HP Network Node Manager i Software

Windows®、HP-UX、Linux、および Solaris のオペレーティングシステム用

ソフトウェアバージョン : 9.10

デプロイメント リファレンス

ドキュメント リリース日 : 2011 年 3 月
ソフトウェア リリース日 : 2011 年 3 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 ソフトウェアです。これらを所有、使用、または複製するには、HP からの正式な使用許諾が必要です。FAR 12.211 および 12.212 に準拠し、商用コンピュータソフトウェア、コンピュータソフトウェアドキュメント、および商用アイテムの技術データは、ベンダーの標準商用ライセンスの下、米国政府にライセンスされています。

著作権について

© Copyright 2008–2011 Hewlett-Packard Development Company, L.P.

商標に関する通知

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

HP 9000 コンピュータ上の HP-UX リリース 10.20 以降および HP-UX リリース 11.00 以降 (32 ビットおよび 64 ビット両方の環境) は、すべて Open Group UNIX 95 製品です。

Microsoft® and 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。

UNIX® は The Open Group の登録商標です。

Oracle テクノロジー — 権利制限について

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

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

謝辞

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

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

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。
- *HP Network Node Manager i Software インストール ガイド* - 一 製品メディアおよび NNMi 管理サーバー上でサポートされている各オペレーティング システムについて入手できます。
- *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 管理サーバーで入手できます。
- *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* - 一 製品メディアおよび NNMi 管理サーバーで入手できます。
- 『HP Network Node Manager iSPI Network Engineering Toolset 計画とインストール ガイド』- *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

このサイトでは、HP Passport への登録とサインインが必要です。HP Passport ID のご登録は、

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

または、HP Passport 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。詳細は HP 販売員にお尋ねください。

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のダウンロード
- サポート契約の管理
- HP サポートの問合せ先の検索
- 利用可能なサービス情報の確認
- ソフトウェアを利用している他のユーザーとの情報交換
- ソフトウェアトレーニング情報の検索および参加登録

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

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

目次

このガイドについて 25
ガイドの説明 25
このドキュメントで使用するパス表記 26
改訂履歴 27
NNMi の詳細 28

準備 31

ハードウェアとソフトウェアの要件 33
対応ハードウェアとソフトウェア 33
必要なパッチの確認 34
システム設定 (UNIX) 35
NNMi および NNM iSPI のインストール 35
NNMi と HP Performance Insight の共存 35
NNMi と HP Operations エージェントの共存 36

設定 37

設定の一般概念 39
タスク フロー モデル 39
ベストプラクティス : 既存の設定を保存 40
ベストプラクティス : 作成者属性を使用する 40
ユーザー インタフェース モデル 40
順序 40
ノード グループおよびインタフェース グループ 41
グループの重複 42
ノード グループのメンバーシップ 43
階層 / コンテインメント 43
デバイス フィルタ 43
追加フィルタ 44
追加ノード 44
ノード グループのステータス 44
インタフェース グループ 45
ノード / インタフェース / アドレス階層 45
すべてを停止して再度やり直す 46

NNMi 通信 47
通信の概念 48
通信の設定レベル 48
ネットワーク待ち時間とタイムアウト 48

SNMP アクセス制御 49
SNMP バージョンの優先 50
管理アドレスの優先 51
ポーリング プロトコル 51
通信設定および nnmsnmp*.ovpl コマンド 52
通信の計画作成 52
デフォルトの通信設定 52
通信設定領域 53
特定のノードの設定 54
再試行とタイムアウトの値 54
アクティブなプロトコル 54
複数のコミュニティ文字列または認証プロファイル 54
SNMPv1 と SNMPv2 のコミュニティ文字列 55
SNMPv3 の認証プロファイル 55
通信の設定 55
NNMi における SNMPv3 プライバシ プロトコルの使用準備 56
通信の評価 56
すべてのノードが SNMP 用に設定されましたか？ 57
デバイスについて SNMP アクセスは現在利用できますか？ 57
管理 IP アドレスは正しいですか？ 57
NNMi は正しい通信設定を使っていますか？ 57
State Poller 設定は通信設定と一致していますか？ 58
通信の調整 58

NNMi 検出 59
検出の概念 59
NNMi はデバイス プロファイルから属性を導き出す 60
検出の計画 61
基本的な検出方法を選択する 61
リストに基づいた検出 61
ルールベースの検出 61
自動検出ルール 62
自動検出ルールの順序 62
デバイスを検出から除外 62
Ping スィープ 63
SNMP トラップからの検出ヒント 63
自動検出ルールの検出シード 63
自動検出ルールのベスト プラクティス 64
例 64
ノード名の解決 64
サブネット接続ルール 65
検出シード 65
再検出の間隔 66
オブジェクトを検出しない 66

NNMi による仮想 IP アドレスの監視 67
検出の設定 68
自動検出ルールを設定する場合のヒント 68
シードを設定する場合のヒント 68
検出の評価 69
初期検出の進行状況をたどる 69
すべてのシードが検出されているか？ 69
すべてのノードには有効なデバイス プロファイルがあるか？ 70
すべてのノードが正しく検出されたか？ 70
自動検出ルール 70
IP アドレス範囲 71
システム オブジェクト ID の範囲 71
すべての接続と VLAN は正しいか？ 71
レイヤー 2 接続の評価 71
NNMi 検出と重複 MAC アドレス 72
デバイスを再検出する 72
検出の調整 72
検出ログ ファイル 73
無番号インタフェース 73
無番号インタフェース機能の有効化 73
無番号インタフェース機能の無効化 74

NNMi 状態ポーリング 77
状態ポーリングの概念 77
状態ポーリングの計画を作成 78
ポーリング チェックリスト 78
NNMi で何を監視できますか？ 79
監視されないノードへのインタフェース 80
監視の停止 81
グループの計画作成 81
インタフェース グループ 82
ノードグループ 82
ポーリング間隔の計画作成 83
どのデータを収集するかの決定 84
状態ポーリングの設定 84
インタフェース グループとノード グループの設定 84
インタフェースの監視の設定 85
ノードの監視の設定 85
デフォルト設定の確認 86
状態ポーリングの評価 86
ネットワーク監視の設定を確認します 86
インタフェースまたはノードは正しいグループのメンバーでしょうか？ 86
どの設定が適用されていますか？ 87
どのデータが収集されていますか？ 87

ステータス ポーリングのパフォーマンスの評価 87
State Poller は最新の状態に付いていっていますか？ 87
状態ポーリングの調整 89

NNMi インシデント 91
インシデントの概念 91
インシデント ライフサイクル 92
トラップおよびインシデント転送 93
比較 : サードパーティ SNMP トラップを別のアプリケーションに転送する 94
MIB 95
カスタムインシデント属性 96
解決済み管理イベント インシデントに追加される CIA 96
インシデント数の削減 97
インシデントの抑制、強化、およびダンプニング 97
ライフサイクル移行アクション 98
インシデントの計画 99
NNMi が処理するデバイス トラップ？ 99
NNMi で表示するインシデント？ 99
インシデントに対する NNMi の対応方法？ 99
NNMi による NNM 管理ステーションからのトラップ受信の可否？ 100
NNMi による別のイベント レシーバへのトラップ転送の可否？ 100
インシデントの設定 100
インシデントの抑制、強化、およびダンプニングの設定 100
ライフサイクル移行アクションの設定 101
インシデントの評価 101
インシデントの調整 102
未定義トラップのインシデントの有効化および設定 102

NNMi コンソール 105
ノード グループの実際的な使用例 105
ノード グループの作成 106
ステップ 1: My Network ノード グループを作成する 106
ステップ 2: USA ノード グループを作成する 106
ステップ 3: フィルタを使用して Colorado ノード グループを作成する 107
ステップ 4: ノード グループ メンバーを表示してノード グループのフィルタ結果を確認する 107
ステップ 5: My Network ノード グループのノード グループ階層を設定する 108
ステップ 6: USA ノード グループのノード グループ階層を作成する 108
ノード グループ マップの設定 108
ステップ 1: ノード グループ マップを作成する 108
ステップ 2: ノード グループ マップを表示する 109
ステップ 3: ノード グループのステータスを設定する 109
ステップ 4: ノード グループ マップの順序の設定 109
ステップ 5: ノード グループ マップに背景イメージを追加する 110
ネットワーク概要マップに表示されるノードの最大数の削減 110

ノード グループ マップの表示ノード数の削減 111

詳細設定 113

NNMi ライセンスの取得 115

恒久ライセンス キーのインストール準備 115
ライセンスの種類および管理対象ノードの数の確認 115
恒久ライセンス キーの取得およびインストール 116
Autopass および HP 注文番号の使用 (ファイアウォール使用時は不可) 116
コマンド行で、シードを追加する 116
追加のライセンスキーを取得する 116

NNMi での証明書の使用 119

すべてをまとめる 120
認証機関証明書を生成する 121
自己署名証明書を使用するようにアプリケーション フェイルオーバーを設定する 124
認証機関を使用するようにアプリケーション フェイルオーバーを設定する 126
自己署名証明書または CA 証明書を使用するように高可用性を設定する 128
自己署名証明書を使用するように高可用性を設定する 128
新規証明書を使用するように高可用性を設定する 128
自己署名証明書を使用するようにグローバル ネットワーク管理機能を設定する 129
認証機関を使用するようにグローバル ネットワーク管理機能を設定する 130
自己署名証明書を使用するようにアプリケーション フェイルオーバーが有効なグローバル ネットワーク管理を設定する 131
ディレクトリ サービスへの SSL 接続を設定する 132
HP BSM バージョン 9.xx への SSL 接続の設定 133

NNMi とシングル サインオンの使用 139

NNMi への SSO アクセス 140
1 つのドメインに対する SSO の有効化 141
異なるドメインに配置されている NNMi 管理サーバーに対する SSO の有効化 141
NNMi と NNM iSPI の SSO アクセス 142
NNMi と HP BSM または HP BAC 間のシングル サインオンの設定 143
NNMi と HP UCMDB 間のシングル サインオンの設定 144
NNMi と HP NA 間のシングル サインオンの設定 145
SSO の無効化 148
SSO セキュリティに関する注意 148

NNMi で使用する Telnet および SSH プロトコルを設定する 151

Telnet または SSH メニュー項目の無効化 151
Windows 上のブラウザへの Telnet または SSH クライアントの設定 152
Windows オペレーティング システム提供の Telnet クライアント 153
サードパーティ Telnet クライアント (標準 Windows) 155
サードパーティ Telnet クライアント (Windows 上のウィンドウ) 156
サードパーティ SSH クライアント (標準 Windows および Windows 上のウィンドウ) 157

Linux で Telnet または SSH を使用する Firefox の設定 158
Linux 上の Telnet 158
Linux 上のセキュア シェル 159
Windows レジストリを変更するファイル例 160
nnmtelnet.reg の例 160
nnmputtytelnet.reg の例 160
nnmtelnet32on64.reg の例 161
nnmssh.reg の例 161

NNMi と LDAP によるディレクトリ サービスの統合 163
NNMi ユーザーのアクセス情報と設定オプション 163
オプション 1: NNMi データベースにすべての NNMi ユーザー情報を保存 164
オプション 2: 一部の NNMi ユーザー情報を NNMi データベースに、一部の NNMi ユーザー情報をディレクトリ サービスに保存 165
オプション 3: すべての NNMi ユーザー情報をディレクトリ サービスに保存 166
ディレクトリ サービスにアクセスする NNMi の設定 167
ディレクトリ サービスのアクセス設定を変更し、NNMi のセキュリティ モデルをサポートする 174
ディレクトリ サービスのクエリ 176
ディレクトリ サービス アクセス 176
ディレクトリ サービスの情報 176
ディレクトリ サービス管理者が所有する情報 180
ユーザー識別 181
ディレクトリ サービスからの NNMi ユーザー アクセスの設定 (詳細な方法) 182
ユーザー グループの識別 183
ディレクトリ サービスからのユーザー グループ取得の設定 (詳細な方法) 184
NNMi ユーザー グループを保存するディレクトリ サービスの設定 186
ディレクトリ サービス統合のトラブルシューティング 187
ldap.properties 設定ファイル リファレンス 188
例 192

NNMi セキュリティおよびマルチテナント 193
オブジェクトのアクセス制限による影響 194
NNMi セキュリティ モデル 195
セキュリティ グループ 196
セキュリティ グループ構造の例 197
NNMi テナント モデル 200
テナント 200
テナント構造の例 201
NNMi のセキュリティおよびマルチテナント設定 203
設定ツール 204
テナントの設定 205
セキュリティ グループの設定 207
設定の確認 208
NNMi のセキュリティおよびマルチテナント設定のエクスポート 210

NNMi セキュリティ、マルチテナント、およびグローバル ネットワーク管理 210
初期 GNM 設定 211
GNM のメンテナンス 213
NPS レポートへの選択インタフェースの追加 213

グローバル ネットワーク管理 215

グローバル ネットワーク管理の利点 215
グローバル ネットワーク管理が自分のネットワークの管理に適しているかどうかを判断するには？ 216
マルチサイト ネットワークを継続的に監視する必要がありますか？ 216
重要デバイスを表示できるか？ 216
ライセンスの考慮事項 216
実践的なグローバル ネットワーク管理の例 217
要件のレビュー 218
リージョナル マネージャとグローバル マネージャの接続 219
初期準備 220
ポート可用性 : ファイアウォールの設定 220
自己署名証明書の設定 220
グローバル ネットワーク管理でアプリケーション フェイルオーバーの設定を行う 220
NNMi 管理サーバー規模の考慮事項 221
システム クロックの同期化 221
グローバル ネットワーク管理で自己署名証明書を使用する場合のアプリケーション フェイルオーバー機能の使用法 221
グローバル ネットワーク管理における自己署名証明書の使用法 221
グローバル ネットワーク管理における認証機関の使用法 221
監視する重要な機器の一覧作成 222
グローバル マネージャとリージョナル マネージャの管理ドメインの検討 222
NNMi ヘルプ トピックの確認 223
SSO およびアクション メニュー 223
グローバル ネットワーク管理用にシングル サインオンを設定する 223
リージョナル マネージャでの転送フィルタの設定 225
転送されるノードを制限する転送フィルタの設定 225
グローバル マネージャとリージョナル マネージャの接続 232
global1 から regional1 と regional2 への 接続ステータスの判定 236
global1 インベントリの確認 237
global1 と regional1 との通信の切断 239
追加情報 241
検出とデータの同期化 241
デバイスのステータス ポーリングまたは設定ポーリング 244
グローバル マネージャを使ったデバイス ステータスの判定と NNMi インシデント生成 245
グローバル ネットワーク管理でアプリケーション フェイルオーバーの設定を行う 246
グローバル マネージャでのアプリケーション フェイルオーバーの設定 246
グローバル ネットワーク管理のトラブルシューティングのヒント 248
NNMi ヘルプのトラブルシューティング情報 248
クロック同期 248

グローバル ネットワーク管理システム情報 248
グローバル マネージャからのリージョナル マネージャ検出の同期化 249
破損した global1 上のデータベースの修復 249
NNMi 9.0x から NNMi 9.10 へのアップグレード 249
グローバルネットワーク管理によってサポートされている NNMi のバージョン 249
グローバルネットワーク管理のアップグレード手順. 249
グローバル ネットワーク管理と NNM iSPI または第三者の統合 250

IPv6 用 NNMi Advanced の設定 251
機能説明 251
必要条件 253
ライセンス. 253
サポートされる設定 254
管理サーバー 254
IPv6 をサポートする SNMP MIB. 255
NNMi のインストール 255
IPv6 機能のアクティブ化 255
IPv6 機能の非アクティブ化 257
非アクティブ化後の IPv6 監視 258
非アクティブ化後の IPv6 インベントリ 258
IPv6 インベントリ クリーンアップ時の既知の問題点 259

Solaris ゾーン環境での NNMi の実行. 261
Solaris ゾーンでの NNMi のインストール. 261
Solaris ゾーンでのトラップ転送. 261
Solaris ゾーン環境での NNMi アプリケーションフェイルオーバーの実行 262
Solaris ゾーン環境の HA での NNMi の実行. 262

復元 265

アプリケーション フェイルオーバー構成の NNMi の設定 267
アプリケーション フェイルオーバーの概要. 268
アプリケーション フェイルオーバーの基本セットアップ 268
アプリケーション フェイルオーバー構成の NNMi の設定 270
アプリケーション フェイルオーバー機能の使用 275
組み込みデータベースを使用したアプリケーション フェイルオーバーの動作 275
Oracle データベースを使用したアプリケーション フェイルオーバーの動作. 276
アプリケーション フェイルオーバーの例 277
その他の ovstart および ovstop オプション 277
アプリケーション フェイルオーバーのインシデント 278
フェイルオーバー後、元の設定に戻る 278
NNM iSPI およびアプリケーション フェイルオーバー. 279
NNM iSPI のインストールに関する情報 279
統合アプリケーション. 280

アプリケーション フェイルオーバーの無効化 281
管理タスクおよびアプリケーション フェイルオーバー 283
アプリケーション フェイルオーバーおよび NNMi 9.10 へのアップグレード 283
アプリケーション フェイルオーバーおよび NNMi パッチ 286
アプリケーションフェイルオーバー用にパッチを適用する (アクティブとスタンバイの両方をシャットダウン) 286
アプリケーションフェイルオーバー用にパッチを適用する (1 つのアクティブ NNMi 管理サーバーを保持) 288
アプリケーション フェイルオーバーおよび NNMi 管理サーバーの再起動 290
アプリケーション フェイルオーバーおよび以前のデータベース バックアップから復旧 (組み込みデータベースのみ) 290
ネットワーク レイテンシ / 帯域に関する考慮 292
アプリケーション フェイルオーバーと NNMi 組み込みデータベース 292
アプリケーション フェイルオーバー環境でのネットワーク トラフィック 293
アプリケーション フェイルオーバーのトラフィック テスト 294

高可用性クラスタに NNMi を設定する 297
HA の概念 298
HA 用語集 299
NNMi HA クラスタのシナリオ 300
マンページ 303
HA 用 NNMi を設定するための前提条件の検証 303
HA の設定 305
HA 用の NNMi 証明書の設定 305
HA 用の NNMi の設定 305
NNMiHA 設定情報 306
プライマリ クラスタ ノードでの NNMi の設定 308
セカンダリ クラスタ ノードでの NNMi の設定 310
HA 用の NNM iSPI の設定 311
NNM iSPI Performance for Metrics、NNM iSPI Performance for QA、および NNM iSPI Performance for Traffic 311
NNM iSPI for MPLS、NNM iSPI for IP Multicast、および NNM iSPI for IP Telephony 312
HA 下で実行中の NNM iSPI Network Engineering Toolset Software と NNMi 312
Oracle 環境での HA 用の NNMi の設定 312
Oracle での NNMi の依存関係 313
Oracle 環境での HA 用の NNMi の設定 313
共有 NNMi データ 314
NNMi の共有ディスク内のデータ 314
設定ファイルの複製 315
共有ディスクの手動準備 315
SAN または物理的に接続されたディスクの設定 315
ov.conf ファイルへの HA 変数の設定 316
NNMi HA リソースグループへの共有ディスクの移動 316
Windows Server での共有ディスク設定についての注記 317
HA クラスタ内の NNMi のライセンス契約 317

HA 設定のメンテナンス 318
メンテナンス モード 318
HA リソース グループをメンテナンス モードにする 318
HA リソース グループのメンテナンス モードを解除する 318
HA クラスタ内の NNMi のメンテナンス 319
NNMi の起動と停止 319
クラスタ環境で NNMi のホスト名や IP アドレスを変更する 319
フェイルオーバーを行わせないように NNMi を停止する 321
メンテナンス後に NNMi を再起動する 322
NNMi HA クラスタ内のアドオン NNM iSPI のメンテナンス 322
HA クラスタ内の NNMi の設定を解除する 322
HA クラスタ内の NNMi の設定を解除する 322
HA の外部の既存データベースを使用した NNMi の実行 325
HA 下の NNMi のパッチ 326
HA 下の NNMi を NNMi 9.0x から NNMi 9.10 にアップグレードする 327
Windows、Linux、または Solaris オペレーティングシステムでの組み込みデータベースを使用した NNMi のアップグレード 327
HP-UX オペレーティングシステムでの組み込みデータベースを使用した NNMi のアップグレード . . 329
サポートされるすべてのオペレーティングシステムでの Oracle を使用した NNMi のアップグレード . 330
HA 設定のトラブルシューティング 331
一般的な設定の誤り 331
HA リソース テスト 332
一般的な HA のトラブルシューティング 333
エラー : 引数の数が正しくない 333
リソースをホストするサブシステムプロセスが予期せず停止する (Windows Server 2008 R2) 333
製品の起動タイムアウト (Solaris) 334
アクティブなクラスタ ノードのログ ファイルが更新されない 334
NNMi HA リソース グループを特定のクラスタ ノードで起動できない 334
NNMi 固有の HA のトラブルシューティング 335
すべてのクラスタ ノードを設定解除した後の HA 用 NNMi の再有効化 336
NNMi を HA 下で正常に起動できない 336
NNMi データへの変更がフェイルオーバーの後に表示されない 337
HA の設定後、nmsdbmgr を起動できない 337
HA の設定後、pmd を起動できない 338
NNMi が 1 つの HA クラスタ ノードでのみ正常に実行される (Windows) 338
ディスク フェイルオーバーが行われない 338
共有ディスクにアクセスできない (Windows) 339
共有ディスクに最新データが含まれない 339
フェイルオーバー後にセカンダリ ノードが共有ディスク ファイルを見つけられない 339
NNM iSPI 固有の HA のトラブルシューティング 340
HA 設定リファレンス 341
NNMi HA 設定ファイル 341
NNMi に付属している HA 設定スクリプト 341
NNMi HA 設定のログ ファイル 343

NNMi のメンテナンス 345

NNMi のバックアップおよびリストア ツール 347
バックアップ コマンドとリストア コマンド 348
NNMi データのバックアップ 348
バックアップ タイプ 348
バックアップ領域 349
NNMi データのリストア 352
同じシステムでのリストア 352
異なるシステムでのリストア 353
バックアップとリストアの方針 353
すべてのデータを定期的にバックアップする 353
設定変更前のデータのバックアップ 354
NNMi またはオペレーティング システムのアップグレード前のバックアップ 354
ファイル システムのファイルのみのリストア 354
組み込みデータベースのみをバックアップおよびリストアする 355

NNMi の保守 357
カスタム ポーラー収集エクスポートの管理 358
カスタム ポーラー収集のエクスポート ディレクトリの変更 358
カスタム ポーラー収集のエクスポートに使用する最大ディスク容量の変更 358
カスタム ポーラー メトリックスの累積周期の変更 359
インシデント アクションの管理 359
同時アクション数の設定 359
Jython アクションのスレッド数の設定 360
アクション サーバー名のパラメータの設定 360
アクション サーバーのキュー サイズを変更する 361
trapFilter.conf ファイルによるインシデントのブロック 362
NNMi コンソールとの HTTPS 専用通信を設定する 363
NNMi 正規化プロパティの変更 363
初期検出後の正規化プロパティの変更 364
同時 SNMP 要求の変更 365
NNMi 自己監視 365
特定ノードの検出プロトコルの使用を抑える 366
検出プロトコル収集の使用の抑制 367
NAT 環境における管理アドレスの ICMP ポーリングの管理 367
NAT 環境における管理アドレスの ICMP ポーリングの有効化 368
NNMi に対する変更点 368
大規模スイッチの VLAN インデックス付けの使用を抑制する 369
VLAN インデックス付けの使用を抑制する 370
NAT 環境における管理アドレスの ICMP ポーリングの概要 371
NAT 環境の管理アドレスの ICMP ポーリング 371

