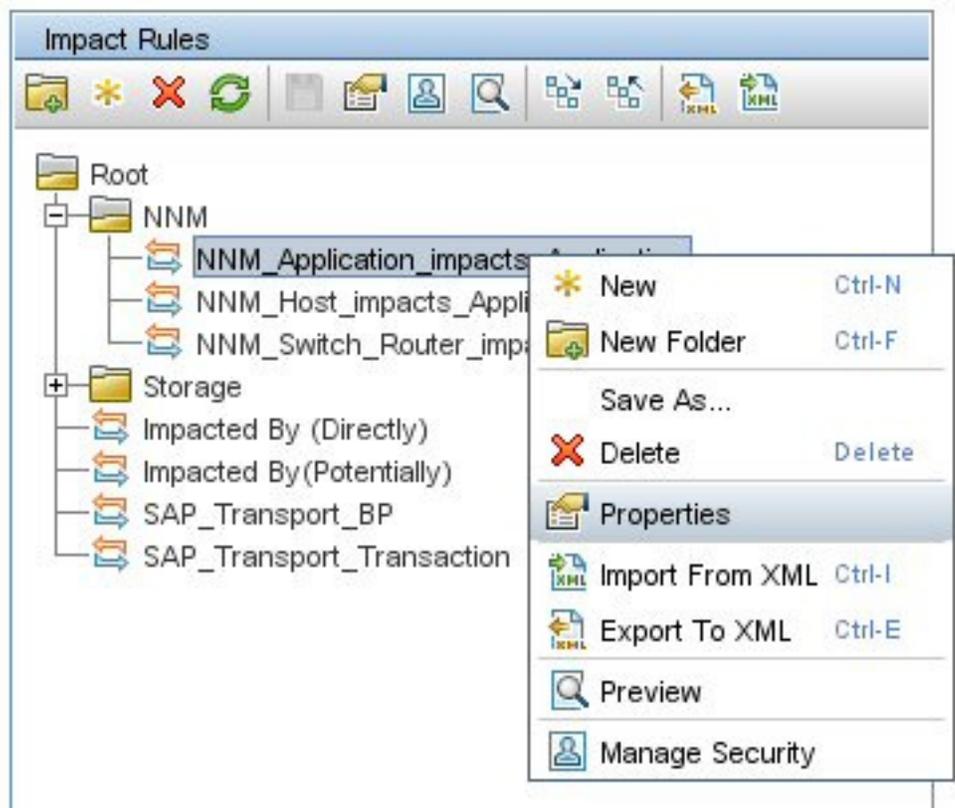
注意: NNMi-BSM 統合を有効にするときにデフォルトの [NNMi] ルールバンドルを選択し、以下の手順の説明に従って [影響分析マネージャー] を使用して提供されるルールを NNMi ルールバンドルに追加しないと、CI のセットが空になります。

- 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/NNMi] 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 [HP NNMi-HP BSM/UCMDB トポロジ統合の有効化の説明](#)に従って NNMi-BSM 統合を有効にしてください。



HP NNMi-HP BSM/UCMDB トポロジ統合の使用法

HP NNMi-HP BSM/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 ページ 32 の説明に従って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ーフェース。
- **InfrastructureElement > NetworkEntity > IPAddress**
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 に関連付けられたインターフェースの 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。



HP NNMi-HP UCMDB 統合では、これらのシャーン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、これらのシャーン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 のシャーン要素と UCMDB/RTSM の CI のシャーン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 UCMDDB 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 UCMDDB 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 ページ 31](#) 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 Layer 2 接続。

- InfrastructureElement > NetworkEntity > Vlan

統合によって BSM 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 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。



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 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。

HP NNMi-HP BSM/UCMDB トポロジ統合は、一方向通信で NNMi 情報と更新を BSM 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 CI のエージング設定に依存します。



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」(CI Lifecycle and the Aging Mechanism) 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、HP NNMi-HP BSM/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。

統合が提供する追加の NNMi 機能

HP NNMi-HP BSM/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 または UCMDB 影響分析の実行

HP NNMi-HP BSM/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。

HP NNMi-HP BSM/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。

HP NNMi-HP BSM/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、[HP NNMi-HP BSM/UCMDB \[トポロジの統合設定\] フォームのリファレンス ページ 29](#) 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。

▶ 変更はただちに有効になります。

HP NNMi-HP BSM/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。

▶ 変更はただちに有効になります。

HP NNMi-HP BSM/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。

- BSM ユーザーインターフェイスでインターフェースラベルが MAC アドレスとして表示される [ページ 28](#)
- RTSM の管理対象ノードで CI が重複する [ページ 29](#)

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ユーザーインターフェイスでインターフェースラベルがMACアドレスとして表示される

RTSM または UCMDB モデルでは、インターフェースラベルとしてインターフェイス名よりも 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ーフェイス名を表示するには、[20 ページの手順 1](#) の説明に従ってインターフェイ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、NNMi 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 HP NNMi-HP BSM/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、HP NNMi-HP BSM/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 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。