NNMi ロギング 373
NNMi ログ ファイル 373
ログ ファイルのプロパティ 374
ロギング ファイルのプロパティの変更 374
ファイル管理 375

NNMi 管理サーバーの変更 377
NNMi 設定移動の準備のベストプラクティス 378
NNMi 設定および組み込みデータベースの移動 378
NNMi 設定の移動 379
NNMi パブリック キー証明書のリストア 379
スタンドアロン NNMi 管理サーバーの IP アドレスを変更する 382
ライセンスの考慮事項 382
NNMi 管理サーバーのホスト名またはドメイン名の変更 383
Oracle データベース インスタンス接続情報の変更 386
NNMi が Oracle データベース インスタンスへの接続に使用するパスワードを変更する 387

Xen 仮想化環境での NNMi の実行 389
Xen をインストールした後の NNMi 管理サーバーの動作に関する問題 389

NNMi 9.0x からのアップグレード 391

NNMi 管理サーバーを適切にアップグレードする 393
既存の NNMi 管理サーバー を NNMi 9.10 にアップグレード 393

別の NNMi 管理サーバーにアップグレードする 395
別の NNMi 管理サーバーへのアップグレード 395

Windows 2003 から Windows 2008 への NNMi の移行 397
Windows 2003 から Windows 2008 への NNMi の変更 397

NNMi Oracle データの移行 401
NNMi Oracle データの以降 401

追加アップグレード情報 403
設定面の相違点 403
アプリケーション フェイルオーバー 404
MIB 405
機能面の相違点 405

NNMi との統合 407

CiscoWorks LAN Management Solution 409
HP NNMi-CiscoWorks LMS 統合 409
値 409
統合製品 410

ドキュメント 410
HP NNMi-CiscoWorks LMS 統合の有効化 410
HP NNMi-CiscoWorks LMS 統合の使用法 411
HP NNMi-CiscoWorks LMS 統合設定の変更 412
HP NNMi-CiscoWorks LMS 統合の無効化 412
HP NNMi-CiscoWorks LMS 統合のトラブルシューティング 412
CiscoWorks LMS アクションが機能しない 412
トラップの MIB キャッシュ メッセージで OID を検出できない 412
[HP NNMi-CiscoWorks LMS の統合設定] フォームのリファレンス 413
NNMi 管理サーバー接続 413
CiscoWorks LMS サーバー接続 414

Clarus Systems ClarusIPC Plus+ 415
HP NNMi-Clarus Systems ClarusIPC Plus+ 統合 415
HP NNMi-Clarus Systems ClarusIPC Plus+ 統合について 416
値 416
統合製品 416
ドキュメント 416
HP NNMi-Clarus Systems ClarusIPC Plus+ 統合の有効化 416
HP NNMi-Clarus Systems ClarusIPC Plus+ 統合の使用法 417
HP NNMi-Clarus Systems ClarusIPC Plus+ 統合の無効化 417
HP NNMi-Clarus Systems ClarusIPC Plus+ 統合のトラブルシューティング 417
HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合 417
HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合について 418
値 418
統合製品 418
ドキュメント 418
HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合の有効化 419
HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合の使用法 419
HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合の無効化 419
HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合のトラブルシューティング . 420

HP Asset Manager 421
HP NNMi-HP Asset Manager 統合 421
値 421
統合製品 422
ドキュメント 422
HP NNMi-HP Asset Manager 統合の使用法 422

HP Business Service Management トポロジ 423
HP NNMi-HP BSM トポロジ統合 424
値 424
統合製品 424
ドキュメント 424

HP NNMi-HP BSM トポロジ統合の有効化 425
HP NNMi-HP BSM トポロジ統合の使用法 426
HP NNMi-HP BSM トポロジ統合の設定の変更 427
HP NNMi-HP BSM トポロジ統合の無効化 427
HP NNMi-HP BSM トポロジ統合のトラブルシューティング 427
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 427
RTSM の管理対象ノードで CI が重複する 428
アプリケーション フェイルオーバーと HP NNMi-HP BSM トポロジ統合 428
HP NNMi-HP BSM トポロジ統合設定フォームのリファレンス 429
NNMi 管理サーバー接続 429
BSM ゲートウェイ サーバー接続 430
BSM トポロジ フィルタ 430

HP Universal CMDB 433
HP NNMi-HP UCMDB 統合 433
値 434
統合製品 434
ドキュメント 434
HP NNMi-HP UCMDB 統合の使用法 434

HP Business Availability Center My BSM 435
HP NNMi-HP BAC My BSM 統合 435
値 436
統合製品 436
ドキュメント 436
My BSM のデフォルト NNMi モジュール 436
デモ ポートレットの設定 438
カスタム NNMi ポートレットの作成 439
ポートレット URL の特定 439
ポートレットの定義 HTML リファレンス 440
HP NNMi-HP BAC My BSM 統合のシングル サインオンの設定 442
HP NNMi-HP BAC My BSM 統合のトラブルシューティング 442
NNMi ポートレットがサインイン ページとして表示される 442
NNMi ポートレットが正しくロードしない 443
NNM iSPI for Performance ポートレットが正しくロードしない 443
NNM iSPI for Performance ポートレットに AsynchWait_Requests エラーが表示される 443
シングル サインオンが正しく機能しない 443
ポートレットの定義を保存すると、My BSM で HTML 検証エラーが発生する 443
HP NNMi-HP BAC My BSM 設定フォームのリファレンス 444

HP Network Automation 447
HP NNMi-HP NA 統合 447
値 448
統合製品 449
ドキュメント 449

HP NNMi-HP NA 統合の有効化 449
NNMi 9.0x からアップグレードされた統合設定 450
新規統合設定 451
HP NNMi-HP NA 統合の使用法 453
NNMi と NA の間のトポロジ同期 453
定期的同期の考慮事項 454
HP Blade System Virtual Connect デバイスのサポート 454
統合が提供する NNMi 機能. 455
NNMi コンソールからの NA ビューの起動. 455
NA Diagnostics コマンド スクリプトをインシデント アクションとして設定 456
NA にアクセスするインシデント アクションの結果の表示 457
不整合な状態のレイヤー 2 接続の特定. 457
統合により提供される NA 機能. 458
デバイス設定変更通知の送信 458
正確なデバイス情報の維持. 458
デバイス設定中のネットワーク管理の無効化 459
デバイス コミュニティ文字列の変更の伝播. 460
NA イベント ルール 460
HP NNMi-HP NA 統合の変更 461
HP NNMi-HP NA 統合の無効化 461
HP NNMi-HP NA 統合のトラブルシューティング 462
統合をテストする. 462
NA デバイスが NNMi トポロジから欠落している 464
アプリケーション フェイルオーバーと HP NNMi-HP NA 統合 464
HP NNMi-HP NA 統合設定フォームのリファレンス 464
NNMi 管理サーバー接続. 465
NA サーバー接続 465
統合動作. 466
NA の NNMi 統合設定リファレンス 467
統合通信. 467
その他の統合動作. 468

HP ProCurve Manager Plus 469
HP NNMi-HP ProCurve Manager Plus 統合 469
値 470
統合製品. 470
ドキュメント 470
HP NNMi-HP ProCurve Manager Plus 統合の使用法 471

HP RAMS MPLS WAN 473
HP NNMi-HP RAMS MPLS WAN 統合 473
値 473
統合製品. 474
ドキュメント 474
HP NNMi-HP RAMS MPLS WAN 統合の使用法 474

HP SiteScope 475
HP NNMi-HP SiteScope イベント統合 475
HP NNMi-HP SiteScope イベント統合について 476
値. 476
統合製品 476
サポートされる SiteScope モニタ 476
ドキュメント. 476
HP NNMi-HP SiteScope イベント統合の有効化 477
HP NNMi-HP SiteScope イベント統合の使用法 477
HP NNMi-HP SiteScope イベント統合の変更 478
HP NNMi-HP SiteScope イベント統合の無効化 478
HP NNMi-HP SiteScope イベント統合のトラブルシューティング 478
NNMi インシデントビューに SiteScopeAlertEvent インシデントが表示されない 478
SiteScope が SiteScop インシデントの URL から正常に開かない 479
HP NNMi-HP SiteScope システム メトリックス統合. 479
HP NNMi-HP SiteScope システムメトリックス統合について 479
値. 480
統合製品 480
サポートされる SiteScope モニタ 481
ドキュメント. 481
HP NNMi-HP SiteScope システム メトリックス統合の有効化 481
HP NNMi-HP SiteScope システム メトリックス統合の使用法 484
HP NNMi-HP SiteScope システム メトリックス統合の変更. 487
NNMi から NPS への接続を変更する 487
SiteScope から NNMi への接続を変更する 487
HP NNMi-HP SiteScope システム メトリックス統合の無効化 487
NNMi から NPS への接続を無効にする 488
SiteScope から NNMi への接続を無効にする 488
HP NNMi-HP SiteScope システム メトリックス統合のトラブルシューティング. 488
統合データ フローを確認する 489
統合設定の NNMi 側を確認する 490
ファイアウォールの背後の NAT 構成環境にノードのレポートデータが存在しない 491
HP NNMi-HP SiteScope システム メトリックス統合設定フォームのリファレンス. 492

HP Systems Insight Manager 493
HP NNMi-HP SIM 統合. 494
値 494
統合製品. 494
ドキュメント 494
HP NNMi-HP SIM 統合の有効化 495
HP NNMi-HP SIM 統合の使用法 496
HP NNMi-HP SIM 統合設定の変更. 496
HP NNMi-HP SIM 統合の無効化 496
HP NNMi-HP SIM 統合のトラブルシューティング 497

SIM アクションが機能しない 497
トラップの MIB キャッシュ メッセージで OID を検出できない 497
[HP NNMi-HP SIM 統合設定] フォームのリファレンス 498
NNMi 管理サーバー接続 498
SIM サーバー接続 499

nGenius Performance Manager 501
HP NNMi-nGenius Performance Manager 統合 502
値 502
統合製品 503
ドキュメント 503
HP NNMi-nGenius Performance Manager 統合の有効化 503
HP NNMi-nGenius Performance Manager 統合の使用法 504
HP NNMi-nGenius Performance Manager 統合の無効化 504
HP NNMi-nGenius Performance Manager 統合のトラブルシューティング 504

NNMi ノースバウンド インタフェース 505
NNMi ノースバウンド インタフェース 506
値 506
サポートされるバージョン 506
用語 506
ドキュメント 507
NNMi ノースバウンド インタフェースの有効化 507
NNMi ノースバウンド インタフェースの使用法 508
インシデント転送 508
インシデント ライフサイクル状態変化通知 509
インシデント相関処理通知 509
インシデント削除通知 510
イベント転送フィルタ 510
NNMi ノースバウンド インタフェースの変更 511
NNMi ノースバウンド インタフェースの無効化 511
NNMi ノースバウンド インタフェースのトラブルシューティング 512
アプリケーション フェールオーバーと NNMi ノースバウンド インタフェース 513
ローカル Northbound アプリケーション 513
リモート Northbound アプリケーション 514
[NNMi Northbound Interface デスティネーション] フォームのリファレンス 515
Northbound アプリケーションの接続パラメータ 515
NNMi Northbound インタフェース統合の内容 516
NNMi Northbound インタフェース転送先のステータス情報 518

HP BSM Operations Management 521
HP NNMi-HP BSM Operations Management 統合 521
値 522
統合製品 522
ドキュメント 523

HP NNMi-HP BSM Operations Management 統合の有効化 523
HP NNMi-HP BSM Operations Management 統合の使用 526
設定項目の ID 526
ヘルス インジケータ 527
デフォルトのポリシー条件 527
ポリシー条件のカスタマイズ 528
詳細情報 528
HP NNMi-HP BSM Operations Management 統合の変更 528
新規 NNMi トラップの SNMP トラップ ポリシー条件の更新 529
設定パラメータの変更 529
HP NNMi-HP BSM Operations Management 統合の無効化 530
HP NNMi-HP BSM Operations Management 統合のトラブルシューティング 530
BSM Operations Management イベント ブラウザに転送されたインシデントが表示されない 530
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 533
[HP 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) 534
BSM Integration Adapter の接続 534
BSM Operations Management 統合コンテンツ 535
BSM Integration Adapter 転送先のステータス情報 537

HP Operations Manager 539
HP NNMi-HPOM 統合 (エージェント実装) 539
HP NNMi-HPOM 統合について (エージェント実装) 540
値 540
統合製品 541
ドキュメント 541
HP NNMi-HPOM 統合の有効化 (エージェント実装) 541
HP NNMi-HPOM 統合の使用法 (エージェント実装) 546
設定項目の ID 546
ヘルス インジケータ 546
デフォルトのポリシー条件 547
ポリシー条件のカスタマイズ 548
詳細情報 548
HP NNMi-HPOM 統合設定の変更 (エージェント実装) 548
新規 NNMi トラップの SNMP トラップ ポリシー条件の更新 548
設定パラメータの変更 549
HP NNMi-HPOM 統合の無効化 (エージェント実装) 549
HP NNMi-HPOM 統合のトラブルシューティング (エージェント実装) 550
HPOM アクティブ メッセージ ブラウザが転送されたインシデントを受信しない 550
HPOM アクティブ メッセージ ブラウザが転送された一部のインシデントを受信しない 552

[HP NNMi-HPOM Agent デスティネーション] フォーム リファレンス (エージェント実装) 553
HP Operations エージェント接続 553
HPOM 統合コンテンツ 554
HP Operations エージェント転送先ステータス情報 556
HP NNMi-HPOM 統合 (Web サービス実装) 557
HP NNMi-HPOM 統合について (Web サービス実装) 557
値 558
統合製品 559
ドキュメント 559
HP NNMi-HPOM 統合の有効化 (Web サービス実装) 559
Windows 用 HPOM 559
UNIX 用 HPOM または Linux 用 HPOM 561
HP NNMi-HPOM 統合の使用法 (Web サービス実装) 563
使用例 563
正常な状況 : 不明な MSI 条件 564
詳細情報 564
HP NNMi-HPOM 統合設定の変更 (Web サービス実装) 564
HP NNMi-HPOM 統合の無効化 (Web サービス実装) 565
すべての HPOM 管理サーバーについて 565
1 つの HPOM 管理サーバーについて 565
HP NNMi-HPOM 統合のトラブルシューティング (Web サービス実装) 565
HPOM は転送されたインシデントを受信しない 565
転送されたインシデントの中に HPOM が受信しないものがある 568
NNMi インシデント情報が HPOM メッセージ ブラウザでは入手できない 568
NNMi と HPOM が同期されない 568
統合がファイアウォールを経由して動作しない 569
[HP NNMi-HPOM Web サービスの統合設定] フォーム リファレンス 570
NNMi 管理サーバー接続 570
HPOM Management Server Connection (HPOM 管理サーバー接続) 571
統合動作 572
Incident Filter (インシデント フィルタ) 573
インシデント フィルタの例 574
インシデント フィルタの制限 575

HP NNMi Integration Module for Netcool Software 577
HP NNMi Integration Module for Netcool Software 577
値 578
統合製品 578
ドキュメント 579
HP NNMi Integration Module for Netcool Software の有効化 579
HP NNMi Integration Module for Netcool Software の使用法 581
HP NNMi Integration Module for Netcool Software の変更 582
HP NNMi Integration Module for Netcool Software の無効化 582
HP NNMi Integration Module for Netcool Software のトラブルシューティング 583

Netcool/OMNIbus は転送された NNMi 管理イベントを受信しない 583
転送された NNMi 管理イベントの中に Netcool/OMNIbus が受信しないものがある 583
レイヤー 2 接続に対して NNMi フォームを起動するとエラーが発生する 584
HP NNMi Integration Module for Netcool Software 転送先フォームのリファレンス 585
Netcool/OMNIbus SNMP Probe の接続 585
統合コンテンツ 586
転送先ステータス情報 589

xMatters
(以前の AlarmPoint). 591
HP NNMi-xMatters 統合 592
HP NNMi-xMatters 統合について 592
値. 592
統合製品 593
ドキュメント. 593
HP NNMi-xMatters 統合の有効化 593
HP NNMi-xMatters 統合の使用法 594
HP NNMi-xMatters 統合の無効化 595
HP NNMi-xMatters 統合のトラブルシューティング. 595
HP NNMi-xMatters mobile access 統合 595
HP NNMi-xMatters mobile access 統合について 595
値. 595
統合製品 595
ドキュメント. 596
HP NNMi-xMatters mobile access 統合の有効化 596
HP NNMi-xMatters mobile access 統合の使用法 596
HP NNMi-xMatters mobile access 統合の無効化 597
HP NNMi-xMatters mobile access 統合のトラブルシューティング 597

追加情報 599

NNMi 環境変数. 601
このドキュメントで使用する環境変数 601
他の使用可能な環境変数. 601
. 604

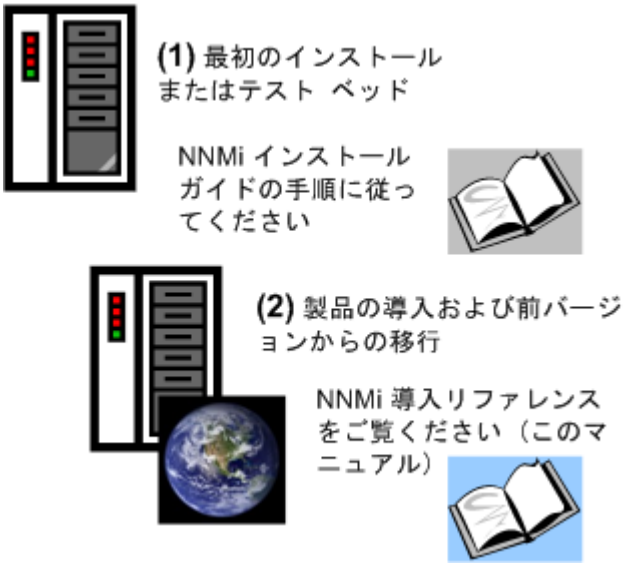
NNMi 9.10 およびウェルノウン ポート 605

設定変更の提案. 609
メッセージおよび解決方法 609
問題および解決策 611

用語集. 615

フィードバックをお待ちしております。. 623

このガイドについて



この章には、以下のトピックがあります。

- ガイドの説明
- このドキュメントで使用するパス表記
- 改訂履歴
- NNMi の詳細

ガイドの説明

このガイドには、NNMi や NNMi Advanced など、HP Network Node Manager i Software を導入するための情報およびベストプラクティスが記載されています。対象読者は、熟練したシステム管理者、ネットワーク エンジニア、または大規模システムのネットワーク導入および管理に経験のある HP サポート エンジニアです。

このガイドでは、制限のある環境 (またはテスト環境) に NNMi をインストール済みであること、クイック スタート設定ウィザードを使用したコニュミティ文字列の設定、ネットワークノードの制限範囲の検出設定、初期管理者アカウントの作成のような、設定作業の開始に慣れていることを仮定しています。これらの作業の詳細は、『NNMi インストール ガイド』を参照してください（3 ページの「使用可能な製品ドキュメント」を参照）。

新しい情報が入手可能になると、製品リリースの間に、HP はこのガイドを更新します。ドキュメントの更新バージョン取得の詳細は、3 ページの「使用可能な製品ドキュメント」を参照してください。

このドキュメントで使用するパス表記

このドキュメントには、NNMi bin ディレクトリに配置されているコマンドのコマンドパスは記載されていません。NNMi bin ディレクトリは以下の場所にあります。

- *Windows Server 2008*: `<drive>¥Program Files¥HP¥HP BTO Software¥bin`
- *UNIX®*: `/opt/OV/bin`

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 2008*:
  - `%NnmInstallDir%`: `<drive>¥Program Files¥HP¥HP BTO Software`
  - `%NnmDataDir%`: `<drive>¥ProgramData¥HP¥HP BTO Software`

  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。

- *UNIX*:
  - `$NnmInstallDir`: `/opt/OV`
  - `$NnmDataDir`: `/var/opt/OV`

  UNIX システムでは、これらの環境変数を使用する場合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、601 ページの「他の使用可能な環境変数」を参照してください。

改訂履歴

次の表に、このドキュメントの新規リリースごとの主要な変更をリストします。

ドキュメント リリース日	主要な変更の説明
2011 年 3 月 (9.10)	完全に更新。 • 英語第 4 版。 • 日本語第 3 版。

NNMi の詳細

NNMi 製品の完全な情報を入手するには、このガイドと他の NNMi ドキュメントを一緒に使用してください。次の表に、現在までのすべての NNMi ドキュメントを示します。ガイドとホワイトペーパーの両方を含みます。

情報はすべて **http://h20230.www2.hp.com/selfsolve/manuals** からダウンロードできます。詳細は、3 ページの「使用可能な製品ドキュメント」を参照してください。

目的	詳しい情報の参照先
このバージョンの NNMi で入手可能な文章の一覧を表示する。	「*NNMi ドキュメント一覧*」をダウンロードします。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 または NNMi Advanced をインストール (初回)。	『NNMi インストール ガイド』をダウンロードします。このガイドには、製品をインストールおよびアンインストールする基本手順、および NNMi クイック スタート設定ウィザードを使用して初期設定を行う方法が記載してあります。 • 『HP Network Node Manager i SoftwareWindows オペレーティング システム用インストール ガイド』 • 『HP Network Node Manager i Software HP-UX オペレーティング システム用インストール ガイド』 • 『HP Network Node Manager i Software Linux オペレーティング システム用インストール ガイド』 • 『HP Network Node Manager i Software Solaris オペレーティング システム用インストール ガイド』
ネットワーク導入の計画 (システム要件へのリンクを含む)。	このガイドの 31 ページの「準備」を参照してください。
製品環境向けに NNMi を設定する。	このガイドの 37 ページの「設定」を参照してください。
NNMi の高度設定を行う。	このガイドの 113 ページの「詳細設定」を参照してください。
NNMi の設定を維持管理する。	このガイドの 345 ページの「NNMi のメンテナンス」を参照してください。
Network Node Manager i ソフトウェアの前バージョン (NNMi 9.0x) から NNMi にアップグレードする。	このガイドの 391 ページの「NNMi 9.0x からのアップグレード」を参照してください。
Network Node Manager の前バージョン (NNM 6.x/7.x) から NNMi にアップグレードする。	『NNMi アップグレード リファレンス』をダウンロードします。
NNMi と統合される製品の詳細を学ぶ。	このガイドの 407 ページの「NNMi との統合」を参照してください。
NNMi 環境変数、ポート、メッセージのリファレンスを参照する。	このガイドの 599 ページの「追加情報」を参照してください。
特定のトピックに関する詳細情報を取得する。	サンプル ドキュメントやホワイト ペーパーからダウンロードします。