HP NNMi-HP BSM/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 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。



Administrator 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 ページ 29](#)
- [BSM ゲートウェイサーバーまたは UCMDB サーバー接続 ページ 30](#)
- [ノードトポロジフィルター ページ 32](#)

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

30 ページの表 2 に、NNMi 管理サーバーへの接続パラメーターをリストします。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	<p>接続プロトコル指定。</p> <ul style="list-style-type: none"> • 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。 • 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。 <p>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。</p>
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 ゲートウェイサーバーまたは UCMDB サーバー接続

表 3 には、BSM 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がリストされています。BSM 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。



設定フォームの BSM への参照は、BSM 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 ゲートウェイサーバーまたは UCMDB サーバーパラメーター	説明
BSM SSL 有効化	<p>BSM または UCMDB に接続するための接続プロトコルの指定。</p> <ul style="list-style-type: none"> • HTTPS を使用するように BSM 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。 • HTTP を使用するように BSM 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。 • 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 10.00 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または UCMDB サーバーの完全修飾ドメイン名。
BSM ポート	<p>BSM または UCMDB に接続するためのポート。</p> <p>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。</p> <p>BSM および UCMDB のデフォルトの https ポートは 8443 です。</p>

表3 BSM ゲートウェイサーバー情報 (続き)

BSM ゲートウェイサーバーまたは UCMDB サーバーパラメーター	説明
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	<p>BSM RTSM または UCMDB 管理者のパスワード。</p> <p>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。内部 RTSM にアクセスして、RTSM ユーザーを設定するには、以下の手順を実行します。</p> <p>createIntegrationUser オプションを使用して、以下の手順を実行できます。詳細については、『HP NNMi - HP BSM トポロジ統合のベストプラクティス』(HP NNMi - HP BSM Topology Integration Best Practices) を参照してください。</p> <ol style="list-style-type: none"> 分散 BSM 配備を使用している場合、BSM Data Processing サーバー (DPS サーバー) にログオンします。通常の BSM 配備を使用している場合、BSM サーバーにログオンします。 <p>リモートデスクトッププロトコル (RDP) (Windows DPS サーバーの場合) または仮想ネットワークコンピューティング (VNC) (Linux DPS サーバーの場合) を使用できます。</p> <ol style="list-style-type: none"> ブラウザのアドレスバーで <code>http://localhost:21212/jmx-console/</code> という URL を指定して、RTSM または UCMDB JMX コンソールをローカルで開きます。 UCMDB:service=Security Services に移動します。 JMX createuser コマンドを使用して、NNMi-BSM 統合モジュールで使用する名前およびパスワードに一致する新しいユーザーを作成します。 <pre>CustomerId = 1 userName = <userName> password = <password></pre> UCMDB:service=Security Services に移動し、JMX setRolesForUser コマンドを使用して、手順 4 で作成した新しいユーザーに管理者ロールを割り当てます。 <pre>CustomerId = 1 userName = <userName> roles = Admin</pre>

設定項目トポロジフィルター

HP NNMi-HP BSM/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、HP NNMi-HP BSM/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ー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ー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 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は、ノードトポロジフィルターを指定するためのパラメーター（省略可能）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	<p>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。</p> <p>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。</p> <p>トポロジフィルターノードグループを指定しない場合、HP NNMi-HP BSM/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。</p>
追加接続ノードグループ	<p>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。</p> <p>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。</p> <p>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、HP NNMi-HP BSM/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。</p> <p>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、HP NNMi-HP BSM/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みのノードとインタフェースに関する情報を転送します。</p> <p>トポロジフィルターノードグループを指定しない場合、HP NNMi-HP BSM/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。</p>

HP Universal CMDB

NNMi 9.00 より古いバージョンの NNMi 製品に対する下位互換性を確保するには、HP NNMi-HP UCMBD 統合をお勧めします。この推奨される統合は、[HP NNMi-HP BSM/UCMBD トポロジ統合](#) ページ 16 で説明されている HP NNMi-HP BSM/UCMBD トポロジ統合とは異なります。HP NNMi-HP UCMBD 統合では、NNMi インベントリのより静的なスナップショットを使用し、設定または資産管理でより役立ちます。

HP Universal CMDB (HP UCMBD) は、HP Discovery and Dependency mapping (DDM、検出および依存関係マッピング) へのネイティブ統合によって、インフラストラクチャーとアプリケーションの関係についての情報を定期的に維持します。

HP UCMBD は以下のタスクで役立ちます。

- 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ー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。
- 既存のデータ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。

HP UCMBD 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。

- [HP NNMi-HP UCMBD 統合](#)
- [HP NNMi-HP UCMBD 統合の使用法](#)
- [HP NNMi と HP UCMBD 間のシングルサインオンの設定](#)