目的	詳しい情報の参照先
NNMi ヘルプを印刷する。	ヘルプ コンテンツの PDF をダウンロードします。
HP NNM iSPI NET (NNM iSPI NET) 診断サーバーをインストールし、 NNM iSPI NET の機能について学ぶ。	Network Node Manager SPI for NET 製品カテゴリから、Windows オペレーティング システム用の『*HP NNM iSPI Network Engineering Toolset Planning and Installation Guide*』をダウンロードします。
NNM Developer's Toolkit (SDK) のドキュメントを入手する。	『*HP Network Node Manager i Software Developer's Toolkit Guide*』をダウンロードします。

準備

この項では以下の章について説明します。

- ハードウェアとソフトウェアの要件

ハードウェアとソフトウェアの要件

この章には、以下のトピックがあります。

- 対応ハードウェアとソフトウェア
- 必要なパッチの確認
- システム設定 (UNIX)
- NNMi および NNM iSPI のインストール
- NNMi と HP Performance Insight の共存
- NNMi と HP Operations エージェントの共存

対応ハードウェアとソフトウェア

NNMi をインストールする前に、表 1 で説明する NNMi のハードウェアとソフトウェアの要件に関する情報を読んでください。

上記の最新版のドキュメントは、以下から入手してください。

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

表 1　ソフトウェアおよびハードウェアのプレインストールのチェックリスト

チェック欄 (はい / いいえ)	確認していただくドキュメント
	NNMi インストール ガイド • ファイル名 = `install-guide_ja.pdf` • **Windows** メディア = DVD メイン ドライブ (root) • **UNIX** メディア = ルート ディレクトリ • **NNMi** コンソール = **[ヘルプ] > [NNMi ドキュメント ライブラリ] > [インストール ガイド]**
	NNMi リリース ノート • ファイル名 = `releasenotes_en.html` • **Windows** メディア = DVD メイン ドライブ (root) • **UNIX** メディア = ルート ディレクトリ • **NNMi** コンソール = **[ヘルプ] > [NNMi ドキュメント ライブラリ] > [リリース ノート]**
	NNMi システムおよびデバイスのサポート マトリックス • ファイル名 = `supportmatrix_en.html` • **Windows** メディア = DVD メイン ドライブ (root) • **UNIX** メディア = ルート ディレクトリ • **NNMi** コンソール = リリース ノートからリンクしている

新しい情報が入手可能になると、HP は『NNMi システムおよびデバイスのサポート マトリックス』を更新します。NNMi を導入する前に、以下の Web サイトで、お持ちのバージョンのソフトウェアに関する最新の NNMi 対応マトリックスをチェックしてください。

http://www.hp.com/go/hpsoftwaresupport/support_matrices

(この Web サイトにアクセスするには、HP Passport の ID が必要です。)

NNM スマート プラグイン (NNM iSPI) をインストールする場合は、NNMi 導入時に、これらの製品のシステム要件を組み入れてください。

必要なパッチの確認

NNMi には、組み込みの Java 仮想マシンと JDK バージョン 1.6 が付属しています。Java が正常に動作するには、特定のオペレーティングシステムパッチが必要です。HP-UX オペレーティングシステムを実行しているサーバーに NNMi をインストールする場合、**`HPjconfig`** コマンドを実行して、必要なパッチがサーバーにインストールされているかどうかを確認できます。**`HPJconfig`** を実行する場合、JDK バージョン 1.6 に適した選択を行ってください。HP-UX に **`HPjconfig`** をインストールして実行する方法の詳細については、以下の URL を参照してください。
https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPJCONFIG

HP-UX 以外でサポートされているオペレーティングシステムを実行しているサーバーに NNMi をインストールする場合は、そのオペレーティングシステムのリリースノートを参照してください。

システム設定 (UNIX)

NNMi 管理サーバーに NNMi のマンページを表示できない場合は、MANPATH 変数に /opt/OV/man の場所が含まれていることを確認します。含まれていない場合は、/opt/OV/man の場所を MANPATH 変数に追加します。

NNMi および NNM iSPI のインストール

いずれかの HP NNM iSPI を NNMi とともに使用する場合、HP NNM iSPI をインストールする前に、NNMi をインストールする必要があります。

NNMi と HP Performance Insight の共存

HP Performance Insight と同じサーバーに NNMi をインストールする場合は、次の手順に従って、インストール シーケンスとポート矛盾の問題を回避してください。

1 HP Performance Insight を最初にインストールします。

手順 1 と 手順 2 を完了してから、NNMi をインストールします。

2 HP Performance Insight の全プロセスを停止します。

3 NNMi をインストールします。特定の指示については、『NNMi インストール ガイド』を参照してください。

4 次のコマンドで NNMi の全プロセスを停止します。

```
ovstop -c
```

5 ポート矛盾を解決するには nms-local.properties ファイルを変更します。このファイルは次のディレクトリにあります。

- *Windows*: %NNM_CONF%¥nnm¥props
- *UNIX*: $NNM_CONF/nnm/props

6 HP Performance Insight プロセスを開始します。

7 次のコマンドで NNMi の全プロセスを開始します。

```
ovstart -c
```

HP Performance Insight と同じサーバーに NNMi がインストールされている場合に NNMi をアンインストールすると、HP PI MIB ブラウザを実行したときに例外が発生します。この例外を回避するには、以下の手順を実行します。

1 NNMi をアンインストールします。

2 snmpmib MIB データベースを再作成します。

a **mkdir -p /var/opt/OV/shared/nnm/conf/**

b **/opt/OV/lbin/nnmloadmib -load /usr/OVPI/mibs/GENMIB2IF.mib**

3 nnmloadmib.ovpl コマンドを使用して、追加の MIB をロードします。

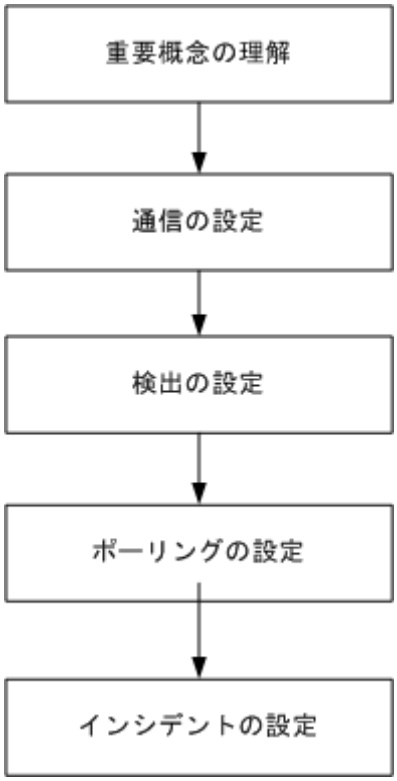
NNMi と HP Operations エージェントの共存

(HP Operations Manager (HPOM) と通信するために) NNMi 管理サーバーに HP Operations エージェントをインストールする場合は、HP Operations エージェントをインストールする前に NNMi をインストールします。

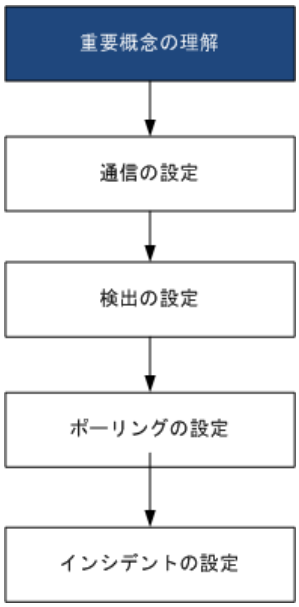
設定

この項では以下の章について説明します。

- 設定の一般概念
- NNMi 通信
- NNMi 検出
- NNMi 状態ポーリング
- NNMi インシデント
- NNMi コンソール



設定の一般概念



この章では概念の概論を説明しています。詳細については、このガイドの後のほうで説明しています。この章では、すべての HP Network Node Manager i Software (NNMi) 設定領域に適用されるベスト プラクティスについても記載しています。

この章には、以下のトピックがあります。

- タスク フロー モデル
- ベストプラクティス : 既存の設定を保存
- ベストプラクティス : 作成者属性を使用する
- ユーザー インタフェース モデル
- 順序
- ノード グループおよびインタフェース グループ
- ノード / インタフェース / アドレス階層
- すべてを停止して再度やり直す

タスク フロー モデル

このガイドの設定の各章では、以下のタスク フローに役立つ情報を記載しています。

1. **概念** - 設定領域の概略を理解できます。このガイドの情報は、NNMi ヘルプの情報を補足しています。
2. **計画** - 設定にどのように取り組むかを決定します。これは、会社のネットワーク管理のマニュアル化を開始または更新するよい機会です。
3. **設定** - NNMi コンソール、設定ファイル、コマンド ライン インタフェースの組み合わせを使用して、設定を NNMi に入力します。具体的な手順については、NNMi ヘルプを参照してください。
4. **評価** - NNMi コンソール で、設定結果を確認します。設定を最適なものにするために、必要に応じて調節します。
5. **調整** - オプション。設定を調整して、NNMi のパフォーマンスを向上します。

ベストプラクティス : 既存の設定を保存

大きな設定変更を行う前には、既存の設定のコピーを保存しておくことをお勧めします。設定を変更した結果が気に入らなくても、保存した設定に簡単に戻すことができます。

nnmconfigexport.ovpl コマンドを使用して、現在の設定を保存します。保存した設定を復元するには、nnmconfigimport.ovpl コマンドを使用します。

これらのコマンドの使用方法の詳細については、該当するリファレンス ページ、または UNIX のマンページを参照してください。

nnmconfigexport.ovpl コマンドでは SNMPv3 資格情報は保持されません。詳細については、*nnmconfigexport.ovpl* リファレンス ページ、または UNIX のマンページを参照してください。

ベストプラクティス : 作成者属性を使用する

多くの NNMi 設定フォームには、**作成者**属性が含まれています。

これらのフォーム上で設定を作成や変更する際は、作成者の組織がわかる値に **[作成者]** 属性を設定してください。NNMi 設定をエクスポートするときに、作成者値を指定して作成者の組織がカスタマイズした項目のみを引き出すことができます。

NNMi をアップグレードする際、作成者値が HP ではない設定は上書きされません。

ユーザー インタフェース モデル

NNMi コンソール フォームの一部では、データベースの更新にトランザクション アプローチが使用されます。NNMi コンソール のフォームで行った変更は、フォームを保存して閉じる操作が NNMi コンソール まで行われないと有効になりません。保存されていない変更 (フォーム上または含まれるフォーム上) が含まれるフォームを閉じると、NNMi によって保存されていない変更があるため、終了を取り消すよう求める警告が表示されます。

[検出シード] フォームは、トランザクション アプローチの例外です。このフォームは便宜上 **[検出の設定]** フォーム上にありますが、他の検出設定からは切り離されています。このため、**[検出の設定]** フォームを保存して閉じて自動検出ルールを実装した後で、これらの自動検出ルールに検出シードを設定する必要があります。

順序

いくつかの NNMi コンソール 設定フォームには、設定を適用する優先順位を設定する**順序**属性が含まれています。ある設定領域で、NNMi は設定内容に対して各項目を、順序番号が最も小さい (低い) ものから大きいものへの順に、NNMi が一致を見つけるまで評価

し続けます。一致が見つかった時点で、NNMi は一致する設定の情報を使用し、これ以上一致を探すのをやめます。(通信設定は例外です。NNMi は、通信設定を完了するためにその他のレベルで情報の検索を続行します。)

順序属性は、NNMi の設定で重要な役割を果たします。予想外の検出結果やステータス結果に遭遇した場合は、その領域の設定の順序を確認してください。

順序はローカル コンテンツ内で適用されます。[メニュー] および [メニュー項目] テーブルには、ローカル コンテキストであるため同じ順序番号の複数のオブジェクトが含まれます。

順序番号は次の箇所でも使用されますが、その意味は異なります。

- **[メニュー]** および **[メニュー項目]** フォームの順序で、関連メニューのローカル コンテキスト内の項目の順序が設定されます。
- **[ノード グループ マップの設定]** フォームのトポロジ マップ順序で、**[トポロジ マップ]** ワークスペースの項目の順序が設定されます。

順序属性が指定の設定領域にどのように影響するかの情報については、その領域の NNMi ヘルプを参照してください。

ベストプラクティス　各設定領域で、小さい順序番号は最も限定的な設定に適用し、大きな順序番号は限定度の最も低い設定に適用します。

ベストプラクティス　各設定領域で、すべての順序番号を一意にしてください。初期設定時は、通常の間隔の順序番号を使用して、将来設定を変更できるような柔軟性を確保しておいてください。たとえば、1 番目から 3 番目の設定には 100、200、300 の順序番号を付けます。

ノード グループおよびインタフェース グループ

NNMi の基本的なフィルタリング手法では、ノードまたはインタフェースをグループ化してから、設定をグループに適用または可視化がグループ別にフィルタリングされます。ノード グループは、以下のいずれかまたはすべての目的に使用できます。

- 監視設定
- インシデント負荷量のフィルタリング
- テーブル フィルタリング
- マップ ビューのカスタマイズ
- グローバル ネットワーク管理機能のリージョナル マネージャからグローバル マネージャに渡されたノードのフィルタリング

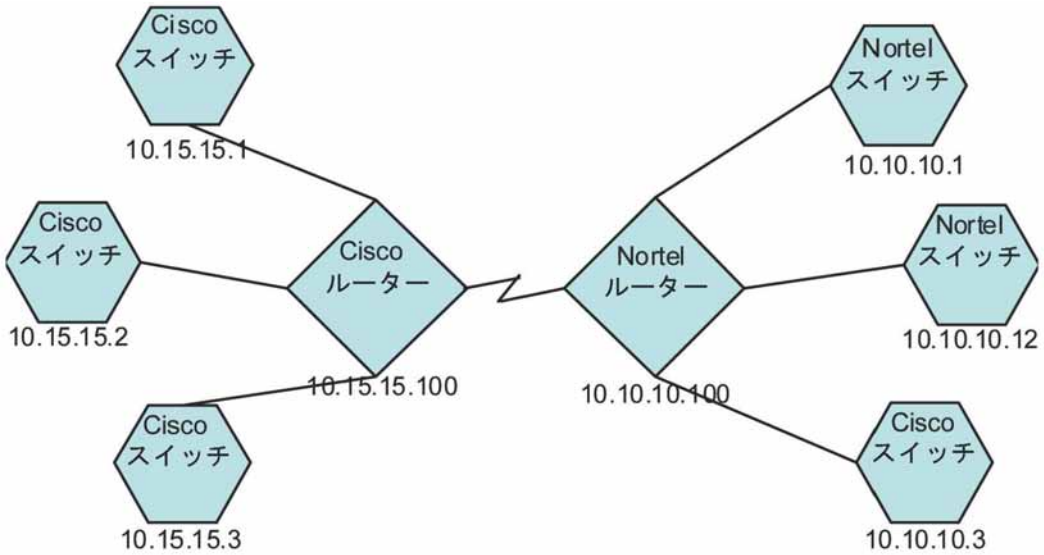
インタフェース グループは、以下のいずれかまたは両方の目的に使用できます。

- 検出からのインタフェース除外
- 監視設定
- インシデント負荷量のフィルタリング
- テーブル フィルタリング

任意のフィルタリング可能な属性に基づきノード グループの階層を作成し、マップ ビューのドリルダウン、監視、またはその両方の設定の継承を管理できます。

グループの重複

グループ定義をどのように使用するかにかかわらず、最初のステップでは、どのノードまたはインタフェースをグループのメンバーにするかを定義します。様々な目的でグループが作成されるため、各々の対象が複数のグループに含まれる可能性があります。次の例を考えてみます。



- 監視を目的とした場合、ベンダーや場所を問わずすべてのスイッチに 3 分間のポーリング間隔を設定するのがよいでしょう。この場合は、デバイス カテゴリ フィルタを使用します。
- 保守を目的とした場合は、すべての Cisco スイッチを 1 つのグループにして、IOS アップグレードではこのグループをまとめてサービス停止にできるようにするのがよいでしょう。この場合は、ベンダー フィルタを使用します。
- 可視化の場合は、10.10.*.* サイト上のすべてのデバイスを、ステータスを反映したコンテナにグループ化するのがよいでしょう。この場合は、IP アドレス フィルタを使用します。

IP アドレスが 10.10.10.3 の Cisco スイッチはこの 3 つのグループすべてに適しています。

設定や表示に便利なようにグループセットを豊富にするのもよいですが、使用されることのない必要以上のエントリを一覧に詰め込みすぎることのないよう、バランスをとってください。

ノード グループのメンバーシップ

NNMi は、検出した各ノードを、設定された各ノード グループと比較することにより、ノード グループのメンバーシップを判断します。

- **[追加のノード]** タブで指定したすべてのノードは、ノード グループのメンバーです。

  NNMi 管理サーバーのリソースを過度に消費するため、**[追加のノード]** タブを使用してノードグループにノードを追加することはほとんどありません。

- **[子ノード グループ]** タブで指定した少なくとも 1 つのノード グループのメンバーになっているすべてのノードは、そのノード グループのメンバーです。
- **[デバイス フィルター]** タブの 1 つ以上のエントリ (存在する場合)、*および* **[追加のフィルター]** タブで指定したフィルタに一致するすべてのノードは、そのノード グループのメンバーです。

階層 / コンテインメント

単純で再利用可能な原子グループを作成し、これらを監視や可視化のために階層的に組み合わせることができます。階層的なノードのコンテナを使用することにより、障害時にオブジェクトの場所やタイプに関する手がかりが得られるので、マップ ビューが大きく向上します。NNMi により、グループの定義とそのドリルダウン順序の徹底管理が可能になります。

単純で再利用可能な原子グループを最初に作成し、その後にこれらを増築するときの子グループとして指定します。また、最初に一番大きな親グループを指定し、それから子グループを作成していくこともできます。

たとえば、ネットワークが Cisco スイッチ、Cisco ルーター、Nortel スイッチ、Nortel ルーターで構成されているとします。Cisco デバイスの親グループとすべてのスイッチの親グループを作成できます。親を作成してその子を指定するときに階層が指定されるので、Cisco スイッチのようなそれぞれの子グループには複数の親ができる可能性があります。

階層は、以下の状況で使用すると効果的です。

- 監視 ニーズが類似したノードのタイプ
- ノードの地理的な配置
- まとめてサービス停止にするノードのタイプ
- オペレータの職務別のノードのグループ

マップ ビューおよびテーブル ビューでグループを使用すると、伝播された (設定可能な) グループのステータスが表示されます。

グループ定義を使用して監視設定を指定する際に階層は設定の順序を示す*のではない*ことを留意してください。小さい順序番号の設定は、ノードに適用されます。順序番号を注意深く増分することで、設定の継承概念を真似ることができます。

設定インタフェースでは、循環階層の定義が自動的に防御されます。

デバイス フィルタ

検出中、NNMi は直接情報を SNMP クエリーで収集し、そこから他の情報を、デバイス プロファイルを通じて導き出します。(詳細については、60 ページの「NNMi はデバイス プロファイルから属性を導き出す」を参照してください。) システム オブジェクト ID を収集することにより、NNMi は正しいデバイス プロファイルを通じて索引化して、次の情報を導き出します。

- ベンダー

- デバイス カテゴリ
- カテゴリ内のデバイス ファミリー

導出されたこれらの値は、デバイス プロファイルそのものとともに、フィルタとして使用できます。

たとえば、特定のベンダー製のすべての対象物を、デバイス タイプやファミリーに関係なくグループ化できます。また、ある種類のデバイス（たとえばルーター）をすべて、ベンダーを問わずにまとめることができます。

追加フィルタ

追加のフィルタ エディタを使用すると、以下のようなフィールドに一致するカスタム論理を作成できます。

- hostname (ホスト名)
- mgmtIPAddress (管理アドレス)
- hostedIPAddress (アドレス)
- sysName (システム名)
- sysLocation (システムのロケーション)
- sysContact (システムの連絡先)
- capability (機能の一意キー)
- customAttrName (カスタム属性名)
- customAttrValue (カスタム属性値)

フィルタには、AND、OR、NOT、EXISTS、NOT EXISTS、およびグループ化 (括弧) 操作を含めることができます。詳細については、NNMi ヘルプの「*ノード グループ追加フィルタの指定*」を参照してください。

機能は、本来は NNMi と統合される他のプログラムを目的としていました。たとえば、ルーター冗長性とコンポーネント稼働状態は、機能 (フィールド) を NNMi データベースに追加します。これらの機能は、すでに検出されてデバイスからノード詳細を調べることにより、見ることができます。

iSPI によりカスタム属性を追加したり、独自のカスタム属性を作成できます。Web Services SDK を購入していない方は、各ノードのフィールドに手動で値を入れる必要があります。たとえば資産番号やシリアル番号は属性となりえますが、機能ではありません。

追加ノード

ノードグループに対してノードを限定するには、**[追加フィルタ]** を使用することをお勧めします。フィルタを使用して制限することが困難である重要なデバイスがネットワークに含まれている場合、それらのデバイスをホスト名ごとに 1 つのグループに追加します。ホスト名ごとにノードをノードグループに追加するのは、他に手段がない場合のみにしてください。

NNMi 管理サーバーのリソースを過度に消費するため、**[追加のノード]** タブを使用してノードグループにノードを追加することはほとんどありません。

ノード グループのステータス

そのように設定すると、以下のいずれかのアルゴリズムを使用して NNMi によってノード グループのステータスが決定されます。

- ノード グループの任意のノードの最も深刻なステータスと一致するようにノード グループを設定します。このアプローチを使用するには、**[ステータスの設定]** フォームの **[ほとんどの重大なステータスを伝達]** チェックボックスを選択します。
- 各ターゲット ステータスに設定されたしきい値を使用してノード グループのステータスを設定します。たとえば、警戒域のターゲット ステータスのデフォルトしきい値は 20% です。NNMi では、ノード グループ内のノードの 20% (または、それ以上) が警戒域ステータスになると、ノード グループのステータスが警戒域に設定されます。このアプローチを使用するには、**[ステータスの設定]** フォームの **[ほとんどの重大なステータスを伝達]** チェックボックスをオフにします。ターゲットしきい値のパーセントしきい値は、このフォームの **[ノード グループのステータス設定]** タブで変更できます。

大きなノード グループのステータス計算には大量のリソースが必要になるため、新規インストール時にはノード グループのステータス計算は NNMi のデフォルトでオフに設定されます。(NNMi 8.x からのアップグレードでは、それ以前のステータス計算設定が保持されます。) ステータスの計算は、各ノード グループの **[ノード グループ]** フォームの **[ステータスの計算]** チェックボックスで有効にすることができます。

インタフェース グループ

インタフェース グループは、ノード内のインタフェースを、IFType 別に、または ifAlias、ifDescr、ifName、ifIndex、IP アドレスなど他の属性別にフィルタリングします。インタフェース グループは階層もコンテインメントも継承しませんが、インタフェースをホスト管理しているノードのノード グループに基づいてメンバーシップをさらに限定することができます。

インタフェース グループを、ノード グループと同様のカスタム機能および属性でフィルタリングできます。

インタフェース グループの制限は、タブ内およびタブ間でまとめて AND を適用します。

ノード / インタフェース / アドレス階層

NNMi は監視設定を、以下の方式で割り当てます。

1. **インタフェース設定** - NNMi は、ノードのインタフェースおよび IP アドレスの各々を、最初に一致する**インタフェース設定**定義に基づいてモニターします。最初に一致するのは、順序番号が最も小さい**インタフェース設定**定義です。
2. **ノード設定** - NNMi によって、各ノードと前回一致しなかった各インタフェースまたは IP アドレスが、最初に一致する**ノード設定**定義に基づき監視されます。最初に一致するのは、順序番号が最も小さい**ノードの設定**定義です。

   子ノード グループは、順序階層に含まれます。親ノード グループの順序番号のほうが小さい場合 (たとえば、親 =10、子 =20)、親ノード グループに指定された監視設定は子ノード グループ内のノードにも適用されます。親ノード グループ 監視設定を上書きするには、子ノード グループの順序番号を親よりも小さな番号に設定します (たとえば、親 =20、子 =10)。

3. **デフォルト設定** - 手順 1 または 手順 2 のノード、インタフェース、IP アドレスに一致が見つからない場合、NNMi ではデフォルトの監視設定が適用されます。

すべてを停止して再度やり直す

検出を完全に再スタートして NNMi 設定のすべてのやり直したい場合、または NNMi データベースが破損した場合は、NNMi 設定およびデータベースをリセットできます。このプロセスにより、NNMi 設定、トポロジ、およびインシデントのすべてが削除されます。

この手順で説明しているコマンドの詳細は、該当する参照ページか UNIX のマンページを参照してください。

以下の手順に従ってください。

1 NNMi サービスを、次のコマンドを使用して停止します。

```
ovstop -c
```

2 オプション。この手順によってデータベースが削除されるため、実行する前に次のコマンドで既存のデータベースをバックアップするとよいでしょう。

```
nnmbackup.ovpl -type offline -target <backup_directory>
```

3 オプション。現在の NNMi 設定をとっておきたい場合は、`nnmconfigexport.ovpl` コマンドを使用して NNMi 設定を XML ファイルに出力します。

nnmconfigexport.ovpl コマンドでは SNMPv3 資格情報は保持されません。詳細については、*nnmconfigexport.ovpl* リファレンス ページ、または UNIX のマンページを参照してください。

4 オプション。`nnmtrimincidents.ovpl` コマンドを使用して、NNMi インシデントをアーカイブします。

5 NNMi データベースを削除して再作成します。

- 組み込みデータベースの場合は、次のコマンドを実行します。

```
nnmresetembdb.ovpl -nostart
```

- Oracle データベースの場合は、Oracle データベース管理者に NNMi データベースの削除と再作成を依頼してください。データベース インスタンス名は、削除せずに保持してください。

6 iSPI または NNMi と統合されるスタンドアロン製品をインストールした場合は、これらの製品をリセットして古いトポロジ識別名を削除します。具体的な手順については、製品のマニュアルを参照してください。

7 NNMi サービスを、次のコマンドを使用して開始します。

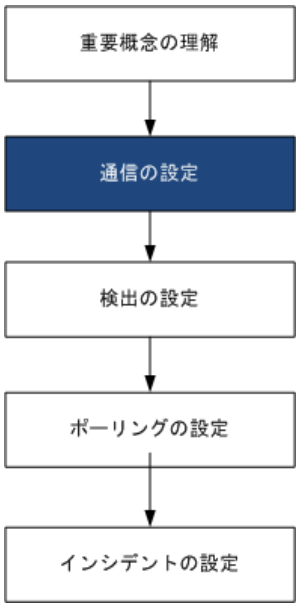
```
ovstart -c
```

これで NNMi はデフォルト設定のみとなり、本製品を新しいシステムにインストールしたのと同じ状態です。

8 NNMi の設定を開始します。以下のいずれかを行います。

- 「クイック スタート設定ウィザード」を使用します。
- NNMi コンソール の **[設定]** ワークスペースに情報を入力します。
- `nnmconfigimport.ovpl` コマンドを使用して、手順 3 で保存した NNMi 設定の一部またはすべてをインポートしてください。

NNMi 通信



HP Network Node Manager i Software (NNMi) は、Simple Network Management Protocol (SNMP) と Internet Control Message Protocol (ICMP ping) の両方のプロトコルを使用して、デバイスを検出し、デバイスのステータスとヘルスを監視します。各自の環境で実行可能な通信を確立するには、ネットワークのさまざまなデバイスとエリアについて、アクセス資格認定、適切なタイムアウト、再試行値すべてで NNMi を設定します。ネットワークのいくつかのエリアでプロトコルを無効にし、トラフィックを削減またはファイアウォールを順守できます。

設定する通信の値は NNMi の検出および状態ポーリングの基礎を形成します。NNMi は、検出またはポーリングのクエリを作成するときに、各デバイスに該当する値を適用します。このように、ネットワークのいくつかの領域との SNMP 通信を無効にするよう NNMi を設定すると、NNMi 検出と NNMi 状態ポーリングはどちらも、SNMP 要求をその領域には送信できません。

この章には、以下のトピックがあります。

- 通信の概念
- 通信の計画作成
- 通信の設定
- 通信の評価
- 通信の調整

通信の概念

NNMi は、SNMP と ICMP をおもに要求と応答の方式で使います。ICMP Ping 要求への応答で、アドレスの応答性を確認します。特定の MIB オブジェクトに対する SNMP 要求への応答で、ノードに関するより総合的な情報を取得します。

以下の概念が NNMi 通信設定に適用されます。

- 通信の設定レベル
- ネットワーク待ち時間とタイムアウト
- SNMP アクセス制御
- SNMP バージョンの優先
- 管理アドレスの優先
- ポーリング プロトコル
- 通信設定および nnmsnmp*.ovpl コマンド

通信の設定レベル

NNMi 通信設定には、以下のレベルがあります。

- 特定のノード
- 領域
- グローバルなデフォルト

各レベルで、アクセス資格認定、タイムアウトと再試行の値、ICMP と SNMP のプロトコル使用可能性、SNMP アクセス設定を設定できます。あるレベルで設定をブランクにしておくと、NNMi は次のレベルのデフォルトを適用します。

指定ノードと通信するとき、NNMi は設定を以下のように適用します。

1. ノードが**特定のノード**の設定と一致する場合、NNMi はその設定に含まれている通信の値をすべて利用します。
2. どの設定もまだ定義されていない場合、NNMi はノードがいずれかの**領域**に属するか判断します。領域は重なる可能性があるため、NNMi では順序番号が最小のものと一致する領域が使用されます。NNMi は、その領域に対して指定された値を、該当する特定のノードの空白の値 (ある場合) に使用します。追加領域の設定は考慮されません。
3. まだ定義されない設定がある場合、NNMi は**グローバルなデフォルト**設定を使用して、残りの空白の設定に取り込みます。

特定のデバイスとの ICMP 通信および SNMP 通信に使用される値は、必要な設定がすべて決まるまで、累積的に構築されます。

ネットワーク待ち時間とタイムアウト

通常のネットワーク遅延は、NNMi 管理サーバーが ICMP クエリと SNMP クエリへの応答を得るための待ち時間に影響を与えます 一般に、ネットワークのエリアが異なれば、応答が返る時間も異なります。たとえば、NNMi 管理サーバーが置かれているローカルネットワークからは、ほぼ即時の応答が返り、ダイヤルアップ ワイド エリア リンク経由

でアクセスする遠隔地にあるデバイスからの応答は、通常、はるかに長く時間がかかります。さらに、負荷が大きいデバイスは処理量が多いため ICMP クエリまたは SNMP クエリにただちに応答できません。タイムアウトと再試行の設定を決定するときには、こうした遅延に関する事項を考慮してください。

ネットワーク領域と特定のデバイスの両方について、固有のタイムアウトと再試行の設定を行うことができます。設定により、応答がない場合に要求を破棄するまでの、NNMi の応答待ち時間、NNMi がデータを要求する回数が決まります。

要求を再試行するたびに、NNMi は設定したタイムアウト値をそれまでのタイムアウト値に加算します。そのため、再試行するごとに停止時間が長くなります。たとえば、NNMi の設定を 5 秒でタイムアウト、再試行は 3 回とすると、NNMi は最初の要求への応答を 5 秒待ち、2 回目の要求への応答は 10 秒待ち、3 回目の要求の応答は 15 秒待ってから次のポーリング サイクルに移ります。

SNMP アクセス制御

管理対象デバイス上の SNMP エージェントとの通信には、アクセス制御資格情報が必要です。

- SNMPv1 と SNMPv2c

  各 NNMi 要求内のコミュニティ文字列は、応答する SNMP エージェントで設定されているコミュニティ文字列と一致する必要があります。通信はすべて、クリア テキスト (暗号化なし) でネットワークを通過します。

- SNMPv3

  SNMP エージェントとの通信は、ユーザーベースのセキュリティ モデル (USM) に従います。各 SNMP エージェントには、設定済みのユーザー名とそれに関連する認証要件のリストがあります (認証プロファイル)。すべての通信のフォーマットは、設定によって制御されます。NNMi SNMP 要求は、有効なユーザーを指定し、そのユーザーに対して設定されている認証とプライバシの制御に従う必要があります。

  — 認証プロトコルは、メッセージダイジェスト アルゴリズム 5 (MD5) またはセキュア ハッシュ アルゴリズム (SHA) のいずれか選択した方を使って、ハッシュベースのメッセージ認証コード (HMAC) を使用します。

  — プライバシ プロトコルは、暗号化を使用しないか、またはデータ暗号化標準 - 暗号ブロック連鎖 (DES-CBC) 対称暗号化プロトコルを使用します。

NNMi は、(IP アドレス フィルタやホスト名フィルタ経由で定義された) ネットワークの領域のマルチ SNMP アクセス制御資格情報の仕様をサポートします。NNMi は、設定したすべての値を、所定の SNMP セキュリティ レベルで並行して試し、その領域内のデバイスと通信しようとします。NNMi がその領域で使用する最小限の SNMP セキュリティ レベルを指定できます。NNMi は、各ノードから返される最初の値 (デバイスの SNMP エージェントからの応答) を検出と監視の目的で使用します。

SNMP バージョンの優先

SNMP プロトコルはバージョン 1 から バージョン 2(c) へと長年をかけて発展したもので、現在はバージョン 3 です。この間、とりわけセキュリティ機能は強化されてきました。NNMi は、各自のネットワーク環境でどのバージョンでも処理できますし、全バージョンの混合したものも処理できます。

NNMi が特定のノードについて受信する最初の SNMP 応答によって、そのノードとの通信に NNMi が使用する通信の資格情報と SNMP バージョンが決まります。

ノードの SNMP バージョンにより、NNMi でのノードからのトラップの受け入れが、以下のように異なります。

- NNMi が SNMPv3 を使用して受信トラップのソース ノードやソースオブジェクトを検出すると、NNMi は、受信する SNMPv1、SNMPv2c、および SNMPv3 のトラップを受け入れます。
- NNMi が SNMPv1 または SNMPv2c を使用して受信トラップのソース ノードやソースオブジェクトを検出すると、NNMi は受信する SNMPv3 トラップを廃棄します。

SNMP バージョンと、ネットワークの各領域で受け入れられる最小レベルのセキュリティ設定を指定します。[SNMP 最小セキュリティレベル] フィールドのオプションは、以下のとおりです。

- **[コミュニティのみ (SNMPv1)]** - NNMi は、コミュニティ文字列、タイムアウトおよび再試行用に設定した値で SNMPv1 を使って更新を試みます。NNMi は、SNMPv2c や SNMPv3 の設定は試みません。
- **[コミュニティのみ (SNMPv1 または v2c)]** - NNMi は、コミュニティ文字列、タイムアウトおよび再試行用に設定した値で SNMPv2c を使って更新を試みます。SNMPv2 を使ったコミュニティ文字列への応答がない場合は、NNMi はコミュニティ文字列、タイムアウト、および再試行用に設定した値で SNMPv1 を使って通信を試みます。NNMi は、SNMPv3 の設定は試みません。
- **[コミュニティ]** - NNMi は、コミュニティ文字列、タイムアウトおよび再試行用に設定した値で SNMPv2c を使って更新を試みます。SNMPv2 を使ったコミュニティ文字列への応答がない場合は、NNMi はコミュニティ文字列、タイムアウト、および再試行用に設定した値で SNMPv1 を使って通信を試みます。機能するものがない場合、NNMi は SNMPv3 を試みます。
- **[認証なし、プライバシなし]** - 認証もプライバシもないユーザーについて、NNMi はタイムアウトと再試行用に設定した値で SNMPv3 を使って通信を試みます。機能するものがない場合、必要に応じて、NNMi は 認証はあるがプライバイシがないユーザー、次に、認証とプライバシがあるユーザーを試みます。
- **[認証、プライバシなし]** - 認証はあるがプライバシはないユーザーについて、NNMi はタイムアウトと再試行用に設定した値で SNMPv3 を使って通信を試みます。機能するものがない場合、NNMi は認証とプライバシのあるユーザーを試みます。
- **[認証、プライバシ]** - 認証もプライバシもあるユーザーについて、NNMi はタイムアウトと再試行用に設定した値で SNMPv3 を使って通信を試みます。

管理アドレスの優先

ノードの**管理アドレス**とは、NNMi がノードの SNMP エージェントと通信する場合に使用するアドレスです。ノードの管理アドレスを指定するか (特定ノードの設定で)、または、ノードに関連する IP アドレスの中から NNMi がアドレスを選択するようにできます。検出設定で検出から特定のアドレスを除外することにより、この動作を微調整できます。NNMi が管理アドレスを決定する方法については、NNMi ヘルプの「[ノード] *フォーム*」を参照してください。

NNMi は、デバイスの検出と監視を継続的に行います。*最初の NNMi 検出サイクルの後*、以前検出した SNMP エージェントが応答しない場合 (たとえば、デバイスの SNMP エージェントを再設定した場合など) は、**[SNMP アドレスの再検出を有効にします]** フィールドの設定により NNMi の動作が制御されます。

- **[SNMP アドレスの再検出を有効にします]** チェック ボックスがオンになっている場合、NNMi は機能するアドレスの検索で設定した値を再試行します。
- **[SNMP アドレスの再検出を有効にします]** チェック ボックスがオフになっている場合、NNMi はデバイスが「停止中」であると報告し、そのデバイスについて別の通信設定を試みません。

[SNMP アドレスの再検出を有効にします] チェック ボックスは、通信設定のすべてのレベルで使用できます。

自動検出ルール設定フィールドの **[SNMP デバイスの検出]** と **[非 SNMP デバイス]** は、NNMi の SNMP 使用方法に影響します。詳細については、NNMi ヘルプにある「*自動検出ルールの基本設定を設定する*」を参照してください。

ポーリング プロトコル

ネットワークの一部で NNMi が SNMP または ICMP 用を使用しないようにすることができます (たとえば、インフラストラクチャ内のファイアウォールが ICMP または SNMP トラフィックを制限する場合など)。

ネットワークのある領域にあるデバイスへの ICMP トラフィックを無効にすると、NNMi では以下のような結果が生じます。

- オプションの自動検出ルール ping スィープ機能は、ネットワークの領域内で追加ノードを見つけられません。すべてのノードが、シードされるか、または隣接 ARP キャッシュ、Cisco Discovery Protocol (CDP)、または Extreme Discovery Protocol (EDP) など、MIB オブジェクト要求への応答を通して使用できる必要があります。広域ネットワーク デバイスは、すべてシードしないと失われる可能性があります。
- StatePoller は、SNMP 要求に応答するように設定されていないデバイスは監視できません。(ただし、デバイスが SNMP に応答すると、StatePoller は ICMP を使用しません。)
- オペレータはトラブルシューティングの間は、**[アクション] > [Ping]** を使ってデバイス到達可能性をチェックできません。

ネットワークのある領域にあるデバイスへの SNMP トラフィックを無効にすると、NNMi では以下のような結果になります。

- 検出では、存在しないデバイスの情報は収集できません。 すべてのデバイスで `No SNMP デバイス` プロファイルを受信します。
- 検出では、クエリによって追加の隣接デバイスを見つけることができません。デバイスはすべて直接にシードされる必要があります。

- 検出では、データベースから接続情報を収集できないため、デバイスは NNMi マップには未接続として示されます。
- No SNMP デバイス プロファイルを持つデバイスについては、StatePoller は ICMP (Ping) のみを使用するデバイスの監視のデフォルトが優先されます。
- StatePoller は、コンポーネントの稼動状態やパフォーマンス データをデバイスから収集できません。
- Causal Engine は、デバイスに接触して近隣分析を実行し、インシデントの根本分析を見つけることはできません。

通信設定および nnmsnmp*.ovpl コマンド

nnmsnmp*.ovpl コマンドは、NNMi データベースで指定されていないデバイス通信設定の値を検索します。この方法では ovjboss プロセスが動作している必要があります。ovjboss が動作していない場合、nnmsnmp*.ovpl コマンドは次のように動作します。

- SNMPv1 エージェントと SNMPv2c エージェントの場合、コマンドは未指定通信設定にデフォルト値を使用します。
- SNMPv3 エージェントの場合は、ユーザーとパスワードを指定すると、コマンドは未指定通信設定にデフォルト値を使用します。ユーザーとパスワードを指定しないと、コマンドはエラーになります。

通信の計画作成

以下の領域で決定します。

- デフォルトの通信設定
- 通信設定領域
- 特定のノードの設定
- 再試行とタイムアウトの値
- アクティブなプロトコル
- 複数のコミュニティ文字列または認証プロファイル

デフォルトの通信設定

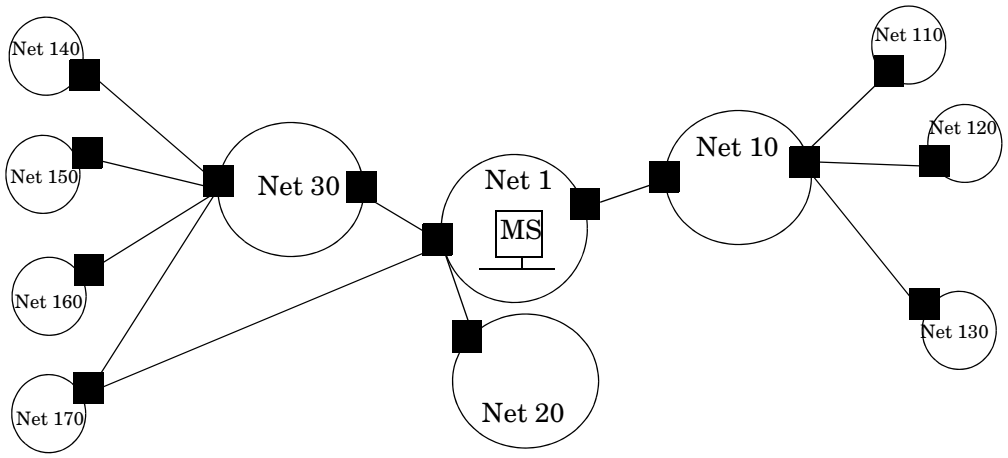
NNMi は、該当する領域や特定のノードで指定しなかった設定をデフォルト値を使用して完成させるため、大半のネットワークで妥当なものになるようデフォルトを設定します。

- NNMi が試す必要のある一般に使われるコミュニティ文字列がありますか？
- ネットワークではどのようなタイムアウトと再試行のデフォルト値が合理的でしょうか？

通信設定領域

領域とは、ネットワーク内で同じ通信設定を適用するのが妥当なエリアのことです。たとえば、NNMi 管理サーバーの近くにあるローカル ネットワークからは、通常はすぐに応答が戻ってきます。複数ホップ離れたネットワーク エリアなら応答にもっと時間がかかるのが普通です。

ネットワークのサブネットやエリアを個別に設定する必要はありません。ラグ タイムが近い複数のエリアを 1 つの領域にまとめることができます。次のネットワーク マップについて考えてみてください。



タイムアウトと再試行を考慮した場合、以下のように領域を設定することができます。

- 領域 A - Net 1
- 領域 B - Net 10、Net 20、および Net 30 を含める
- 領域 C - さらに遠くにある外部のネットワーク

NNMi 管理サーバーから 1 ホップまたは 2 ホップのどちらのパスを優先するようトラフィック管理構成が設定されているかどうかに従って、Net 170 をグループにまとめる最良の方法を決定します。

また、類似したアクセス資格認定を使用するデバイスをグループにまとめる場合にも領域を使用します。ネットワークのすべてのルーターで同じコミュニティ文字列 (または可能なコミュニティ文字列の一部) が使用されていて、命名規約 (`rtr`*`nnn`*`.yourdomain.com` など) でルーターを識別できる場合は、全ルーターを 1 つの領域に設定すれば、すべてのルーターが同じように処理されます。ワイルドカードを使ってデバイスをグループにまとめられない場合は、各デバイスを特定のノードとして設定できます。

同じタイムアウト/再試行の値とアクセス資格証明設定を 1 つの領域のすべてのノードに適用できるように、領域設定を計画してください。

領域定義は重複することがあり、1 つのデバイスが複数の領域の定義にあてはまることもあります。NNMi は、順序番号が最も小さい (かつ、他に一致する領域がない) 領域から設定を適用します。

特定のノードの設定

固有の通信設定要件を持つデバイスの場合、特定ノードの設定を使用して、そのノードの通信設定を指定します。特定ノードの設定の使用例として、以下の例があります。

- SNMPv2c/SNMPv3 GetBulk 要求に適切に応答しないノード
- 他の類似ノードと名前のパターンが一致しないノード

再試行とタイムアウトの値

タイムアウトの時間を長く、再試行の回数を多く設定すると、ビジー状態にあるか、または離れたところにあるデバイスからより多くの応答を集められます。このように応答率が高まると、偽のダウン メッセージを除外できます。しかし、実際にダウンしているデバイスに注意が必要なことを知るのに時間がかかるようにもなります。ネットワークの各領域のバランスを見出すことは重要であり、このために各自の環境で値のテストと調整の期間が必要になる可能性があります。

各ホップの現在のラグ タイムに関するヒントを得るには、以下を実行します。

- *Windows*: それぞれのネットワーク エリア内のデバイスに対して `tracert` を実行する。
- *UNIX*: それぞれのネットワーク エリア内のデバイスに対して `traceroute` を実行する。

アクティブなプロトコル

通信の設定と監視の設定を使用して、ネットワーク内でデバイスと通信を行うときに NNMi が生成するトラフィックの種類を制御することができます。インフラストラクチャのファイアウォールで ICMP または SNMP のトラフィックが許可されていない場合は通信の設定を使用します。デバイスに関するデータの特定のサブセットが必要ない場合は、監視の設定を使用してプロトコルの使用を微調整します。通信または監視の設定のどちらかによってデバイスのプロトコルが無効にされると、NNMi はその種類のトラフィックをデバイスに送信しません。