HP NNMi-HP UCMBD 統合

HP NNMi-HP UCMBD 統合は、NNMi トポロジ情報を HP UCMBD と共有します。HP UCMBD は、設定項目 (CI) として各デバイスを NNMi トポロジに保存します。HP UCMBD は、Discovery and Dependency Mapping (DDM、検出と依存関係マッピング) パターンを NNMi トポロジ用の CI に適用し、デバイス障害の影響を予測します。この影響分析は、HP UCMBD ユーザーインターフェースおよび NNMi コンソールから入手できます。



この章の HP NNMi-HP UCMBD 統合情報は、NNMi と HP Universal CMDB バージョン 9.0x 間の統合を指します。

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。

- HP NNMi–HP 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 UCMDB CI に関連付けることができます。詳細については、設定項目の ID ページ 46 を参照してください。
- HP NNMi–HPOM 統合のエージェント実装では、NNMi 管理対象デバイスに関するインシデントを UCMDB CI に関連付けることができます。詳細については、設定項目の ID ページ 46 を参照してください。

値

HP NNMi–HP UCMDB 統合では、NNMi をネットワークデバイス関係の信頼できるソースとして設定します。この統合では、UCMDB 影響分析と CI の詳細に NNMi コンソールからアクセスできます。

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 UCMDB.



サポートされるバージョンは、NNMi システムとデバイス対応マトリックスにリストされています。

- NNMi 10.00

NNMi と HP UCMDB 9.0x は同じコンピューターにインストールできません。これら 2 つの製品は、以下の構成のどちらかである異なるコンピューターにインストールする必要があります。

- 異なるオペレーティングシステム。たとえば、NNMi 管理サーバーを Linux システムにし、UCMDB 9.0x サーバーを Windows システムにします。
- 同じオペレーティングシステム。たとえば、NNMi 管理サーバーを Windows システムにし、UCMDB 9.0x サーバーを 2 番目の Windows システムにします。

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、両方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

HP NNMi–HP UCMDB 統合については、HP UCMDB オンラインヘルプ (バージョン 10.0 以降) の「HP Network Node Manager (NNMi) 統合」(HP Network Node Manager (NNMi) Integration) セクションで詳しく説明されています。

HP NNMi-HP UCMDB 統合の使用法



NNMi は、HP Business Service Management (BSM) トポロジおよび HP UCMDB と同時に統合することはできません。この NNMi 管理サーバーで HP NNMi-HP BSM/UCMDB トポロジ統合を設定した場合は、その設定を無効にしてから、HP NNMi-HP UCMDB 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。

- [HP Business Service Management](#) および [HP Universal CMDB](#) ページ 15 の説明に従って、HP NNMi-HP BSM/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 HP UCMDB の統合を設定します。HP UCMDB 製品のこのマニュアルは、次の URL から入手することもできます。
<http://h20230.www2.hp.com/selfsolve/manuals>

HP NNMi-HP UCMDB 統合の有効化、使用法、無効化、およびトラブルシューティングについては、『[HP Universal CMDB-HP Network Node Manager \(NNMi\) 統合ガイド](#)』を参照してください。

HP NNMi と HP 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 Universal CMDB (UCMDB) 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 コンソールにログオンし、HP UCMDB にログオンすることなく HP UCMDB ビューを起動できます。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。HP NNMi と HP UCMDB のログオンパスワードが異なる場合があります。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 NNMi では通常の権限、HP UCMDB では管理者権限を有する場合があります。

NNMi から UCMDB 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。

UCMDB 初期化スト リング

以下のようにして、UCMDB 初期化ストリングを特定します。

- 1 UCMDB の JMX コンソールには以下の場所でアクセスできます。
`http://<UCMDB_hostname>:<UCMDB_JMX_port>/jmx-console/`
- 2 **service=LW-SSO Configuration** (Topaz の下) を選択します。
初期化ストリングは、**InitString** パラメーターの値です。
- 3 **InitString** パラメーターの値を変更した場合は、[**変更を適用**] をクリックします。

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 以下のファイルをテキストエディターで開きます。
 - `Windows: %NNM_PROPS%\nms-ui.properties`

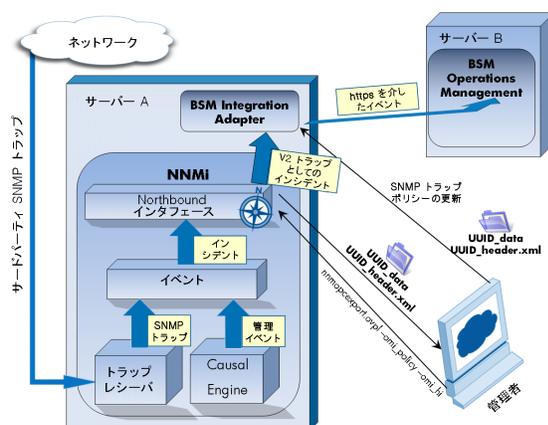
- **Linux** の場合 : \$NNM_PROPS/nms-ui.properties
- 2 スtring `initString` を検索します。
初期化Stringは、`initString` パラメーターの値です。引用符は含みません。
たとえば、`nms-ui.properties` ファイルに以下のテキストが含まれているとします。

```
initString=E091F3BA8AE47032B3B35F1D40F704B4
```