SNMP 通信を無効にすると、ネットワークの NNMi のステータスと稼動状態の監視機能がかなり危険な状態になります。

各領域または特定のデバイスは ICMP トラフィックを受信するはずであるかに注意してください。

アクセス資格認定を与えないデバイスとの SNMP 通信を明示的に無効にする必要はありません。デフォルトで、NNMi はこれらのデバイスを `No SNMP` デバイス プロファイルに割り当て、ICMP のみを使ってデバイスを監視します。

複数のコミュニティ文字列または認証プロファイル

ネットワークの各エリアで試みるコミュニティ文字列と認証プロファイルの計画を作成します。デフォルト設定と領域設定については、並行して試みる複数のコミュニティ文字列と認証プロファイルを設定できます。

有望なコミュニティ文字列を試す間に、NNMi クエリにより、デバイスで資格認定不合格が生成されることがあります。NNMi が初期検出を完了する間に、資格認定不合格は安全に無視できる可能性があることを業務部に知らせてください。代わりに、領域 (と試行する関連コミュニティ文字列と認証プロトコル) が可能な限り厳しく設定して、資格認定不合格の数を最小にすることもできます。

環境で SNMPv1 または v2 と SNMPv3 が使用されている場合は、各領域で受け入れられる最低のセキュリティ レベルを決定してください。

SNMPv1 と SNMPv2 のコミュニティ文字列

SNMPv1 または v2c アクセスが可能な領域では、領域内で使用されるコミュニティ文字列と特定のデバイスで必要とされるコミュニティ文字列を集めます。

SNMPv3 の認証プロファイル

SNMPv3 アクセスが可能なデバイスを含む領域では、受け入れられる最小限のデフォルト認証プロファイル、各領域に適した認証プロファイル、および特定のデバイスで使用される固有の認証資格証明 (ある場合) を決定します。ネットワーク内で使用中の認証プロトコルとプライバシ プロトコルも判断します。

SNMPv3 通信の場合、NNMi では以下の認証プロトコルがサポートされます。

- HMAC-MD5-96
- HMAC-SHA-1

SNMPv3 通信の場合、NNMi では以下のプライバシ プロトコルがサポートされます。

- DES-CBC
- TripleDES
- AES-128
- AES-192
- AES-256

固有ノードまたは領域設定ごとに、1 つの認証プロトコルおよび 1 つのプライバシ プロトコルを指定できますが、指定しないこともできます。

TripleDES、AES-192、AES-256 のプライバシ プロトコルを使用するには、Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files ライブラリが必要です。詳細については、56 ページの「NNMi における SNMPv3 プライバシ プロトコルの使用準備」を参照してください。

通信の設定

この項を読んだ後、特定の手順については、NNMi ヘルプの「*通信プロトコルを設定する*」を参照してください。

大きな設定変更を行う前には、既存の設定のコピーを保存しておくことをお勧めします。詳細については、40 ページの「ベストプラクティス : 既存の設定を保存」を参照してください。

通信の以下のエリアの設定

- デフォルト設定
- 領域定義とその設定
- 特定のノードの設定

特定のノードについて、NNMi コンソール または構成ファイルによって、ノードの設定を入力できます。

すべての［**通信の設定**］を［**保存して閉じる**］と、NNMi コンソール に戻り、変更が導入されます。

ベストプラクティス　定義した領域の順序番号をダブルチェックします。ノードが複数の領域を認証する場合、NNMi はそのノードの順序番号の最も小さい領域の設定を適用します。

NNMi における SNMPv3 プライバシ プロトコルの使用準備

NNMi コンソールの **[SNMPv3 設定]** フォームでは、SNMPv3 デバイスとのやり取りに使用するプライバシ プロトコルを指定できます。Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files ライブラリが NNMi 管理サーバーにインストールされている場合に限り、AES-192、AES-256、TripleDES のプロトコルを使用できます。

SNMPv3 通信用に AES-192、AES-256、TripleDES のプライバシ プロトコルを NNMi で使用できるようにするには、以下の手順を実行します。

1. Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files ライブラリを、Java 開発者用の Oracle Technology Network Web サイト (**http://www.oracle.com/technetwork/java/index.html**) からダウンロードします。直接リンクは以下のとおりです。
   https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_Developer-Site/en_US/-/USD/ViewProductDetail-Start?ProductRef=jce_policy-6-oth-JPR@CDS-CDS_Developer
2. ダウンロードしたパッケージを展開してから、両方の JAR ファイル (`local_policy.jar` および `US_export_policy.jar`) を以下の場所にコピーします。
   - *Windows*: `%NnmInstallDir%¥nonOV¥jdk¥nnm¥jre¥lib¥security`
   - *UNIX*: `$NnmInstallDir/nonOV/jdk/nnm/jre/lib/security`
3. 以下のコマンドを実行して `ovjboss` を再開します。
   a. **`ovstop ovjboss`**
   b. **`ovstart ovjboss`**

通信の評価

この項では、通信設定の進行と成功を評価する方法をリストします。これらの作業のほとんどを完了できるのは、検出が完了した後です。

以下について考えます。

- すべてのノードが SNMP 用に設定されましたか？
- デバイスについて SNMP アクセスは現在利用できますか？
- 管理 IP アドレスは正しいですか？
- NNMi は正しい通信設定を使っていますか？
- State Poller 設定は通信設定と一致していますか？

すべてのノードが SNMP 用に設定されましたか？

1 **[ノード]** インベントリ ビューを開きます。

2 **[デバイス プロファイル]** 列を、文字列 `No SNMP` が含まれるようにフィルタリングします。

- 管理するデバイスごとに、特定ノードの通信設定を行います。その代わりに、領域を拡張して、ノードを組み入れ、アクセス資格認定を更新することもできます。
- 通信設定が正しい場合は、デバイスの SNMP エージェントが実行中であり、適切に設定されていることを確認します (ACL を含みます)。

デバイスについて SNMP アクセスは現在利用できますか？

1 インベントリ ビューでノードを選択します。

2 **[アクション] > [ステータス ポーリング]** または **[アクション] > [ポーリングの設定]** を選択します。

結果に SNMP の値が表示された場合、通信は動作中です。

コマンド ラインから `nnmsnmpwalk.ovpl` コマンドで通信をテストすることもできます。詳細については、*nnmsnmpwalk.ovpl* リファレンス ページ、または UNIX のマンページを参照してください。

管理 IP アドレスは正しいですか？

デバイスに対して NNMi が選択した管理アドレスを判定するには、以下の手順を実行します。

1 インベントリ ビューでノードを選択します。

2 **[アクション] > [通信の設定]** を選択します。

3 **[通信の設定]** ウィンドウで、[アクティブな SNMP エージェント設定] リストにある SNMP エージェントの管理アドレスが正しいことを確認します。

NNMi は正しい通信設定を使っていますか？

SNMP コミュニティ文字列が欠落しているか、または正しくない場合は、検出が不完全になる可能性があり、検出パフォーマンスに悪影響を及ぼす可能性もあります。

デバイスの通信設定を確認するには、`nnmcommconf.ovpl` コマンドを使用するか、または以下の手順を実行します。

1 インベントリ ビューでノードを選択します。

2 **[アクション] > [通信の設定]** を選択します。

3 **[通信の設定]** ウィンドウで、SNMP 設定テーブルにリストされた値が、NNMi でこのノードに使用する設定であることを確認します。

通信設定が正しくない場合、問題解決の手始めとして、SNMP 設定テーブル内のソース情報を使用します。領域や特定ノードの設定や順序番号を変更する必要がでてくる場合もあります。

State Poller 設定は通信設定と一致していますか？

通信設定によってネットワークの領域へのプロトコル トラフィックが許可される場合でも、その種類のトラフィックは監視設定で無効にされることがあります。設定が上書きされるかどうかを知る手順は次のとおりです。

1 インベントリ ビューでノードを選択します。

2 **［アクション］> ［モニタリングの設定］** を選択します。

監視設定または通信設定のどちらかによってデバイスへのある種類のトラフィックが無効にされる場合、そのトラフィックは NNMi から送信されません。

通信の調整

認証不合格の削減

検出の間に NNMi があまりにも多くの認証トラップを生成している場合は、NNMi が試行するアクセス資格認定の、より小さいグループで小さい領域または特定のノードを設定します。

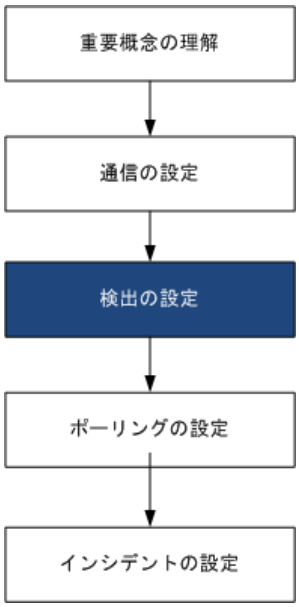
タイムアウトと再試行の調整

NNMi が検出中に SNMP を使ってデバイスに接触を試みるとき、通信設定は NNMi が必要なデバイス情報を収集できるかどうかを調べます。通信設定に正しい SNMP コミュニティ文字列が含まれていない場合、または NNMi が非 SNMP デバイスを検出している場合、NNMi は SNMP タイムアウトと再試行用に設定済みの構成を使います。この場合、タイムアウトの値が大きいか、または再試行の回数が多いと、検出の全般的パフォーマンスに悪影響が及ぶ可能性があります。SNMP/ICMP 要求に低速で応答することが分かっているデバイスがネットワークにある場合は、**［通信の設定］** フォームの **［領域］** タブまたは **［特定ノードの設定］** タブを使ってこれらのデバイスについてのみタイムアウト値と再試行値を微調整することを考えてください。

デフォルト コミュニティ文字列の削減

デフォルト コミュニティ文字列が多数あると、検出パフォーマンスに悪影響が及ぶことがあります。多数のデフォルト コミュニティ文字列を入力する代わりに、**［通信の設定］** フォームの **［領域］** タブまたは **［特定ノードの設定］** タブを使って、ネットワークの特定エリアのコミュニティ文字列設定を微調整します。

NNMi 検出



ネットワーク管理で最も重要な作業の一つは、常に最新のネットワーク トポロジを把握しておくことです。HP Network Node Manager i Software (NNMi) 検出により、トポロジ インベントリにネットワーク内のノードに関する情報が挿入されます。NNMi では、継続的な スパイラル検出によってこのトポロジ情報が維持され、根本原因解析ツールとトラブルシューティング ツールで、インシデントに関する正確な情報を把握できるようになります。

この章では、NNMi 検出を設定するために役立つ情報を記載しています。検出がどのようにして行われるのかと検出の設定方法については、NNMi ヘルプの「*ネットワークの検出*」を参照してください。

NNM 6.x/7.x の使用経験があり、NNMi 9.10 で検出がどのように変わったのかを知りたい方は、相違点の概要について NNMi アップグレード リファレンスの「ネットワーク検出」を参照してください。

この章には、以下のトピックがあります。

- 検出の概念
- 検出の計画
- 検出の設定
- 検出の評価
- 検出の調整

検出の概念

ルーターとスイッチのみを検出する NNMi のデフォルト動作により、ネットワーク管理を最も重要なデバイスに集中させることができます。つまり、最初にネットワークの基幹をターゲットにします。一般に、末端ノード (たとえばパソコンやプリンタ) を管理対象にするのは、それらを重大リソースと見なすのでない限り避けるべきでしょう。たとえば、データベースやアプリケーション サーバーがクリティカルなリソースとして考えられます。

NNMi で検出するデバイスを管理して NNMi トポロジに加えるには、いくつかの方法があります。ネットワークをどのように構成するかや NNMi で何を管理するかによって、検出構成を非常に単純にしたり、極めて複雑にしたり、その間の適当なレベルにできます。

NNMi はデフォルトの検出を何も実行しません。各種のデバイスが NNMi トポロジに存在する前に、検出を設定する必要があります。

検出された各ノード (物理または仮想ホスト) は、NNMi がそのノードを積極的に管理しているかどうかに関係なく、ライセンスの限度までカウントします。所有している NNMi ライセンスの内容は、検出方法にも影響を及ぼします。

ステータス 監視の考慮事項も、選択肢に影響を及ぼします。State Poller は、デフォルトでは NNMi が検出したデバイスに接続したインタフェースしか監視しません。ネットワークのいくつかの領域ではこのデフォルト設定を変更できるため、職責の範囲を超えたデバイスの検出が可能になります。(StatePoller の詳細については、77 ページの「NNMi 状態ポーリング」を参照してください。)

NNMi には、次の 2 つの基本的な検出設定モデルがあります。

- **リストベース検出** - NNMi に、リストのシードによってどのデバイスをデータベースに追加し、監視するかを明示的に指定します。
- **ルールベース検出** - NNMi にネットワークのどの領域とデバイス タイプをデータベースに追加するかを伝え、NNMi に各領域の開始アドレスを指定して、NNMi に定義されたデバイスを検出させます。

リストベース検出とルールベース検出を自由に組み合わせて、NNMi の検出対象を設定できます。初回の検出によってこれらのデバイスが NNMi トポロジに追加され、スパイラル検出ではネットワークが日常的に再検出されるため、トポロジは常に最新の状態が維持されます。

マルチテナントを設定する場合は、ネットワーク検出を開始する前に、テナントを設定してください。

NNMi はデバイス プロファイルから属性を導き出す

NNMi はデバイスを検出する際に、SNMP を使用していくつかの属性を直接収集します。重要な属性の 1 つは MIB II システム オブジェクト ID (`sysObjectID`) です。システム オブジェクト ID から、NNMi はベンダー、デバイス カテゴリ、デバイス ファミリーなどの追加属性を導き出します。

検出中、NNMi は MIB II システムの性能を収集して、データベースのトポロジ部分に格納します。システム性能は、**ノード** フォームに表示されます。ただし、これらの性能は NNMi の他の部分 (つまり、監視設定) では使用されません。NNMi では、デバイス カテゴリ (システム オブジェクト ID のデバイス プロファイルにより) を使用して、デバイスをノード グループに分類します。ノード ビュー表では、**「デバイス カテゴリ」**列に各ノードのデバイス カテゴリが明示されます。

NNMi には、リリース時に入手できた数千のシステム オブジェクト ID のデバイス プロファイルが付属しています。ご使用の環境内にしかないデバイス用にデバイス プロファイルをカスタム設定して、これらのデバイスをカテゴリ、ベンダーなどに対応付けることができます。

検出の計画

以下の領域で決定します。

- 基本的な検出方法を選択する
- 自動検出ルール
- ノード名の解決
- サブネット接続ルール
- 検出シード
- 再検出の間隔
- オブジェクトを検出しない

基本的な検出方法を選択する

完全なリストベース検出を行うのか、完全なルールベース検出を行うのか、それともこの 2 つの方法を組み合わせて使用するのかを決定します。

リストに基づいた検出

リストベース検出では、NNMi で検出する各ノードを (検出シードとして) 明確に指定します。

マルチテナントを設定する場合は、リストベース検出を使用して検出することをお勧めします。

リストベース検出のみを使用することの利点を以下に示します。

- NNMi の管理対象を厳密に管理できます。
- 検出時にデフォルト以外のテナントの仕様をサポートします。
- 設定が最も簡単です。
- 固定的なネットワークに適しています。
- NNMi を初めて使用する場合に適した方法です。自動検出ルールを、徐々に追加していくことができます。

リストベース検出のみを使用することのデメリットを以下に示します。

- NNMi は、ネットワークに新規ノードが追加されても検出しません。
- 検出対象とするノードのリストを指定しなければなりません。

ルールベースの検出

ルールベース検出では、NNMi が検出して NNMi トポロジに入れるネットワークの領域を定義するために 1 つ以上の自動検出ルールを作成します。各々のルールに対して、1 つ以上の検出シードを (シードを明確に指定するか ping スィープを有効にすることにより) 指定する必要があります。それにより NNMi がネットワークを自動的に検出します。

ルールベース検出を使用することの利点を以下に示します。

- 大規模なネットワークに適しています。NNMi は大量の数のデバイスを、最低限の設定項目に基づいて検出できます。

- 頻繁に変わるネットワークに適しています。ネットワークに追加した新しいデバイスは、管理者が介在しなくても検出されます (各デバイスは自動検出ルールの適用範囲内であることが前提)。
- 新規デバイスをタイミングよく管理するためのサービス内容合意書や、許可されていない新規デバイスがあれば注意を与えるためのセキュリティ ガイドラインを順守するために、新しいデバイスがネットワークに追加されると検出されます。

ルールベース検出を使用することのデメリットを以下に示します。

- すぐにライセンス限度に達してしまいます。
- ネットワークの構造によっては、自動検出ルールの調整が複雑になることがあります。
- 自動検出ルールが非常に広範囲で、管理しようしている数よりも多くのデバイスを NNMi が検出する場合は、不要なデバイスを NNMi トポロジから削除できます。ノードの削除には時間がかかる可能性があります。
- すべての非シード ノードは、検出時にデフォルトのテナントを受信します。NNMi マルチテナント方式を使用する場合は、検出後にテナント割り当てを更新する必要があります。

ルールベース検出のみ

自動検出ルール

自動検出ルールの順序

自動検出ルールの**順序**属性の値は、検出範囲に次のように影響します。

- IP アドレス範囲

  デバイスが 2 つの自動検出ルールに該当すると、順序番号が小さい方の自動検出ルールの設定が適用されます。たとえばある自動検出ルールにより IP アドレスの一式が除外されると、それより大きな順序番号の自動検出ルールはこれらのノードを処理せず、そのアドレス範囲内のノードは、検出シードとしてリストされない限り検出されません。
- システム オブジェクト ID の範囲
  - 自動検出ルールに IP アドレス範囲が含まれていない場合は、システム オブジェクト ID の設定が、それより大きな順序番号のすべての自動検出ルールに適用されます。
  - 自動検出ルールに IP アドレス範囲が含まれている場合、システム オブジェクト ID 範囲は自動検出ルール内でのみ適用されます。

デバイスを検出から除外

- 特定のオブジェクト タイプが検出されないようにするには、検出したくないシステム オブジェクト ID を無視する自動検出ルールを、順序番号を小さくして作成します。このルールに IP アドレス範囲を含めないでください。この自動検出ルールに小さい順序番号を付けることで、このルールに一致するオブジェクトを検出プロセスはすぐにとばします。
- IP アドレス範囲またはシステム オブジェクト ID 範囲の**ルールにより無視**設定は、その自動検出ルールのみに影響します。無視される範囲内に含まれるデバイスは、別の自動検出ルールに含めることが可能です。

- **[検出の設定]** フォームの **[除外対象 IP アドレス]** タブでリストされるアドレスは、すべての自動検出ルールに適用されます。これらのアドレスは検出シードとして設定されない限り、NNMi トポロジには追加されません。(検出シードは常に検出されます。)

一部のネットワークでは、Hot Standby Router Protocol (HSRP) や Virtual Router Redundancy Protocol (VRRP) などのルーティング プロトコルを使用して、ルーターに冗長性を持たせています。HSRP を使用するときのように、ルーターがルーター冗長グループ (RRG) で設定されている場合、RRG で設定されているルーターは保護された IP アドレス (1 つがアクティブで、1 つがスタンバイ) を共有します。NNMi は、同じ保護された IP アドレスを使用して設定された複数の RRG の検出および管理をサポートしません。各 RRG には固有の保護された IP アドレスが必要です。

Ping スィープ

ping スィープを使用して、設定した自動検出ルールの IP アドレス範囲内のデバイスを検索することができます。初期検出では、すべてのルールで ping スィープを有効にするとよいでしょう。そうすることで十分な情報が NNMi 検出に提供されるので、検出シードを設定する必要がなくなります。

ping スィープは、16 ビット以下のサブネット (たとえば `10.10.*.*`) で機能します。

ping スィープは特に、ISP ネットワークのように制御が不要な WAN 全体でのデバイスの検出で便利です。

ファイアウォールは ping スィープをネットワークに対する攻撃としてみなすことがよくあり、その場合、ファイアウォールは ping スィープを発信したデバイスからのすべてのトラフィックをブロックすることがあります。

ベストプラクティス　ping スィープは、小さな検出範囲にのみ有効にしてください。

SNMP トラップからの検出ヒント

NNMi 9.01 の時点で、NNMi は受信した SNMP トラップのソース IP アドレスを自動検出ルールに対するヒントとして処理するようになりました。この機能は、WAN 内でデバイスを検出する場合に特に役立ちます。

自動検出ルールの検出シード

自動検出ルールごとに少なくとも 1 つの検出シードを指定してください。検出シードを指定するためのオプションを以下に示します。

- **[検出の設定]** フォームの **[検出シード]** タブでシードを入力します。
- `nnmloadseeds.ovpl` コマンドを使用して、シード ファイルから情報をロードします。
- 少なくとも初回の検出で、ping スィープをルールに対して有効にします。
- SNMP トラップを NNMi 管理サーバーに送信するようにデバイスを設定します。

自動検出ルールのベスト プラクティス

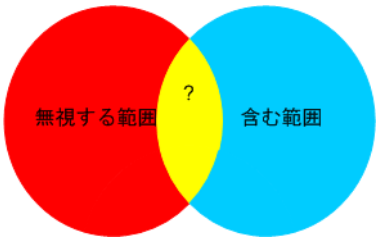
- NNMi はすべての検出対象デバイスを自動的に管理するため、管理したいネットワークの範囲に厳密に一致する IP アドレス範囲を使用してください。
  - 複数の IP アドレス範囲を 1 つの自動検出ルール内で使用して、検出を限定することができます。
  - 自動検出ルールに大きな IP アドレス範囲を追加した後に、そのルール内の検出からいくつかの IP アドレスを除外することができます。
- システム オブジェクト ID 範囲の指定は接頭部分であり、絶対値ではありません。たとえば、範囲 1.3.6.1.4.1.11 は 1.3.6.1.4.1.11.* と同じです。

例

検出ルールの重複

図 1 は、重複する 2 つの検出範囲を示しています。左側の円は、NNMi 検出で無視される IP アドレス範囲またはシステム オブジェクト ID 範囲を表しています。右側の円は、NNMi 検出で検出されて含まれる IP アドレス範囲またはシステム オブジェクト ID 範囲を表しています。重複している領域は、これらの自動検出ルールの順序に応じて検出に含まれるか無視されます。

図 1　　重複している検出範囲



デバイス タイプ検出を制限する

ネットワーク内のプリンタ以外のすべての HP デバイスを検出するには、HP エンタープライズ システム オブジェクト ID (1.3.6.1.4.1.11) を含む範囲を持つ 1 つの自動検出ルールを作成します。この自動検出ルールで、HP プリンタ (1.3.6.1.4.1.11.2.3 9) のシステム オブジェクト ID を無視する 2 番目の範囲を作成します。IP アドレス範囲を未設定のままにしてください。

ノード名の解決

デフォルトでは、NNMi はノードを次の順序で識別しようとします。

1. 短い DNS 名
2. 短い sysName
3. IP アドレス

以下のシナリオでは、ノード名解決のデフォルト順序を変更したほうがよい場合を説明しています。

- 組織が DNS 設定の更新を外部者にまかせている場合、ネットワークに新しいデバイスが追加されるごとにその sysName を定義するポリシーを設定できます。この場合、sysName の選択をノード名解決の最初の選択肢として設定して、新しいデバイスがネットワークに導入されるとすぐに NNMi が検出できるようにします。(sysName を、そのデバイスを使用している間は維持します。)
- 組織が管理対象デバイスの sysName を設定も維持もしない場合、sysName をノード名解決の 3 番目の選択肢として選択します。

ベストプラクティス　DNS 完全名または DNS 短縮名を基本的な命名方法として使用している場合、NNMi 管理サーバーからすべての管理対象デバイスへの順方向と逆方向の DNS 解決があることを確認してください。

DNS 完全名が命名方法の場合、トポロジ マップ上のラベルを長くできます。

ベストプラクティス　NNMi では最小のループバック アドレスを Cisco デバイスの管理アドレスとして選択されるため、各 Cisco デバイスの最小のループバック アドレス上に DNS 解決を配置してください。(NNMi 8.0x では、最大のループバック アドレスが管理アドレスとして選択されます。)

サブネット接続ルール

リストベース検出のみ　リストベース検出では、NNMi はサブネット接続ルールを使用して WAN 上の接続を検出します。NNMi は予測される接続の各末端で検出したデバイスのサブネット メンバーシップを評価し (IP アドレスとサブネット接頭部を調べて)、サブネット接続ルールで一致があるか調べます。

ルールベース検出のみ　自動検出ルールが有効で NNMi が /28 と /31 の間のサブネット接頭部で設定されたデバイスを見つけると：

1. NNMi は適用可能なサブネット接続ルールについて調べます。
2. 一致が見つかると、NNMi はサブネット内の有効な各アドレスをヒントとして使用して、そのアドレスでの検出を試みます。

ベストプラクティス　デフォルトの接続ルールを使用してください。問題がある場合のみそれらを変更してください。

検出シード

検出シードとして使用するデバイスをリストします。

ベストプラクティス　優先管理 IP アドレスを選択する NNMi のルールの 1 つによって、最初に検出した IP アドレスを管理アドレスとして使用することが指定されます。優先 IP アドレスをシード アドレスとして設定することにより、NNMi に影響を与えることができます。

ベストプラクティス　Cisco デバイスの場合、ループバック アドレスを検出シードとして使用してください。ループバック アドレスが、デバイス上の他のアドレスより確実に到達可能であるためです。DNS が、デバイス ホスト名からループバック アドレスを解明するように正しく設定されていることを確認します。

リストベース検出のみ　リストベース検出の場合、NNMi の管理対象にするすべてのデバイスをリストします。このリストを、資産管理ソフトウェアから、または他のツールからエクスポートすることが可能です。

NNMi はこのリストにデバイスを自動的に追加することがないため、責任を負っているデバイスだけがリストに追加含まれるようにするか、監視 / ステータス計算に影響を及ぼすデバイスだけがリストに含まれるようにしてください。

ルールベース検出のみ

ルールベース検出の場合、検出シードはオプションです。

- ping スィープが自動検出ルールに対して有効の場合、そのルールのシードを指定する必要はありません。
- ping スィープが無効な各自動検出ルールで、ルールごとに少なくとも 1 つのシードを確認してください。ルールに IP アドレス範囲が複数含まれる場合、ルーターは WAN リンク全体の ARP エントリを維持しないため、それぞれのルーティング可能範囲でシードが必要になります。

ベストプラクティス

ルールベース検出を最も完璧なものにするためには、スイッチではなくルーターを検出シードとして使用してください。一般にルーターはスイッチより大きな ARP キャッシュを持っているためです。検出したいネットワークにコア ルーターが接続されていれば、検出シードとしては最適な選択肢になります。

再検出の間隔

NNMi は、データベース内の各デバイスの設定情報を、設定された再検出間隔に従って再チェックします。さらに、NNMi は自動検出ルールの対象となる各ルーターから ARP キャッシュを収集して、ネットワーク上に新しいノードがあるか調べます。

デバイスの通信関連の設定に、インタフェースの番号変更のような変更があると、NNMi は自動的に、そのデバイスとその隣接デバイスに関するデータを更新します。

次のような変更では自動再検出は行われません。デバイスは設定された再検出間隔に基づいて更新されます。

- ノード内の変更 (たとえば、ファームウェア アップグレードまたは接点システム)。
- ネットワークに追加された新しいノード。

ネットワーク内の変更のレベルに合った再検出間隔を選択します。非常に動的なネットワークでは、最低 24 時間の間隔を使用するとよいでしょう。これより安定したネットワークでは、その期間を広げることができます。

オブジェクトを検出しない

NNMi では、NNMi が特定のオブジェクトを無視するように設定する 3 つの方法があります。

- **[通信の設定]** フォームで、ICMP 通信または SNMP 通信あるいはその両方を、グローバル レベル、通信領域レベル、または特定のホスト名または IP アドレスのレベルの異なるレベルでオフにできます。これらのプロトコルのいずれかまたは両方を無効にした場合の影響の詳細については、51 ページの「ポーリング プロトコル」を参照してください。
- **[検出の設定]** フォームで、NNMi に特定の IP アドレスや SNMP システム オブジェクト ID からヒントを収集しないように指示する自動検出ルールを設定できます。この基準に一致するノードはマップとデータベース上で存在し続けますが、スパイラル検出はこれらの IP アドレスまたはオブジェクト タイプを超える隣接デバイスまで行われません。
- **[検出の設定]** フォームで、特定の IP アドレス範囲または特定の IP アドレス、あるいはその両方をデータベースから除外するよう NNMi に指示する自動検出ルールを設定できます。スパイラル検出では、あらゆるノードのアドレス リストでこれらのアドレスを表示したり、デバイス間に接続を確立するときこれらのアドレスを使用することがないので、NNMi がこれらのアドレスの使用状況を監視することはありません。

NNMi による仮想 IP アドレスの監視

NNMi は、仮想 IP アドレスを共有するクラスタ化されたサーバーなどのデバイスを検出および監視します。クラスタが新しいアクティブ ノードにフェイルオーバーすると、NNMi はその仮想 IP アドレスを新しいアクティブ ノードに関連付けます。フェイルオーバーしてから NNMi が変更を検出するまでにしばらく時間がかかるため、この関連付けはすぐには行われません。

特定の状況に合わせて NNMi を設定するため、いくつかのアクションを実行できます。

NNMi で仮想 IP アドレスを監視する場合は、*以下のオプションのいずれか 1 つだけを使用してください。*

- オプション 1: このオプションの場合、NNMi は N+1 個の非 SNMP デバイスを管理します。ここで N は、非仮想 IP アドレスによって検出されたクラスタに属するメンバーの数です。NNMi は、さらにもう 1 つの (+1) 非 SNMP ノードを検出し、仮想 IP アドレスを使用して設定します。

  NNMi が仮想 IP アドレスを検出する動作を停止しないでください。この方法を使用することにより NNMi は、仮想 IP アドレスと、この仮想 IP アドレスを使用するように設定されたデバイスのネットワーク インタフェース カード (NIC) に関連付けられている物理 IP アドレスを検出します。NNMi は、各デバイスを別々の非 SNMP ノードとして検出および監視します。

- オプション 2: デバイスの物理 IP アドレスをクラスタ化されたサーバーの優先される管理アドレスとして使用するように NNMi を設定します。この方法の詳細については、NNMi のヘルプの「*特定ノードの設定フォーム (通信設定)*」のトピックを参照してください。

  NNMi は、アクティブ ノードから新しいアクティブ ノードへの仮想 IP アドレスの移行をすぐには認識しない場合があります。NNMi は、クラスタ内の現在のアクティブ ノードとは別のノードを使用して仮想 IP アドレスのステータスを表示することがあります。

NNMi で仮想 IP アドレスを監視しない場合は、NNMi コンソールを使用して以下の手順を実行します。

1. **[設定]** ワークスペースの **[検出の設定]** をクリックします。
2. **[除外対象 IP アドレス]** タブをクリックします。
3. 仮想 IP アドレスまたはアドレス範囲を、検出対象から除外するアドレスの一覧に追加します。
4. 作業内容を保存します。

検出の設定

ここでは、設定のヒントを一覧にし、いくつかの設定例について説明します。このセクションの情報を読んだ後で、特定の手順の NNMi ヘルプの「*検出の設定*」を参照してください。

NNMi は、**[検出シード]** フォームを**保存して閉じる**とすぐにシードから検出を開始するので、シードを設定する前に次のことを必ず行ってください。

- すべての通信設定を完了する。
- すべての自動検出ルール (ある場合) を完了する。
- サブネット接続ルールを設定する。
- 名前解決設定を設定する。
- コンソールまでさかのぼって **[保存して閉じる]** を行う。

大きな設定変更を行う前には、既存の設定のコピーを保存しておくことをお勧めします。詳細については、40 ページの「ベストプラクティス : 既存の設定を保存」を参照してください。

自動検出ルールを設定する場合のヒント

- 新しい自動検出ルールを定義するときは、それぞれの設定を慎重に確認してください。新しいルールでは、自動検出はデフォルトで有効になっており、IP アドレス範囲はデフォルトで含まれており、システム オブジェクト ID 範囲はデフォルトで*無視*されます。

シードを設定する場合のヒント

- 検出対象ノードがリストされたファイルがすでにある場合は、この情報をシード ファイルとして書式設定して、`nnmloadseeds.ovpl` コマンドを使用してそのノード リストを NNMi にインポートします。
- シード ファイルで、管理アドレスとして NNMi が選択する IP アドレスに影響を与える手段として IP アドレスを指定します。(ホスト名を使用すると、DNS は IP アドレスを各ノードに提供します。)
- シード ファイルのエントリとして適切な書式を以下に示します。

  ```
  IP_address # node name
  IP_address2, <tenant_UUID_or_tenant_name> # node name
  ```

  以下の書式は、NNMi と人間の両方が容易に理解できます。
- 保守目的のため、使用するシード ファイルは 1 つだけにすることをお勧めします。ノードを必要に応じて追加して、`nnmloadseeds.ovpl` コマンドを再度実行します。NNMi は新しいノードを検出しますが、既存のノードは再判定しません。
- ノードをシード ファイルから削除しても、NNMi トポロジからは削除されません。ノードは直接 NNMi コンソール で削除してください。
- ノードをマップやインベントリ ビューから削除しても、シードは削除されません。
- NNMi でノードを再検出したい場合は、そのノードをマップまたはインベントリ ビューから、そしてNNMi コンソール の **[検出の設定]** フォームの **[検出シード]** タブから削除してから、そのノードを NNMi コンソール で入力するか、`nnmloadseeds.ovpl` コマンドを実行します。

ルールベース検出のみ

- 検出ルールを、そのルールのシードを指定する*前に*、完全に設定します。つまり、**[検出の設定]** フォームで **[保存して閉じる]** をクリックします。(**[検出シード]** タブは、つながっているように見えますが、分離したフォームであり、データベース モデルの **[検出の設定]** フォームの一部ではありません。結果として、**[検出シード]** タブについての情報を保存すると、NNMi によってシード設定は直ちに更新されます。)

検出の評価

ここでは、検出の進行状況と成功したかどうかを判定する方法を記載しています。

初期検出の進行状況をたどる

NNMi 検出は、動的かつ継続的です。完了することはないため、「検出完了」のメッセージが表示されることはありません。初回の検出と接続には、多少の時間がかかります。初期検出の進行状況を測定する方法を以下に示します。

- **[システム情報]** ウィンドウの **[データベース]** タブで、ノード カウントが予想レベルに達して一定になるのを監視します。このウィンドウは自動的に更新されません。初期検出時に、**[システム情報]** ウィンドウを複数回開きます。
- **[検出の設定]** フォームで、**[検出シード]** タブを見てください。このタブを、すべてのシードに「ノードが作成されました」結果が表示されるまで更新してください。「ノードが作成されました」結果は、デバイスがトポロジ データベースに追加されたことを示します。この結果は、NNMi がデバイスからすべての情報を収集してデバイスの接続を処理したことを示すものでは*ありません*。
- 代表ノードの **[ノード]** フォームを開きます。**[検出状態]** フィールドが `Discovery Completed` に移行するときには、NNMi はノードの基本特性、ノードの ARP キャッシュ、隣接検出プロトコル (該当する場合) の収集を済ませています。この状態は、NNMi がデバイスの接続解析を完了したことを示す*ものではありません*。
- **[ノード]** インベントリ ビューで、ネットワークの様々な領域のキー デバイスが存在していることを確認します。
- 代表ノードの **[レイヤ 2 近隣接続ビュー]** を開き、その領域の接続解析が完了したかどうかを確認します。
- **[レイヤ 2 接続]** および **[VLAN]** インベントリ ビューを調べて、レイヤ 2 処理の進行状況を測定します。

すべてのシードが検出されているか？

1. **[検出の設定]** フォームを開きます。
2. **[検出シード]** タブで、ノードのリストを **[検出シードの結果]** 列でソートします。ノードがエラー状態の場合は、以下について検討してください。
   - ノードに到達できなかったか DNS 名が解決されなかったために検出が失敗した - これらのタイプの失敗に対しては、ノードへのネットワーク接続を確認して、DNS 名解決が正しいかどうかを調べてください。DNS 問題に対処するには、IP アドレスを使用してノードをシードするか、ホスト名を `hostnolookup.conf` ファイルに加えます。

- ライセンス ノード数超過 - この状況は、すでに検出されたデバイス数がライセンス限度に達したときに発生します。検出したノードをいくつか削除するか、ノード パック ライセンスを追加購入します。
- ノードが検出されたが SNMP 応答がない - SNMP 通信の問題は、シードされたデバイスだけでなく自動検出によって検出されたデバイスにも発生します。詳細については、56 ページの「通信の評価」を参照してください。

すべてのノードには有効なデバイス プロファイルがあるか？

1 **[ノード]** インベントリ ビューを開きます。

2 **[デバイス プロファイル]** 列を、「デバイス プロファイルなし」文字列が含まれるようにフィルタリングします。

3 ノードが検出されてもデバイス プロファイルがない場合は、**[設定] > [デバイスのプロファイル]** で新規デバイス プロファイルを追加してから、ノード上で設定ポーリングを実行してそのデータを更新します。

すべてのノードが正しく検出されたか？

検出の問題を回避するには、管理ドメイン内の他のドメインには表示されない固有の IP アドレスを使用するノードのみを NNMi で管理するようにします。たとえば、ノードが突然消えたり、データベース内の別のノードとマージされたりし、そのノードがルーター冗長グループ (RRG) の一部になっている場合には、特別な要件があります。RRG に参加しているルーターを管理するには、ルーターの管理アドレスとして固有の IP アドレス (保護されたアドレス以外) を使用する必要があり、そのアドレスで SNMP を有効にする必要があります。NNMi は、保護された IP アドレスを管理アドレスとして使用しようとすると、ルーターを適切に管理できません。

[ノード] インベントリ ビューでデータを調べます。管理アドレスがないノードがある場合は、これらのノードの通信設定を 57 ページの「すべてのノードが SNMP 用に設定されましたか？」の説明にしたがって確認します。

予想したノードが **[ノード]** インベントリ ビューにない場合は、以下について確認します。

- 見つからなかったノードごとに、検出プロトコル (たとえば CDP) が正しく設定されていることを確認します。
- 見つからないノードが WAN 上にある場合、そのノードを含む自動検出ルールの ping スィープを有効にします。

リストベース検出のみ

自動検出ルール

予期しない検出結果に遭遇した場合は、自動検出ルールを再検討します。

NNMi 検出でアドレス ヒントが見つかる場合は、最初の一致ルールを使用してノードを作成するかどうかを判定しています。一致するルールがない場合、NNMi 検出はヒントを廃棄します。自動検出ルールの順序番号によって、自動検出ルール設定が適用される順序が決まります。

それぞれの自動検出ルールで、以下の設定を確認してください。

- **[含まれているノードの検出]** を有効にし、自動検出がルールに実行されるようにする必要があります。
- 以下の設定が、検出したいノードのタイプに対して正しいかどうかを確認します。
  - **SNMP デバイスの検出**
  - **非 SNMP デバイスの検出**

  デフォルトではルーターとスイッチのみが検出されて、SNMP 以外のノードは検出*されない*ことを忘れないでください。ご使用の環境を考慮せずにこれらの設定を有効にすると、NNMi が予期した以上のノードを検出してしまう可能性があります。

IP アドレス範囲

検出ヒントの IP アドレスは、IP アドレス範囲リスト内の **[ルールに含める]** エントリに一致する必要があります。含まれる IP アドレス範囲が自動検出ルールの中にない場合、すべてのアドレス ヒントが一致とみなされます。(この場合は、68 ページの「自動検出ルールを設定する場合のヒント」を参照してください。) さらに、ヒントは **「ルールにより無視」** とマークされたエントリと一致*してはなりません*。すべてのチェックが正常に一致すると、このルールの設定がヒントの処理に使用されます。

- 予想したデバイスのいくつかが検出されない場合、設定した IP 範囲を確認してそのデバイスの IP アドレスが範囲の中に含まれていて小さい順序番号のルールで無視されないようにしてください。
- 必要以上のデバイスが検出されている場合は、含む範囲を変更するか、検出したくないデバイスの IP アドレスの無視される範囲を追加してください。また、**[SNMP デバイスの検出]** も有効かどうかを確認します。

システム オブジェクト ID の範囲

検出ヒントのシステム オブジェクト ID (OID) は、システム オブジェクト ID 範囲リストの中の **[ルールに含める]** エントリと一致する必要があります。含まれるシステム オブジェクト ID 範囲が自動検出ルールの中にない場合、すべてのオブジェクト ID が一致とみなされます。さらに、OID は **「ルールにより無視」** とマークされたエントリと一致してはなりません。すべてのチェックが正常に一致すると、このルールの設定がヒントの処理に使用されます。

- システム オブジェクト ID 範囲を使用して、自動検出を拡大してデフォルトのルーターおよびスイッチ以外も含めるか、特定のルーターおよびスイッチを除外します。
- 各ノードは、検出されてトポロジ データベースに追加される前に指定された IP アドレス範囲とシステム オブジェクト ID 範囲の両方と一致する必要があります。

すべての接続と VLAN は正しいか？

NNMi はレイヤ 2 接続と VLAN を、デバイスがトポロジに追加された後の別個のステップとして作成します。NNMi に接続と VLAN を評価する前の初期検出として十分な時間を考慮してください。

レイヤー 2 接続の評価

レイヤ 2 の接続を評価するには、対象とする各ネットワーク領域のノード グループを作成し、続いてそのノード グループのトポロジ マップを表示します。(**[ノード グループ]** インベントリで、ノード グループを選択して、**[アクション]** > **[ノード グループ マップ]** をクリックします。) このマップで他のノードに接続していないノードを探します。

VLAN を評価するには、**[VLAN]** インベントリ ビューから、各々の **[VLAN]** フォームを開いて、その VLAN のポートのリストを調べます。

NNMi 検出と重複 MAC アドレス

NNMi は、検出の実行中、ネットワーク デバイス間の通信パスを判断するため、ネットワーク内の Ethernet スイッチから転送データベース (FDB) テーブルを読み取ります。NNMi は、これらの FDB テーブルで、検出されたノードに関する情報を検索します。NNMi 管理サーバーは、重複するメディア アクセス制御 (MAC) アドレスへの FDB 参照を検出すると、以下の処理を行います。

- 検出された 2 つ以上のノードに同じ MAC アドレスに関連付けられたインタフェースが含まれる場合、NNMi は、FDB にあるそれらの重複 MAC アドレスについて記録されている通信パスを無視します。これにより、それらの重複 MAC アドレスを含むネットワーク領域の NNMi マップで、接続が失われる場合があります。

  NNMi Advanced - グローバル ネットワーク管理機能 : 2 つの NNMi 管理サーバーが、同じ MAC アドレスに関連付けられている 1 つのインタフェースを含むノードを検出すると、リージョナル NNMi 管理サーバーのマップで認識される接続がグローバル NNMi 管理サーバーのマップでは失われる可能性があります。

- 1 つのノードに同じ MAC アドレスを持つ複数のインタフェースが含まれる場合、NNMi は、それらのインタフェースについてのすべての通信パス情報を収集し、NNMi マップにその情報を表示します。

デバイスを再検出する

1 デバイスの設定ポーリングを実行します。

2 デバイスを削除します。

そのデバイスがシードの場合、シードを削除し、それからシードを再度追加します。

検出の調整

標準的な検出が行われるようにするためには、検出設定を調整して重大なデバイスと重要なデバイスのみが検出されるようにしてください。

- IP アドレス範囲またはシステム オブジェクト ID、あるいはその両方でフィルタリングします。
- 非 SNMP デバイスと SNMP デバイス (スイッチでもルーターでもないデバイス) の検出を制限します。

コマンドラインで NNMi データベースから 1 つ以上のノードを削除するには、`nnmnodedelete.ovpl` コマンドを使用します。このコマンドにより、NNMi データベースからノードが削除されますが、シード定義は削除されません。

コマンドラインで NNMi データベースから 1 つ以上のシード定義を削除するには、`nnmseeddelete.ovpl` コマンドを使用します。

検出プロトコル コレクションまたは `VLAN` のインデックス付けを無効にすることによって修復できる、特別な検出状況もあります。詳細については、366 ページの「特定ノードの検出プロトコルの使用を抑える」または 369 ページの「大規模スイッチの VLAN インデックス付けの使用を抑制する」を参照してください。

検出ログ ファイル

nnm.?.0.log ファイル内で、文字列 com.hp.ov.nms.disco で始まるクラスの Exception というキーワードを含むメッセージを探します。ログ ファイルの詳細については、373 ページの「NNMi ロギング」を参照してください。

無番号インタフェース

NNMi 9.10 パッチ 2 より前の NNMi は、xDP を有効にしない限り、無番号インタフェースのレイヤー 2 接続を検出しませんでした。NNMi 9.10 パッチ 2 では、無番号インタフェース検出と監視ソリューションを提供しており、デフォルトの MIB-II ipRoutingTable と ipCidrRoutingTable を使用するデバイスをサポートします。

NNMi 9.10 は、このセクションで説明するソリューションを使用して、IPv4 無番号インタフェースとそれに関連付けられたレイヤー 2 接続を検出および監視します。

このセクションで説明するソリューションは、グローバル ネットワーク管理設定で以下のように機能します。

- リモート NNMi 管理サーバーでは通常どおり動作します。
- グローバル NNMi 管理サーバーの場合は、そのサーバーで管理されるノードの場合にのみ動作します。
- リモート NNMi 管理サーバーによって管理されるノードのグローバル NNMi 管理サーバーでは動作しません。

無番号インタフェース機能の有効化

1. 無番号インタフェースを含むデバイスを含むノード グループを作成します。デバイス ID を含む 1 つのノード グループを作成するか、デバイス ID を含む複数の子ノード グループを代表する親ノード グループを作成します。
2. 以下のファイルを作成します。

   Windows: %NNM_DATA%¥shared¥nnm¥conf¥disco¥UnnumberedNodeGroup.conf

   UNIX: $NNM_DATA/shared/nnm/conf/disco/UnnumberedNodeGroup.conf
3. 単一のノード グループ名をこのファイルに追加します。繰り返しますが、このファイルには、デバイス ID を含む 1 つのノード グループの名前を含める必要があります。あるいは、デバイス ID を含む複数の子ノード グループを代表する親ノード グループの名前にすることもできます。