この場合、以下が初期化Stringです。

```
E091F3BA8AE47032B3B35F1D40F704B4
```
 - 3 `initString` パラメーターの値を変更した場合は、以下のコマンドを実行して変更をコミットします。
`nnmssso.ovpl -reload`
-

HP BSM Operations Management



HP Business Service Management (BSM) プラットフォームの Operations Management 機能には、管理オペレーティングシステム、ミドルウェア、アプリケーションイン

フラストラクチャー用に、包括的なイベント管理、プロアクティブなパフォーマンスモニタリング、自動化されたアラート、レポート、グラフが備えられています。HP NNMi—HP BSM Operations Management 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 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。

- [HP NNMi—HP BSM Operations Management 統合 ページ 39](#)
- [HP NNMi—HP BSM Operations Management 統合の有効化 ページ 41](#)
- [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 ページ 44](#)
- [HP NNMi—HP BSM Operations Management 統合の使用法 ページ 45](#)
- [HP NNMi—HP BSM Operations Management 統合の変更 ページ 48](#)
- [HP NNMi—HP BSM Operations Management 統合の無効化 ページ 50](#)
- [HP NNMi—HP BSM Operations Management 統合のトラブルシューティング ページ 50](#)
- [NNMi\[—HPOM Agent デスティネーション\] フォームリファレンス \(BSM Operations Management 統合\) ページ 53](#)

HP NNMi—HP BSM Operations Management 統合

HP NNMi—HP 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 NNMi 管理サーバーの BSM Connector に転送します。BSM Connector は、NNMi トラップをフィルターし、それを BSM Operations Management イベントブラウザーに転送します。

HP NNMi—HP 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。

HP NNMi—HP BSM Operations Management 統合では、BSM Operations Management イベントブラウザ内から NNMi コンソールにアクセスできます。



この章では、NNMi と BSM Operations Management イベントブラウザとの間の直接接続について説明します。

HP NNMi—HP BSM Operations Management 統合は、NNMi Northbound インタフェースの具体的な実装です。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。

HP NNMi—HP BSM Operations Management 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

HP NNMi—HP BSM Operations Management 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 イベントブラウザで統合できるため、BSM Operations Management 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 イベントブラウザに表示されます。
- BSM Operations Management イベントブラウザから 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。

- BSM (HP Operations Manager i ライセンス付き)



サポートされるバージョンは、NNMi システムとデバイス対応マトリックスにリストされています。

- NNMi 10.00 (Windows または Linux オペレーティングシステムのみ)

NNMi と BSM 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 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、異なっても構いません。

BSM Connector は、NNMi のインストール後に NNMi 管理サーバーコンピューターにインストールする必要があります。

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 イベントブラウザと通信するように 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 『BSM Connector インストールおよびアップグレードガイド』(BSM Connector Installation and Upgrade Guide)
- BSM 『BSM Connector ユーザーガイド』 (BSM Connector User Guide)
- BSM Connector ヘルプ
- BSM Operations Management 拡張性ガイド

HP NNMi—HP BSM Operations Management 統合の有効化

HP NNMi—HP BSM Operations Management 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。



NNMi を HP Business Service Management (BSM) トポロジデータベースと統合すると、HP NNMi—HP 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 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 ページ 46](#) を参照してください。

HP NNMi—HP BSM Operations Management 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] 状態が表示される必要があります。

- 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。

```
nmmopcexport.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的な 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。



これらの出力ファイルを編集したり名前を変更したりすると、**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](#) 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、[HP NNMi—HP BSM Operations Management 統合の使用法](#) ページ 45 を参照してください。

2 BSM Connector をインストールおよび設定します。

- a **NNMi** 管理サーバーで、『**BSM Connector** インストールおよびアップグレードガイド』(**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** で、『**BSM** アプリケーション管理ガイド』の説明に従って、**BSM** との **BSM Connector** 統合を設定します。



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** ユーザーガイド』(**BSM Connector User Guide**) を参照してください。

- c **BSM Connector** ユーザーインターフェースを使用して、この手順の **手順 1** 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** ヘルプ』(**BSM Connector Help**) の「**BSM Connector** の操作」(**Working with BSM Connector**) > 「ポリシー管理」(**Policy Management**) > 「ポリシーのインポート方法」(**How to Import Policies**) を参照してください。
- d **BSM Connector** ユーザーインター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** ヘルプ』(**BSM Connector Help**) の「**BSM Connector** の操作」(**Working with BSM Connector**) > 「ポリシー管理」(**Policy Management**) > 「ポリシーをアクティブ/非アクティブにする方法」(**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 **手順 4** (**BSM Connector** 用) と **手順 5** (**NNMi** 用) の両方でこのポート番号を使用します。



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 は **NNMi** 管理サーバーにインストールされるため、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。

- a NNMi 管理サーバーから、`nmtrapconfig.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 との間で 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、その出力から手順 b 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 NNMi 管理サーバーで、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。

- Windows NNMi 管理サーバー：

- a エージェントを設定します。

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

- b エージェントを再起動します。