   ```
   # This is the name of an node group containing devices with
   unnumbered interfaces.
   Unnumbered Node Group
   ```

   上の例では、Unnumbered Node Group という名前のノード グループが NNMi 内に存在しています。# 文字を先頭に付けて、コメント情報を別の行で追加します。
4. *オプション ステップ*: 以下のファイルを作成します。

   Windows: %NNM_DATA%¥shared¥nnm¥conf¥disco¥UnnumberedSubnets.conf

   UNIX: $NNM_DATA/shared/nnm/conf/disco/UnnumberedSubnets.conf

5 *オプション ステップ*: このファイルに情報を追加して、NNMi で検出する必要がある特定のルーティング アドレス範囲を示します。複数行の IPv4 CIDR サブネット エントリをランダムな順序でこのファイルに追加できます。

このファイルを作成および設定しない場合、NNMi は、MIB-II ルーティング テーブル全部が、設定されたノード グループのノードに向かって進むようにします。NNMi は、`UnnumberedSubnets.conf` ファイルを使用して、指定されたサブネット宛先の範囲に収まるルートのみから MIB データを要求します。このファイルを使用し、デバイスでの検出トラフィックの量とパフォーマンスへの影響を軽減することは、優れた手法の 1 つです。

以下に、`UnnumberedSubnets.conf` ファイルに追加するエントリの例をいくつか示します。

```
10.1.5.0/18   #This entry filters the following routes: 10.1.0-63.

15.2.126.0/16 #This entry filters the following routes: 15.2.*.*

192.168.1.0/24 #This entry filters the following routes:
192.168.1.0-255
```

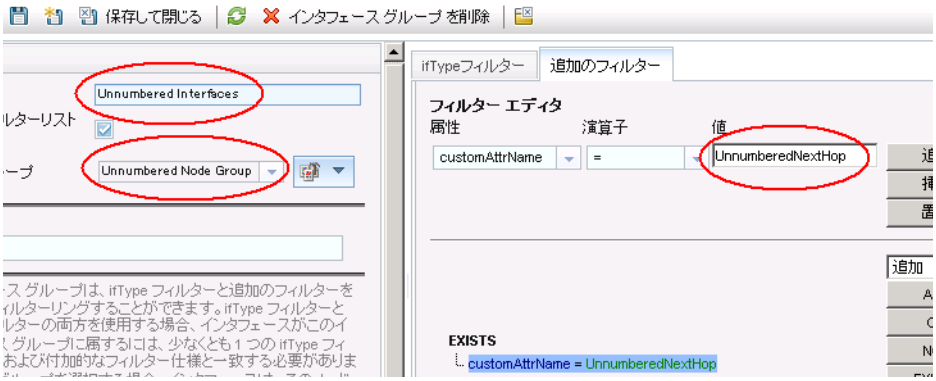
6 NNMi 管理サーバーを再起動します。

a NNMi 管理サーバーで **`ovstop`** コマンドを実行します。

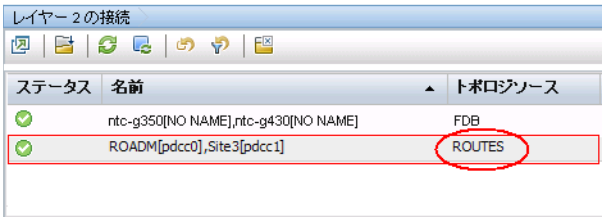
b NNMi 管理サーバーで **`ovstart`** コマンドを実行します。

7 NNMi が次の検出サイクルを完了するまで待ちます。

8 無番号インタフェースをすべて検出するには、`UnnumberedNextHop` という名前のカスタム属性を持つインタフェースを含める新しいインタフェース グループを設定します。



9 このソリューションによって作成されたレイヤー 2 接続を表示するには、**[レイヤー 2 接続]** ビューに移動し、`ROUTES` からソースを探します。



無番号インタフェース機能の無効化

無番号インタフェース機能を無効にする場合は、以下の手順を実行します。

1 以下のファイルを削除します。

Windows: `%NNM_DATA%¥shared¥nnm¥conf¥disco¥UnnumberedNodeGroup.conf`

UNIX: `$NNM_DATA/shared/nnm/conf/disco/UnnumberedNodeGroup.conf`

2 以下のファイルが存在する場合は削除します。

   Windows: `%NNM_DATA%¥shared¥nnm¥conf¥disco¥UnnumberedSubnets.conf`

   UNIX: `$NNM_DATA/shared/nnm/conf/disco/UnnumberedSubnets.conf`

3 NNMi 管理サーバーを再起動します。

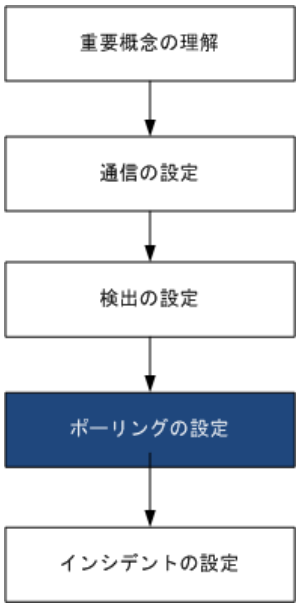
   a NNMi 管理サーバーで **ovstop** コマンドを実行します。

   b NNMi 管理サーバーで **ovstart** コマンドを実行します。

4 NNMi が次の検出サイクルを完了するまで待ちます。

詳細については、`UnnumberedNodeGroup.conf` および `UnnumberedNodeGroup.conf` のリファレンスページ、または UNIX マンページを参照してください。

NNMi 状態ポーリング



この章では、HP Network Node Manager i Software (NNMi) StatePoller サービスを設定し、ネットワーク監視を拡張および微調整するのに役立つ情報を示します。この章は、NNMi ヘルプの情報を補充するものです。監視動作方法の紹介、および監視設定方法の詳細は、NNMi ヘルプの「*ネットワークの稼動状態の監視*」を参照してください。

NNM 6.x/7.x で作業した経験があり、NNMi 9.10 で監視がどのように変更されたかを知りたい場合は、『NNMi アップグレード リファレンス』の「ステータス監視」に記載されている相違点の概要を参照してください。

この章には、以下のトピックがあります。

- 状態ポーリングの概念
- 状態ポーリングの計画を作成
- 状態ポーリングの設定
- 状態ポーリングの評価
- 状態ポーリングの調整

状態ポーリングの概念

この項では、State Poller がポーリング グループの評価に使う順序など、ネットワーク 監視の簡単な概要を示します。この項を読んだ後、さらに詳細な情報については 78 ページの「状態ポーリングの計画を作成」に進んでください。

ネットワーク検出と同じように、ネットワークでクリティカルであるか、または最も重要なデバイスのネットワーク 監視に関心を集中する必要があります。NNMi では、トポロジ データベースでのみデバイスをポーリングできます。NNMi がどのネットワーク デバイスを監視するか、使用するポーリングの種類、およびポーリングする間隔を制御できます。

[監視の設定] フォームのインタフェースとノードの設定を使って、デバイスのステータス ポーリングを高度化し、さまざまなクラス、インタフェースの種類、およびノードの種類についてポーリングの種類と間隔を設定することができます。

State Poller のデータ収集が ICMP (ping) 応答を基礎にするように、または SNMP データを基礎にするように設定できます。NNMi は、ユーザーが有効にするデータ収集の種類から、実際の MIB オブジェクトへの内部的なマップを自動処理し、設定を大幅に簡単にします。

ポーリング設定の計画を作成するときは、State Poller サービス用にインタフェース グループとノード グループをセットアップする方法を注意深く考える必要があります。グループという概念が初めての場合は、その概要について 41 ページの「ノード グループおよびインタフェース グループ」と 45 ページの「ノード / インタフェース / アドレス階層」を参照してください。

評価の順序

インタフェースまたはノードは複数のグループに属することがあるので、StatePoller は、明確に定義された評価順序で、設定されたポーリング間隔およびポーリング種類を適用します。検出されたトポロジ内の各オブジェクトについて：

1. オブジェクトがインタフェースの場合、State Poller は基準を満たすインタフェース グループを探します。グループは最も小さい順序番号から最も大きい順序番号へという順序で評価されます。最初に一致するグループが使われ、その時点で評価は停止します。
2. オブジェクトを把握したインタフェース グループがない場合、グループは最も小さい順序番号から最も大きい順序番号への順序で評価されます。最初に一致するグループが使われ、その時点で評価は停止します。含まれているインタフェースのうち、独自の特性に関してインタフェース グループの基準を満たしていないものは、ホストであるノードからポーリング設定を継承します。
3. 検出されたものの、ノードまたはインタフェースの設定定義に含まれないデバイスは、グローバルな監視設定 (**[監視の設定]** フォームの **[デフォルト設定]** タブ) によって監視動作が確定されます。

状態ポーリングの計画を作成

この項では、ポーリング設定チェックリストなど、State Poller 設定の計画作成について説明します。監視の計画作成に便利な詳細情報によって、ポーリング グループの作成法が決まり、ポーリング プロセスの間にどの種類のデータを取得する必要があるかが決まります。

ポーリング チェックリスト

次のチェックリストを使って、State Poller 設定の計画を作成できます。

- ☐ NNMi で何を監視できますか？
- ☐ オブジェクトの種類、場所、相対的重要性、その他の基準に基づいて、監視対象は論理的にどのように分類できますか？
- ☐ NNMi は、各グループをどのくらいの頻度で監視する必要がありますか？
- ☐ 監視されるアイテムの情報を取得するために、何のデータを収集する必要がありますか？以下のものが含まれることがあります。
  - — ICMP (ping) 応答
  - — SNMP 障害データ
  - — 1 つ以上の NNM Performance iSPI に対応するライセンスが 1 つある場合は、SNMP パフォーマンス データ
  - — 追加の SNMP コンポーネント稼働状態データ

ポーリング設定の例

ポーリング設定プロセスの理解を深めるために、次の例について考えます。ネットワークに ProximiT の最新のプロキシ サーバーが含まれていると仮定します。これらのデバイスに到達できることを確認する必要がありますが、プロキシ サーバーの SNMP 監視は要求しません。

1 NNMi で何を監視できますか？

監視できるのは検出されたもののみであるため、自動検出ルールを設定して、NNMi のデータベースに自分の ProximiT プロキシ サーバーがあることを確認します。検出の設定の詳細は、59 ページの「NNMi 検出」を参照してください。

2 監視対象は論理的にどのように分類できますか？

複数の ProximiT プロキシ サーバーを 1 つのグループにまとめ、同じ監視設定を適用することは理にかなっています。デバイスのインタフェース (SNMP) 監視を行っているのですから、インタフェース グループは必要ありません。

このノード グループを使って、ビューをフィルタし、プロキシ サーバーのステータスをグループとしてチェックし、グループをサービス外 にしてファームウェアを更新することもできます。

3 NNMi は、各グループをどのくらいの頻度で監視する必要がありますか？

サービス レベル契約条項で、プロキシ サーバーについて 5 分間のポーリング間隔で十分です。

4 どのデータを収集する必要があるでしょうか？

監視設定が他のグループと異なるのは次の点です。ProximiT proxy サーバーの例として、ICMP 障害の監視を有効にし、SNMP 障害およびポーリングの監視を無効にします。グループについての SNMP 障害監視がない場合、コンポーネント稼働状態監視は適用されません。

これらの設定選択肢に関する計画作成情報の詳細は、以下のトピックを参照してください。

— 79 ページの「NNMi で何を監視できますか？」

— 81 ページの「グループの計画作成」

— 83 ページの「ポーリング間隔の計画作成」

— 84 ページの「どのデータを収集するかの決定」

NNMi で何を監視できますか？

デフォルトで、NNMi State Poller は SNMP ポーリングを使って以下を監視します。

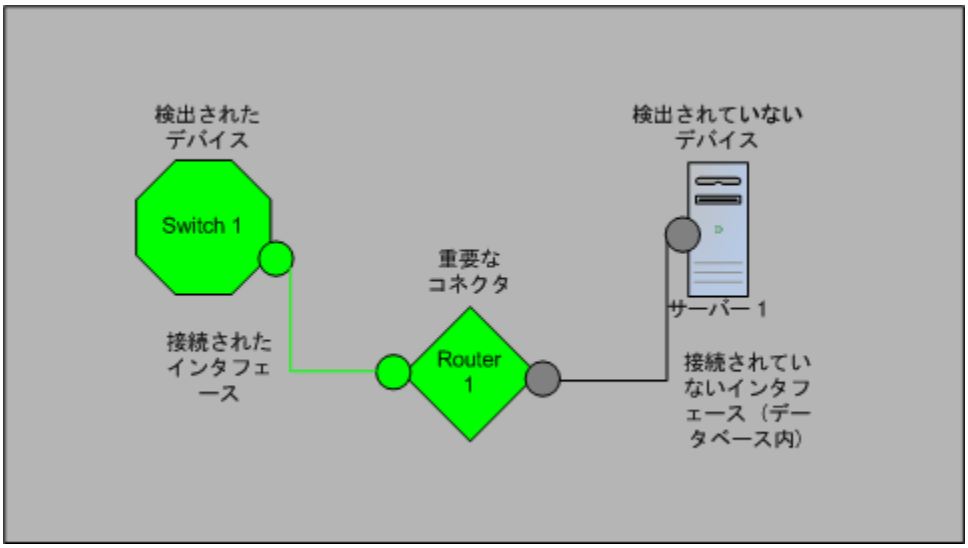
- NNMi 検出対象デバイス上で既知の別のインタフェースに接続されたインタフェース。
- IP アドレスをホストするルーター インタフェース。

ほとんどの場合、インタフェースに接続されたポーリングによってのみ、十分に正確な根本原因分析ができます。監視対象インタフェースのセットを拡張すると、ポーリングのパフォーマンスに影響が及ぶ可能性があります。

監視の拡張　監視を拡張して、以下が含まれるようにできます。

- 未接続インタフェース。デフォルトでは、NNMi が監視する未接続インタフェースは IP アドレスのあるもののみであり、**ルーター** ノード グループに含まれます。

  NNMi は、次のように、NNMi が検出した別のデバイスに接続されていないインタフェースとして未接続インタフェースを定義します。



- ルーター インタフェースのように、IP アドレスのあるインタフェース。
- SNMP をサポートしないデバイス用の ICMP ポーリング。デフォルトで、ICMP ポーリングは、**非 SNMP デバイス**ノード グループについて有効です。

監視されないノードへのインタフェース

直接管理していないデバイスに接続されているインタフェースのステータスを知る必要があることがあります。たとえば、アプリケーションまたはインターネット サーバーへの接続が確立されているかどうか知る必要があるものの、そのサーバーのメンテナンスは担当していないことがあります。検出ルールにそのサーバーを組み入れていないと、NNMi はそのサーバーに面するインタフェースを未接続と見なします。

監視されていないノードに接続する重要なインタフェースのステータスを監視する方法には次の 2 つがあります。

- 監視されていないノードの検出。

  監視されていないノードを NNMi トポロジに追加するとき、NNMi は、トポロジの残りの部分にノードを接続しているインタフェースを接続済みと見なします。この場合、NNMi は、監視設定に従ってこれらのインタフェースをポーリングできます。NNMi はノードを管理対象として検出します。NNMi に監視させたくない、管理されていないノード。

  検出された各ノードは、NNMi が積極的にそのノードを管理しているかどうかに無関係に、ライセンスの最大数まで数えられます。

- 未接続インタフェースのポーリング

  未検出ノードの接続を備えたネットワーク デバイスを含むノード グループを作成できます。次に、ノード グループの未接続インタフェースのポーリングを有効にします。

  NNMi は、多数のインタフェースのあるデバイスに大量のトラフィックを追加できる、ノード グループのデバイス上のインタフェースをすべてポーリングします。

監視の停止

NNMi 管理モードを使って、デバイスまたはインタフェースを管理対象外 または サービス外 に設定できます。管理対象外 は恒久的な状況と見なされます。オブジェクトのステータスを知る心配をする必要はありません。サービス停止中 は一時的な状況と見なされます。1 つ以上のオブジェクトがオフラインになり、ダウン インシデントは過剰になります。

すべてのグループ設定全体のオーバーレイとして、管理モードを考えてください。グループ、ポーリング間隔、種類に無関係に、オブジェクトのステータスが 管理対象外 または サービス外 に設定されている場合、State Poller はそのオブジェクトと通信しません。

ベストプラクティス

検出を行い、データベースに配置することを選択したデバイスやインタフェース (または その両方) の中には、ポーリングの必要がないものもあります。管理対象外 に恒久的に設定するオブジェクトに注意してください。1 つ以上のノード グループを作成し、管理モードを簡単に設定することもできます。

グループの計画作成

ノード グループとインタフェース グループをセットアップしてから、監視を設定する必要があります。したがって、ノード グループとインタフェース グループを設定するときはポーリング要求について考慮する必要があります。重要なデバイスを頻繁に監視できるようにノード グループとインタフェース グループを設定するのが理想的です。クリティカルでないデバイスのチェックをあまり頻繁でないようにできます (そもそもチェックを行う場合です)。

ベストプラクティス

ネットワーク監視を行うノードおよびインタフェース グループのセットを 1 つ設定します。マップにより、ネットワーク可視化用に異なるノード グループのセットを設定します。

これらグループは、**[設定] > [ノード グループ]** または **[設定] > [インタフェース グループ]** サークスペースを使用して定義します。これらグループは、デフォルトで、インシデント、ノード、インタフェース、およびアドレス ビューをフィルタするのに使うのと同じグループです。監視設定用にノード フィルタまたはインタフェース フィルタの別個のセットを作成するには、ノード グループまたはインタフェース グループを開き、**[ノード グループ]** フォームまたは **[インタフェース グループ]** フォームで **[ビュー フィルタ リストに追加]** チェック ボックスをオンにします。**[保存して閉じる]** をクリックします。

[監視の設定] フォームの **[ノードの設定]** タブと **[インタフェースの設定]** タブにあるノード グループまたはインタフェース グループのレベルで、ポーリングの種類とポーリングの間隔を設定します。

類似のポーリングのニーズごとに、インタフェースやデバイス (またはその両方) をグループにまとめる基準を決定します。計画作成に際して考慮すべきいくつかの要因は次のとおりです。

- ネットワークのどのエリアにこれらのデバイスがありますか? タイミング制限があるか?
- デバイスの種類ごとに収集したポーリング間隔またはデータを差別化しますか? インタフェースの種類ごとにか ?
- NNMi には使用できる事前設定されたグループがあるか ?

ベストプラクティス

同時にサービス外 になりそうなオブジェクトのグループ定義を、場所ごとであれ、他の何らかの基準ごとであれ、作成することができます。たとえば、IOS アップグレードを適用しながら、すべての Cisco ルーターを サービス外 モードにできます。

インタフェース グループ

基準に基づいて、どのインタフェース グループを作成するか決定します。インタフェース グループが最初に評価されることを覚えておいてください (77 ページの「状態ポーリングの概念」参照)。インタフェース グループはノード グループ メンバーシップを参照できるので、計画を実現するインタフェース グループの前に、ノード グループの設定を完了できます。

事前設定されたインタフェース グループ

NNMi には、使用できるように既に設定済みの便利なインタフェース グループがいくつかあります。たとえば、次のとおりです。

- ISDN 接続に関連付けられた IFType のある全インタフェース
- 音声接続用のインタフェース
- ポイントツーポイント通信用のインタフェース
- ソフトウェア ループバック インタフェース
- VLAN インタフェース
- リンク集合プロトコルに関与するインタフェース

HP は、時間をかけてさらに多くのデフォルトのグループを追加し、設定作業を簡単にしていきます。既存のグループを使用または変更するか、または自分専用のグループを作成できます。

インタフェースには次の 2 つの種類の修飾子があります。つまり、ホストであるノードと IFType のノード グループ メンバーシップ、またはインタフェース用の他の属性です。これらは次のように組み合わせできます。

- ノード グループ内のノードの全インタフェースを IFType と無関係にグループにまとめます。IFType または属性 (名前、エイリアス、説明、速度、インデックス、アドレス、またはその他の IFType 属性など) は選択しません。
- 特定の IFType または属性のセットのインタフェースは、それらインタフェースが存在するノードに無関係にすべてグループにまとめられます。
- 特定のノード グループに存在する特定の IFType または属性のインタフェースのみがグループにまとめられます。

ノードグループ

インタフェース グループの計画を作成してから、ノード グループの計画を作成します。監視用に作成された全ノード グループがフィルタ ビューに意味があるとは限らないので、ノード グループは独立に設定できます。

事前設定されたノード グループ

HP は、ノード グループのデフォルト集合を用意して、設定作業を簡単にしています。これらの基礎になっているのは、検出プロセスの間にシステム オブジェクト ID から導出されたデバイス カテゴリです。デフォルトのノード グループには以下が含まれます。

- ルーター
- ネットワーキング インフラストラクチャ デバイス (スイッチ、ルーターなど)
- Microsoft Windows システム
- SNMP コミュニティ文字列を持っていないデバイス
- 重要ノード。Causal Engine によって内部的に使用されており、コネクタ障害の危険にさらされているデバイスの特殊処理を提供します。詳細については、NNMi ヘルプの「*定義済ビュー フィルタとして使用されるノード グループ*」を参照してください。

HP は、時間をかけてさらに多くのデフォルトのグループを追加し、設定作業を簡単にしていきます。既存のグループを使用または変更するか、または自分専用のグループを作成できます。

次のノード属性を使用して、関連するノードの定義に条件を付けることができます。

- ノード上の IP アドレス
- ホスト名ワイルドカード規約
- デバイス プロファイル派生物。たとえば、カテゴリ、ベンダー、ファミリ
- MIB II sysName、sysContact、sysLocation

ベストプラクティス

簡単で再使用可能な極小のグループを作成し、監視または視覚化のためにこれらを結合して階層クラスタにすることができます。グループ定義は重なることがあります。たとえば、「すべてのルーター」と「IP アドレスの末尾が 100 のすべてのシステム」です。ノードは複数のグループに属することができると考えられます。

バランスを取るためには、使われない余分なエントリのリストで負担を大きくしないように、設定および表示用に豊富なグループのセットを作成します。

デバイス プロファイルとの相互作用

各デバイスが検出されると、NNMi はシステム オブジェクト ID を使用して、使用可能なデバイス プロファイルのリストにインデックスを作成します。デバイス プロパティは、ベンダー、製品、ファミリ、デバイス カテゴリなど、デバイスの追加属性を導出するために使用されます。

ノード グループを設定するとき、これら導出された属性を使用して、監視設定に適用するデバイスをカテゴリにまとめられます。たとえば、ベンダーを問わず、ネットワーク全体のすべてのスイッチを特定のポーリング間隔でポーリングすることもできます。デバイス カテゴリ「スイッチ」を自分のノード グループの定義特性として使えます。システム オブジェクト ID がカテゴリ「スイッチ」にマップされる、検出されたデバイスはすべて、ノード グループについての設定を受け取ります。

ポーリング間隔の計画作成

オブジェクト グループごとに、NNMi がデータを収集するのに使うポーリング間隔を選択します。サービス レベル契約条項に最も適切に一致するように、間隔は 1 分間と短くすることもできますし、数日間と長くすることもできます。

ベストプラクティス

間隔が短いと、可能な限り迅速にネットワーク問題を認識するのに役立ちます。しかし、あまりに短い間隔であまりに多くのオブジェクトをポーリングすると、State Poller にバックログを発生させる可能性があります。各自の環境について、リソース利用と間隔の間で最良のバランスを見つけてください。

どのデータを収集するかの決定

State Poller サービスは、ポーリングを使って、ネットワークで監視されているデバイスに関する状態情報を収集します。ポーリングは ICMP や SNMP (またはその両方) を使用して実行できます。

ICMP (ping)

ICMP アドレス 監視は、ping 要求を使って、管理対象の各 IP アドレスの使用可能性を確認します。

SNMP

SNMP 監視は、監視されている各 SNMP エージェントが SNMP クエリーに応答していることを確認します。

- State Poller は、間隔ごとに 1 つのクエリーで、監視されている各オブジェクトから設定済み SNMP 情報を収集するよう、高度に最適化されています。設定の変更を保存すると、State Poller は、各オブジェクトのグループ メンバーシップを再計算し、収集する設定済み間隔とデータ セットに再適用します。
- SNMP 監視は、監視されているすべてのインタフェースとコンポーネントに SNMP クエリーを発行し、MIB II インタフェース テーブル、HostResources MIB、およびベンダー特有の MIB から現在の値を要求します。障害監視に使われる値もあります。NNM iSPI Performance for Metrics をインストールしてある場合は、パフォーマンス測定に使われる値もあります。

SNMP コンポーネント稼働状態データ

コンポーネント ヘルス監視をグローバルなレベルで有効または無効にできます。障害に関するコンポーネント稼働監視は、デバイスの障害ポーリング間隔設定に従います。

ポーリングごとに追加データを収集しても、ポーリングを実行する時刻への影響はありません。しかし、各オブジェクトについて保存された追加データによって、State Poller 用にメモリ要求が増加する可能性があります。

パフォーマンス 監視設定は NNM iSPI Performance for Metrics でのみ使用されます。パフォーマンスに関するコンポーネント稼働監視は、デバイスのパフォーマンス ポーリング間隔設定に従います。

ベストプラクティス

監視設定変更をバッチ処理すると、State Poller の進行中の操作が混乱することは少なくなります。

状態ポーリングの設定

この項では、設定のヒントを示し、設定例をいくつか挙げます。この項を読んだ後、特定の手順については、NNMi ヘルプの「*監視動作の設定*」を参照してください。

大きな設定変更を行う前には、既存の設定のコピーを保存しておくことをお勧めします。詳細については、40 ページの「ベストプラクティス：既存の設定を保存」を参照してください。

インタフェース グループとノード グループの設定

[設定] ワークスペースでインタフェース グループとノード グループを作成します。詳細については、NNMi ヘルプの「*ノードまたはインタフェースのグループ作成*」を参照してください。

例　たとえば、ProximiT プロキシ サーバー用にノード グループを設定する方法は次のとおりです。

1. **[設定] > [ノード グループ]** を開き、**[新規作成]** をクリックします。
2. グループ **`Proxy Servers`** という名前を挙げ、**[ビュー フィルタ リストに追加]** をオンにします。
3. **[追加のフィルター]** タブで、**`hostname`** 属性を選択し、演算子の設定を **=** のままにします。
4. 値は、**`prox*.example.com`** のようにワイルドカードを入力します。

   ProximiT デバイスについて Device Profile (デバイス プロファイル) と Category (カテゴリ) を設定してある場合は、**[デバイス フィルター]** タブを使って **[デバイス カテゴリ]** セレクタにアクセスし、作成した Proxy Server カテゴリをグループの基礎にすることができます。
5. グループ定義で **[保存して閉じる]** をクリックします。

ノード グループを設定してから、インタフェース グループ設定でノード グループを参照する必要があります。

インタフェースの監視の設定

State Poller は、ノード グループの前に、インタフェース グループ メンバーシップを分析します。作成した各インタフェース グループ、および使用する既存のインタフェース グループごとに、**[監視の設定]** ダイアログと **[インタフェースの設定]** タブを開き、State Poller がそのグループを処理する方法に関する指示のカスタム セットを作成します。指示には以下のものが含まれます。

- 障害ポーリングの有効化または無効化
- 障害ポーリング間隔の設定
- NNM iSPI Performance for Metrics がある場合、パフォーマンス ポーリングの有効化または無効化
- NNM iSPI Performance for Metrics がある場合、パフォーマンス ポーリング間隔の設定
- NNM iSPI Performance for Metrics がある場合、パフォーマンス管理しきい値の設定
- NNMi がグループ内の未接続インタフェース (または IP アドレスをホストしている未接続インタフェース) を監視するかどうかの選択

インタフェース グループごとに異なる設定ができます。State Poller は、小さい順序番号から大きい順序番号へとリストを評価することを覚えておいてください。

ベストプラクティス　複数のグループにあてはまるオブジェクトは最も順序番号の小さいグループから設定を適用されることを頭に入れておきつつ、順序番号をダブルチェックします。

ノードの監視の設定

あるオブジェクトが設定済みのインタフェース グループにあてはまらない場合、State Poller はノード グループ内のメンバーシップについて、そのオブジェクトを評価します。最も小さい順序番号から最も高い順序番号へと、設定は最初の合致するノード グループに適用されます。

ノード グループごとに、**[監視の設定]** フォームを開いてから **[ノードの設定]** タブを開きます。State Poller がグループを処理する方法に関する指示のカスタム セットを作成します。指示には以下のものを入れられます。

- 障害ポーリングの有効化または無効化
- 障害ポーリング間隔の設定
- NNM iSPI Performance for Metrics がある場合、パフォーマンス ポーリングの有効化または無効化
- NNM iSPI Performance for Metrics がある場合、パフォーマンス ポーリング間隔の設定
- NNM iSPI Performance for Metrics がある場合、パフォーマンス管理しきい値の設定
- NNMi がグループ内の未接続インタフェース (または IP アドレスをホストしている未接続インタフェース) を監視するかどうかの選択

ノード グループごとに異なる設定ができます。

ベストプラクティス　複数のグループにあてはまるオブジェクトは最も順序番号の小さいグループから設定を適用されることを頭に入れておきつつ、順序番号をダブルチェックします。

デフォルト設定の確認

State Poller は、定義済みのインタフェース設定またはノードの設定に合致しないオブジェクトについて **[デフォルト設定]** タブの設定を適用します。このタブの設定を検討し、デフォルト レベルで自分の環境に合致することを確認します。たとえば、デフォルト設定としてすべての未接続インタフェースをポーリングすることはほとんどありません。

➤ 変更を実現するためには、コンソールに戻り、すべての **[設定の監視]** ダイアログ ボックスを必ず **[保存して閉じる]** ようにしてください。

状態ポーリングの評価

この項では、監視設定の進行と成功を評価する方法をリストします。

ネットワーク監視の設定を確認します

NNMi が指定のノードまたはインタフェースの監視に使う設定を決定すると、ステータス ポーリングをいつでも開始できます。

インタフェースまたはノードは正しいグループのメンバーでしょうか？

あるグループにどのインタフェースまたはノードが属するか確認するには、**[設定]** ワークスペースで次の 1 つを選択します。

- ノードグループ
- インタフェース グループ

ヘルプの指示に従って、グループのメンバーを表示します。オブジェクトは複数のグループのメンバーになれること、他のグループの順序番号の方が小さい可能性があることを念頭に置いてください。

その代わりに、オブジェクト (インタフェースまたはノード) を開き **[ノード グループ]** タブまたは **[インタフェース グループ]** タブをクリックして、オブジェクトが属するグループの完全なリストを表示することもできます。このリストは、グループ名ごとにアルファベット順であって、どの設定が適用されるかを決定する順序番号を反映していません。

オブジェクトがグループのメンバーでない場合は次のとおりです。

1 インベントリ ビューのデバイス プロファイルを取得します。

2 **[設定] > [デバイスのプロファイル]** 下にあるデバイス プロファイルに関する属性マップを確認します。

3 ノード グループ定義の属性要件を確認します。

不一致がある場合は、[デバイスのプロファイル] に由来するカテゴリを調整して、その種類のデバイスが自分のノード グループに当てはまるようにできます。**[アクション] > [設定のポーリング]** を実行して、ノードが当てはまるようにノードの属性を更新する必要がある場合もあります。

どの設定が適用されていますか？

特定のノード、インタフェース、またはアドレスに有効な監視設定をチェックするには、該当する [インベントリ] ビュー内のそのオブジェクトを選択し、**[アクション] > [モニタリングの設定]** を選択します。NNMi に現在の監視設定が表示されます。

[有効化された障害ポーリング] と **[障害ポーリング間隔]** の値を調査します。これらの値が予想どおりでない場合は、**[ノード グループ]** または **[インタフェース グループ]** の値を見て、どの順序付けられたグループ一致が適用されるか調べます。

オブジェクト用にトラフィックが無効にされていないことを確認するために、オブジェクトの **[アクション] > [通信の設定]** をチェックする必要があることもあります。

どのデータが収集されていますか？

特定のデバイスのステータス ポーリングを開始し、予想された種類のポーリング (SNMP、ICMP) がそのデバイスについて実行されていることを確認できます。ノードを選択し、**[アクション] > [ステータス ポーリング]** をクリックします。NNMi はデバイスのリアルタイムのステータス チェックを実行します。実行中のポーリングの種類と結果は出力に表示されます。ポーリングの種類が予想したものでない場合は、ノードの監視設定、および監視設定のそれぞれのグローバル、インタフェース、またはノードに関する設定をチェックします。

ステータス ポーリングのパフォーマンスの評価

自分の環境のステータス ポーリングのパフォーマンスを評価するには、State Poller 稼働状態チェックの情報を使って、State Poller サービスの動作を数値で表し、評価します。

State Poller は最新の状態に付いていっていますか？

表 2 に説明されているように、**[システム情報]** ウィンドウの **[StatePoller]** タブで StatePoller サービスの現在の稼動状態統計をいつでもチェックできます。

表 2　**StatePoller 稼動状態情報**

情報	説明
ステータス	State Poller サービスの全般的なステータス
ポーリング カウンタ	• 最後の 1 分に要求された収集 • 最後の 1 分に完了された収集 • 進行中の収集
最後の 1 分にスキップを実行する時刻	設定済みのポーリング間隔内で完了しなかった、定期的にスケジュールされたポーリングの数。値がゼロでない場合は、ポーリング エンジンが最新の状態に付いていっていないか、またはターゲットが応答より速くポーリングされています。 • 監視すべきもの : この値が増加し続ける場合は、ターゲットとの通信に問題があるか、または NNMi の負荷が過剰です。 • 実行すべきアクション : `nnm.?.0.log` ファイルで文字列 `com.hp.ov.nms.statepoller` で始まるクラスのメッセージを探して、スキップされたポーリングのターゲットを特定します。 — スキップされたポーリングのターゲットが同じ場合、設定を変更してこれらのターゲットのポーリング頻度を低くするか、タイムアウトを増やします。 — スキップされたポーリングのターゲットが異なる場合、NNMi のシステム パフォーマンス (特に ovjboss の使用可能メモリ) を確認します。
過去 1 分以内の古い収集	古い収集というのは、少なくとも 10 分間、ポーリング エンジンから応答を受信していない収集のことです。稼働状態が良好なシステムでは古い収集はありません。 • 監視すべきもの : この値が一定して増加する場合は、ポーリング エンジンに問題があります。 • 実行すべきアクション : `nnm.?.0.log` ファイルで文字列 `com.hp.ov.nms.statepoller` で始まるクラスのメッセージを探して、古い収集のターゲットを特定します。 — 古い収集のターゲットが 1 つの場合、この問題を解決できるまでターゲットを管理から除外します。 — 古い収集のターゲットが異なる場合、NNMi システムと NNMi データベースのパフォーマンスを確認します。NNMi を停止して再起動します。
ポーリング結果のキューの長さ	• 監視すべきもの : この値はほとんどの時間 0 に近いはずです。 • 実行すべきアクション : キューのサイズがきわめて大きい場合、ovjboss はメモリを超えて実行されている可能性があります。
状態マッパー入力キューの長さ	• 監視すべきもの : この値はほとんどの時間 0 に近いはずです。 • 実行すべきアクション : このキューのサイズがきわめて大きい場合は、NNMi システムと NNMi データベースのパフォーマンスをチェックします。
状態アップデータ キュー期間	• 監視すべきもの : この値はほとんどの時間 0 に近いはずです。 • 実行すべきアクション : このキューのサイズがきわめて大きい場合は、NNMi システムと NNMi データベースのパフォーマンスをチェックします。

状態ポーリングの調整

状態ポーリングのパフォーマンスは次の重要な変数の影響を受けます。

- ポーリングされるデバイス / インタフェースの数
- 設定されるポーリングの種類
- 各デバイスのポーリングの頻度

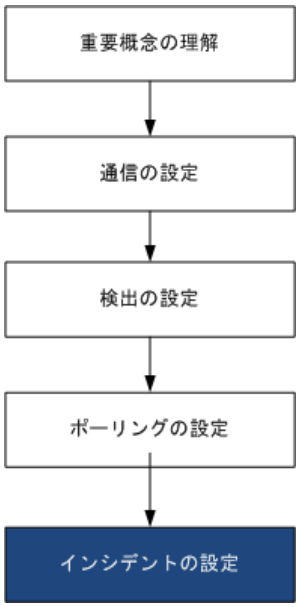
これらの変数は、ネットワーク管理のニーズによって促進されます。ステータス ポーリングについてパフォーマンス上の問題がある場合は、次の設定を考慮してください。

- 個別のノードのポーリング設定はノード グループとインタフェース グループ内のメンバーシップによって制御されるので、類似のポーリング要求のあるノードまたはインタフェースがグループに含まれていることを確認します。
- 未接続インタフェースまたは IP アドレスをホストするインタフェースをポーリングしている場合は、設定をチェックして、必要なインタフェースのみをポーリングしていることを確認します。**[ノードの設定]** フォームまたは **[インタフェースの設定]** フォーム (**[監視の設定]** フォームでグローバルにではなく) でこれらのポーリングを有効にし、最も特定な制御を維持し、ポーリングするインタフェースの最も小さいサブセットを選択します。
- 未接続インタフェースのポーリングでは、未接続の すべてのインタフェースが監視されることを覚えておいてください。IP アドレスのある未接続のインタフェースのみを監視するには、IP アドレスをホストするインタフェースのポーリングを有効にします。

監視設定とは無関係に、ステータス ポーリングは、ネットワーク応答性に左右され、全般的なシステム パフォーマンスの影響を受ける可能性があります。デフォルトのポーリング間隔のあるステータス ポーリングは多くのネットワーク負荷をかけませんが、サーバーとポーリングされているデバイスの間のネットワーク リンクのパフォーマンスが低い場合、ステータス ポーリングのパフォーマンスも低くなる可能性があります。タイムアウトを大きく、再試行の数を小さく設定すると、ネットワーク負荷を低減できますが、これらの設定変更でできるのはそれだけです。タイミングの良いポーリングを行うには、適切なネットワーク パフォーマンスと十分なシステム リソース (CPU、メモリー) が必要です。

コンポーネント稼働状態監視を有効または無効にしても、ポーリングのタイミングには影響がありません。スケジュールされた時刻に、追加の MIB オブジェクトが収集されるだけです。ただし、コンポーネント ヘルス監視を無効にすると、StatePoller が使用するメモリの量が減少する可能性があります。

NNMi インシデント



HP Network Node Manager i Software (NNMi) には、NNMi コンソールに作業可能インシデント数を提供する受信 SNMP トラップをフィルタリングする多数のデフォルト インシデントと相関処理が用意されています。この章では、NNMi インシデントを設定することでネットワーク管理を微調整するのに役立つ情報を説明します。この章は、NNMi ヘルプの情報を補充するものです。NNMi インシデントの概要およびインシデント設定方法の詳細については、NNMi ヘルプの [*インシデントを設定する*] を参照してください。

NNM 6.x/7.x で作業した経験があり、NNMi 9.10 でのイベント 監視がどのように変更されたかを理解したい場合は、相違点の高レベル概要に関する *NNMi アップグレード リファレンス*の「イベント 監視のカスタマイズ」を参照してください。

この章には、以下のトピックがあります。

- インシデントの概念
- インシデントの計画
- インシデントの設定
- インシデントの評価
- インシデントの調整

インシデントの概念

NNMi では、以下のソースからネットワーク ステータス情報が収集されます。

- NNMi の Causal Engine ではネットワークの稼動状態が分析され、継続的に各デバイスの稼動状態ステータス値が提供されます。Causal Engine では、可能な場合は常にネットワーク障害の根本原因も広範囲に評価され、決定されます。
- ネットワーク デバイスからの SNMP トラップ。NNMi の Causal Engine は、分析中にトラップを症状に関する情報として使用します。
- 1 つ以上の NNM 6.x/7.x 管理ステーションから転送される NNM 6.x/7.x イベント。

NNMi は、この情報をネットワーク管理に有用な情報を提供するこのネットワーク ステータス情報に変換します。NNMi には、ネットワーク オペレータが考慮する必要があるインシデント数を減らす多くのデフォルト インシデント相関処理が用意されています。デフォルトのインシデント相関処理をカスタマイズして、環境のネットワーク管理要件に一致する新規インシデント相関処理を作成することができます。

NNMi コンソール のインシデント設定によって、NNMi が作成できるインシデント タイプが定義されます。インシデント設定が受信した SNMP トラップまたは NNM 6.x/7.x イベントと一致しない場合、その情報は廃棄されます。トラップ ソースの管理モードが、NNMi データベースで [管理対象外] または [サービス対象外] に設定されている場合、NNMi では常に受信トラップは廃棄されます。

`nnmtrapconfig.ovpl -dumpBlockList` は、インシデント設定がないか、または無効なためインシデント パイプラインに渡されなかった SNMP トラップなど、現在のインシデント設定に関する情報を出力します。

さらに、NNMi では NNMi トポロジにないネットワーク デバイスからの SNMP トラップは廃棄されます。このデフォルト動作の変更の詳細については、NNMi ヘルプの「*未解決受信トラップの処理*」を参照してください。

詳細については、以下を参照してください。

- NNMi ヘルプの「*イベント パイプラインについて*」
- NNMi ヘルプの「*NNMi の Causal Engine とインシデント*」
- **http://h20230.www2.hp.com/selfsolve/manuals** から入手できる『NNMi 因果関係分析ホワイトペーパー』

インシデント ライフサイクル

表 3 は、インシデントのライフサイクルの段階を説明したものです。

表 3　NNMi インシデント ライフサイクル

ライフサイクル状態	説明	状態設定者	インシデント使用者
なし	NNMi イベント パイプラインはすべてのソースから入力を受領し、必要に応じてインシデントを作成します。	該当なし	• NNMi
抑止済み	インシデントは保管場所にあり、別のインシデントとの相関処理待ちです。インシデント ビューアのインシデントを減らすために、この待機期間があります。 ダンプニング周期はインシデント タイプによって異なります。詳細については、97 ページの「インシデントの抑制、強化、およびダンプニング」を参照してください。	NNMi	• NNMi
登録済み	インシデントは、インシデント ビューで見ることができます。 インシデントは任意の設定済み宛先へ転送されます (近隣またはグローバル マネージャ)。	NNMi ユーザーはインシデント ビューでこの状態を設定することもできます。	• ユーザー • ライフサイクル移行アクション • インシデントを転送する統合

表 3　NNMi インシデント ライフサイクル (続く)

ライフサイクル状態	説明	状態設定者	インシデント使用者
進行中	インシデントは問題を調査するいずれかのユーザーに割り当てられています。 ネットワーク管理者によってこの状態の特定の意味が定義されます。	ユーザー	• ユーザー • ライフサイクル移行アクション • インシデントを転送する統合
完了	インシデントによって指定された問題の統合は完了し、ソリューションが配置されています。 インシデントが識別する問題 ネットワーク管理者によってこの状態の特定の意味が定義されます。	ユーザー	• ユーザー • ライフサイクル移行アクション • インシデントを転送する統合
解決済み	このインシデントによってレポートされた問題が解決したことを NNMi が確認したことを示します。たとえば、デバイスからインタフェースを取り外すと、そのインタフェースに関するインシデントはすべて自動的に「解決済み」になります。	ユーザーまたは NNMi	• ユーザー • ライフサイクル移行アクション • インシデントを転送する統合

トラップおよびインシデント転送

表 4 は、トラップおよびインシデントを NNMi 管理サーバーから別の宛先へ転送する方法を要約したものです。テーブルの補足テキストによって、NNMi の SNMP トラップ転送メカニズムと NNMi のノースバウンド インタフェース SNMP トラップ転送メカニズムが比較できます。

表 4　トラップおよび NNMi インシデント転送でサポートされている方法

	NNMi トラップ転送	NNMi Northbound インタフェース トラップ転送	グローバル ネットワーク管理のトラップ転送
転送対象	• ネットワーク デバイスからの SNMP トラップ • NNM 管理ステーションからの NNM 6.x/7.x イベント	• ネットワーク デバイスからの SNMP トラップ • NNMi 管理イベント	• ネットワーク デバイスからの SNMP トラップ • NNM 管理ステーションからの NNM 6.x/7.x イベント
転送フォーマット	受信したままの SNMPv1、v2c、または v3 トラップ (SNMPv3 トラップは SNMPv2c トラップへ変換可能)	NNMi インシデントから作成された SNMPv2c トラップ	NNMi インシデント
追加情報	ほとんどの場合、NNMi は varbind を追加して元のトラップ ソースを識別します。 NNMi が SNMPv1 トラップを変更することはありません。	NNMi は varbind を追加して元のトラップ ソースを識別します。	リージョナル マネージャ プロセスによってインシデントに追加された情報はすべて、転送済みインシデントに保持されます。

表 4　トラップおよび NNMi インシデント転送でサポートされている方法 (続く)

	NNMi トラップ転送	NNMi Northbound インタフェース トラップ転送	グローバル ネットワーク管理のトラップ転送
設定先	**[設定]** ワークスペースの **[トラップ転送の設定]**	**[統合モジュールの設定]** ワークスペースの **[HPOM]**、**[Northbound インタフェース]**、または **[Netcool]**	**[SNMP トラップの設定]** フォームまたは **[リモート NNM 6.x/7.x のイベント設定]** フォームの **[グローバル マネージャへの転送]** タブ
注		NNMi には、NNMi ノースバウンド インタフェース上に以下の統合が構築されています。 • 505 ページの「NNMi ノースバウンド インタフェース」 • 539 ページの「HP NNMi-HPOM 統合 (エージェント実装)」 • 577 ページの「HP NNMi Integration Module for Netcool Software」	グローバル マネージャのインシデント ビューに表示されるリモート インシデントを転送します。転送済みインシデントはグローバル マネージャ上での相関処理に参加します。