```
ovc -restart opctrapi
```

- Linux NNMi 管理サーバー：

- a エージェントを設定します。

```
ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> ¥
-set SNMP_SESSION_MODE NO_TRAPD
```

- b エージェントを再起動します。

```
ovc -restart opctrapi
```

<custom_port> では、この手順の手順 3 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 Agent 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 NNMi 管理サーバー上の BSM Connector への接続に関する情報を入力します。トラップ転送先ポートは、この手順の手順 3 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 ページ 54 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 統合コンテンツ ページ 54 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 省略可能。BSM 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 は自動モニタリングコンポーネント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 <username> -password <password> -uploadOM -input <policy header file>

または

— <BSM_Root_Directory>%opr%\bin\ConfigExchange.bat -username <username> -password <password> -uploadOM -input <dir in which policy header file is located>

Linux の場合：

— <BSM_Root_Directory>/opr/bin/ConfigExchange -username <username> -password <password> -uploadOM -input <policy header file>

または

— <BSM_Root_Directory>/opr/bin/ConfigExchange -username <username> -password <password> -uploadOM -input <dir in which policy header file is located>

BSM Connector OM Agent 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。

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 HP BSM Operations Management 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 **OMBackSync.pl** スクリプトを正しい場所にコピーします。

Windows: %ovdatadir%\%conf%\nnm\backsync\OMBackSync.pl を %ovdatadir%\%conf%\backsync\OMBackSync.pl にコピーします。

Linux の場合： /var/opt/OV/conf/nnm/backsync/OMBackSync.pl を /var/opt/OV/conf/backsync/OMBackSync.pl にコピーします。

- 2 **OMBackSync.pl** スクリプトを変更します。以下の例を参考にして、スクリプトのパラメーターを変更します。

```
my $nnmi_server = 'localhost';
my $nnmi_port   = <http port used to access NNMi>;
my $nnmi_user   = '<administrator user name>';
```

```
my $nnmi_pass = '<administrator password>';
my $logfilepath = OV_DATA_DIR.'/log/OMBacksync-NNMi.log';
my $verbosity = 2
```

- 3 OMBBackSync.pl スクリプトを編集し、以下の行を検索します。
`__END__`
`__END__` から OMBBackSync.pl スクリプトの最後までテキストをすべて削除します。
 忘れずに設定内容を保存してください。
- 4 Windows のみ: %ovinstalldir% ディレクトリから、
`newconfig%HPNmsCommon%scripts%nnm-configure-perl.ovpl -source
 newconfig%HPNmsCommon%perl%a -target nonOV%perl%a` というコマンドを
 実行します。
- 5 コマンド `ovc -restart ombacksync` を実行し、ombacksync プロセスを再起動し
 ます。
- 6 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、HP BSM
 Operations Management 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。



NNMi 10.00を再インストールする場合は、BSM Connectorを再インストールし、44 ページの**手順 1**～45 ページの**手順 6**を繰り返す必要があります。



BSM Connector を NNMi 管理サーバーで再インストールする場合は、44 ページの**手順 1**～45 ページの**手順 6**を繰り返す必要があります。BSM Connector を再インストールすると、44 ページの**手順 1**～45 ページの**手順 3**でコピーおよび変更した OMBBackSync.pl スクリプトが上書きされるため、変更内容がすべて失われます。この問題を回避するには、BSM Connector を再インストールする前に OMBBackSync.pl スクリプトのバックアップコピーを作成します。

HP NNMi—HP BSM Operations Management 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 HP BSM Operations Management 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。HP NNMi—HP BSM Operations Management 統合では、BSM および BSM Operations Management イベントブラウザーと、NNMi 管理イベントおよび SNMP トラップとの間で、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 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。



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 イベントブラウザーに表示します。BSM Operations Management 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 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

HP Business Service Management (BSM) および **HP Universal CMDB Software (HP 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 HP UCMDB と統合すると、NNMi は、NNMi が管理するデバイスの BSM または HP UCMDB と CI 情報を共有します。この場合、HP NNMi—HP 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 HP 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 HP UCMDB との統合の詳細については、以下を参照してください。

- [HP Business Service Management および HP Universal CMDB ページ 15](#)
- [HP Universal CMDB ページ 35](#)

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 ページ 46](#) 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 ページ 46](#) 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** イベントブラウザに表示されます。
- これらのトラップには、[設定項目の ID ページ 46](#) 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** イベントブラウザが 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** イベントブラウザ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** イベントブラウザが管理対象デバイスから直接受信したトラップと関連させるようにポリシーを設定できます。
- **Syslog**
 - NNMi は、NNMi が生成した管理イベントと HP 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。
- **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** イベントブラウザに表示されません。
 - NNMi SNMP トラップポリシーファイルにより、**BSM Connector** は、**BSM Operations Management** イベントブラウザで解決済みの 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** イベントブラウザに転送しません。
- **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** イベントブラウザに転送しません。
- **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** イベントブラウザに表示されません。
 - **BSM Connector** は、NNMi 相関トラップを処理して、**BSM Operations Management** イベントブラウザで 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 ユーザーインター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 ヘルプ**』(**BSM Connector Help**)の「**BSM Connector とのデータの統合**」(**Integrating Data With BSM Connector**) > 「**SNMP トラップポリシー**」(**SNMP Trap Policies**) > 「**SNMP ポリシーユーザーインターフェース**」(**SNMP Policy User Interface**) > 「**SNMP ポリシーでのルールの設定**」(**Configuring Rules in SNMP Policies**) を参照してください。

詳細情報

HP NNMi—HP BSM Operations Management 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。
- HP NNMi—HP BSM Operations Management 統合の詳細については、『**BSM Operations Management 拡張性ガイド**』（HP BSM Operations Management Extensibility Guide）を参照してください。

HP NNMi—HP BSM Operations Management 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](#) ページ 48
- [設定パラメーターの変更](#) ページ 49

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。



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** 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\[HPOM Agent デスティネーション\] フォームリファレンス \(BSM Operations Management 統合\)](#) ページ 53 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。

HP NNMi—HP BSM Operations Management 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 ヘルプ』(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。

HP NNMi—HP 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 ページ 50
- 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 ページ 53

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



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 NNMi 管理サーバーで、エージェント設定を確認します。

- Windows NNMi 管理サーバー :
`%OVBIN%\ovconfget eaagt`
- Linux NNMi 管理サーバー :
`$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 Agent 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 手順 1 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[手順 3](#)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、[43 ページの 手順 4](#)を繰り返します。
- <custom_port> の値が 162 であるか、[NNMi-HPOM Agent 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 [42 ページの 手順 3](#) から [43 ページの 手順 5](#)を繰り返します。

3 NNMi 管理サーバーで、エージェントが実行されていることを確認します。

- Windows NNMi 管理サーバー :
`%OVBIN%\opcgagt -status`
- Linux NNMi 管理サーバー :
`$OVBIN/opcgagt -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 NNMi 管理サーバーで、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 [手順 1](#) 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。
- 5 NNMi 管理サーバーで、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 NNMi 管理サーバー :

```
%OVBIN%\%ovpolicy -list
```

- Linux NNMi 管理サーバー :

```
$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、[41 ページの 手順 1](#) で nnmopcxport.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 NNMi 管理サーバーで、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「Northbound インタフェース NNMi 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。



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 Agent デスティネーション] フォームリファレンス (BSM Operations Management 統合)

[NNMi-HPOM Agent 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。)



[NNMi-HPOM Agent 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 Agent 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 ページ 54
- BSM Operations Management 統合コンテンツ ページ 54
- BSM Connector 転送先のステータス情報 ページ 56

統合設定への変更を適用するには、[NNMi-HPOM Agent 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

54 ページの図 5 に、BSM Connector への接続設定用パラメーターをリストします。

表 5 BSM Connector の接続情報

フィールド	説明
ホスト	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • NNMi FQDN NNMi は、NNMi 管理サーバーの 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。 これがデフォルトの推奨設定です。 • ループバックを使用 このオプションは使用しないでください。 • その他 このオプションは使用しないでください。 <p>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。</p>
ポート	<p>BSM Connector が SNMP トラップを受信する UDP ポート。</p> <p>BSM Connector 固有のポート番号を入力します。この値は、42 ページの手順 3 で指定したポートです。</p> <p>ポートを決定するには、NNMi 管理サーバー上で <code>ovconfget eaagt</code> 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。</p> <p>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。</p>
コミュニティ文字列	<p>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。</p> <p>HP NNMi—HP BSM Operations Management 統合では、デフォルト値 public を使用します。</p>

BSM Operations Management 統合コンテンツ

55 ページの表 6 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リストします。

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	<p>インシデント転送の送信オプション。</p> <ul style="list-style-type: none"> • 管理 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。 • SNMP サードパーティトラップ 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。 • Syslog 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。 これがデフォルト設定です。 <p>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。</p>
ライフサイクル状態の変化	<p>インシデント変更通知の送信オプション。</p> <ul style="list-style-type: none"> • 解決済みに変化 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。 これがデフォルト設定です。 • 変化した状態 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、インシデントライフサイクル状態変化トラップを BSM Connector に送信します。 • 両方 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、この統合では、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、インシデントライフサイクル状態変化トラップを BSM Connector に送信します。 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。
関連処理	<p>インシデント関連処理の送信オプション。</p> <ul style="list-style-type: none"> • なし NNMi は、NNMi の因果関係分析によるインシデント関連処理結果を BSM Connector に通知しません。 これがデフォルト設定です。 • 単一 NNMi は、NNMi 因果関係分析で判明した親子インシデント関連関係ごとにトラップを 1 つ送信します。 • グループ 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関連処理ごとに、トラップを 1 つ送信します。 注: 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。

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
削除	<p>インシデント削除の送信オプション。</p> <ul style="list-style-type: none"> • 送信しない 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。これがデフォルト設定です。 • 送信 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	<p>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。</p> <p>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。</p>
インシデントフィルター	<p>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。</p> <p>以下のオプションの 1 つを選択します。</p> <ul style="list-style-type: none"> • なし NNMi は、すべてのイベントを BSM Connector に送信します。これがデフォルト設定です。 • 含む 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。 • 除外する 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。 <p>インシデントフィルターを指定します。</p> <ul style="list-style-type: none"> • 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。 • 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 に、BSM Connector に使用する読み取り専用のステータス情報をリストします。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	<p>BSM Connector の転送先ホスト名の解決先となる IP アドレス。</p> <p>この値は、この転送先に固有の値です。</p>

表7 BSM Connector 転送先のステータス情報 (続き)

フィールド	説明
アップタイム (秒)	<p>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。</p> <p>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。</p>
NNMi URL	<p>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。</p> <p>この値は、このノースバウンド転送先に固有です。</p>

HP Business Service Management 内の NNMi の視覚化

HP 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。

この章には、以下のトピックがあります。

- [MyBSM ポータル ページ 59](#)
- [NNMi と BSM または UCMDB 間のシングルサインオンの設定 ページ 61](#)
- [BSM への SSL 接続の設定 ページ 62](#)
- [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 ページ 66](#)
- [BSM からの NNMi の視覚化の有効化 ページ 68](#)

BSM Operations Management イベントブラウザ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、[HP NNMi—HP BSM Operations Management 統合の使用法 ページ 45](#) 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。



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 ページ 60](#) 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ー設定]>[ファウンデーション]>[他のアプリケーションとの統合]>[HP NNMi])。

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ーには、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ド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ド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 からの NNMi の視覚化の有効化** ページ 68 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 または UC MDB 間のシングルサインオンの設定** ページ 61 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 HP NNMi-HP BSM/UCMDB トポロジ統合の有効化 ページ 20 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)。



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。UCMDB 製品のこのマニュアルは、次の 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。
- ユーザー定義の MyBSM ページ内で、[**コンポーネントギャラリー**] を開きます。
 - 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、『How to Create Your MyBSM Workspace』の「HP BSM Using MyBSM Guide」を参照してください。

NNMi と BSM 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 MyBSM ポータルにログオンし、HP NNMi にログオンすることなく 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ります。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。

HP BSM から HP 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。

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。

- BSM の JMX コンソールには以下の場所でアクセスできます。
`http://<BSM_hostname>:<BSM_JMX_port>/jmx-console/`
- service=LW-SSO Configuration (Topaz の下)** を選択します。
初期化ストリングは、**InitString** パラメーターの値です。
- InitString** パラメーターの値を変更した場合は、[**変更を適用**] をクリックします。

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。

- 以下のファイルをテキストエディターで開きます。
 - Windows:** %NNM_PROPS%\nms-ui.properties
 - Linux の場合:** \$NNM_PROPS/nms-ui.properties

- 2 スtring `initString` を検索します。
初期化String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Stringです。

```
E091F3BA8AE47032B3B35F1D40F704B4
```
- 3 手順 2 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て、変更をコミットします。

```
nmssso.ovpl -reload
```

BSM への SSL 接続の設定

BSM への SSL 接続を設定するには、以下の手順を実行します。

- 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:


```
%NnmInstallDir%\nonOV\jdk\%nnm%\bin\keytool.exe -export -alias  
hostname.selfsigned -file C:%temp%\cert -keystore  
%NnmDataDir%\%shared%\nnm%\certificates\%nnm%.keystore -storepass  
nnmkeypass
```
- 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\%nnm%\bin\keytool.exe`」を使用してください。
- Linux の場合:


```
$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -export -alias  
hostname.selfsigned -file /tmp/cert -keystore $NnmDataDir/  
shared/nnm/certificates/nnm.keystore -storepass nnmkeypass
```
- 2 「Certificate stored in file <directory>:%cert」というメッセージが表示されることを確認します。
 - 3 手順 1 で作成した `cert` ファイルから BSM サーバーに証明書をコピーします。
 - 4 BSM サーバーでコマンドウィンドウを開きます。
 - 5

```
cd C:%HPBSM%\JRE64%\bin
```

 コマンドを使用してディレクトリを変更します。
 - 6

```
keytool.exe -import -keystore  
<directory>:%HPBSM%\odb%\conf%\security\%server.keystore -storepass  
hpass -trustcacerts -file <directory>%cert
```

 というコマンドを実行します。

「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 server.keystore を server.truststore に置き換えて、手順 6 で説明されているコマンドを実行します。 **keytool.exe -import -keystore <directory>:%HPBSM%odb%conf%security%server.truststore -storepass hppass -trustcacerts -file <directory>:%cert**

「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 の証明書を JRE に追加するには、以下のコマンドを実行します。**keytool.exe -import -file <directory>:%cert -keystore <directory>:%HPBSM%JRE%lib%security%cacerts -trustcacerts -storepass changeit.**

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

```
keytool.exe -import -file <directory>%cert -keystore  
<directory>%HPBSM%JRE64%lib%security%cacerts -trustcacerts  
-storepass changeit.
```

「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
```

- 10 BSM 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 サーバーで以下のコマンドを実行します。

```
keytool.exe -export -alias clientcert -file  
<directory>%truststore -keystore  
<directory>%HPBSM%odb%conf%security%server.truststore  
-storepass hppass
```

コマンドの実行が終了すると、BSM トラストストア証明書は
<directory>%truststore ファイルに保存されます。

- b BSM サーバーで以下のコマンドを実行します。

```
keytool.exe -export -alias hpcert -file  
<directory>%keystore -keystore  
<directory>%HPBSM%odb%conf%security%server.keystore  
-storepass hppass
```

コマンドの実行が終了すると、BSM キーストア証明書は
<directory>%keystore ファイルに保存されます。

- c truststore ファイルおよび keystore 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。これらのファイルは、残りのコマンドにおいて、NNMi 管理サーバーの<ディレクトリ>:%temp%keystore および<ディレクトリ>:%temp%truststore、または /tmp/keystore および /tmp/truststore にあると表示されます。
- 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:

```
keytool.exe -import -alias hpcert -keystore  
%NnmDataDir%shared%nnm%certificates%nnm.keystore  
-storepass nnmkeypass -file <directory>%temp%keystore
```

- Linux:


```
keytool -import -alias hpcert -keystore $NnmDataDir/
shared/nnm/certificates/nnm.keystore -storepass
nnmkeypass -file
/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:


```
keytool.exe -import -alias clientcert -keystore
%NnmDataDir%\shared\%nnm%\certificates\%nnm.truststore
-storepass ovpass -file <directory>:\%temp%\truststore
```
 - Linux:


```
keytool -import -alias clientcert -keystore $NnmDataDir/
shared/nnm/certificates/nnm.truststore -storepass ovpass
-file /tmp/truststore
```
- f 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) 署名証明書を使用していない場合)。BSM 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:


```
keytool.exe -import -alias bsm_ca_root_cert -keystore
%NnmDataDir%\shared\%nnm%\certificates\%nnm.truststore
-storepass ovpass -file <directory>:/temp/keystore
```
 - Linux:


```
keytool -import -alias bsmcert -keystore $NnmDataDir/
shared/nnm/certificates/nnm.truststore -storepass ovpass
-file /tmp/keystore
```
- g 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。この手順で、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 証明書は別々にインポートする必要があります。たとえば、ルート証明書および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:


```
keytool.exe -import -alias bsm_ca_root_cert -keystore
%NnmDataDir%\shared\%nnm%\certificates\%nnm.truststore
-storepass ovpass -file <directory>:/temp/keystore
```
 - keytool.exe -import -alias bsm_ca_intermediate_cert -keystore


```
%NnmDataDir%\shared\%nnm%\certificates\%nnm.truststore
-storepass ovpass -file <directory>:/temp/keystore
```
 - Linux:


```
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
```

- 11 省略可能 : NNMi 管理サーバーで、以下の一連のコマンドを実行します。
- a **ovstop**
 - b **ovstart**
- 12 省略可能 : NNMi 管理サーバーと BSM 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: **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 サーバーの場合 : **keytool.exe -list -keystore <directory>:%HPBSM%\odb%\conf%\security\%server.keystore -storepass hppass**
- 13 省略可能 : NNMi 管理サーバーと BSM 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: **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 サーバーの場合 : **keytool.exe -list -keystore <directory>:%HPBSM%\odb%\conf%\security\%server.truststore -storepass hppass -v**
- 14 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 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 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。 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。 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。

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 (続き)

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
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 からの NNMi の視覚化の有効化** ページ 68 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 または UCMDDB 間のシングルサインオンの設定** ページ 61 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 **HP NNMi-HP BSM/UCMDDB トポロジ統合の有効化** ページ 20 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 省略可能。BSM サーバーで、HPOprInf インフラストラクチャー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 拡張性ガイド』を参照してください。

BSM 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
- 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 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 ユーザーインターフェイスで [**インフラストラクチャー設定**] 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ー設定**])。
- 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 :

```
%NmDataDir%\conf\nnm\props\nms-local.properties
```

— Linux の場合 : \$NmDataDir/conf/nnm/props/nms-local.properties

SSL 以外の接続では、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 接続には、jboss.https.port の値を使用します。これはデフォルトでは 443 です。

- **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。

フィードバックをお待ちしております。

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

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

製品名およびバージョン: NNMi 10.00

ドキュメントタイトル: HP Network Node Manager i Software—HP Business Service Management 統合ガイド

フィードバック: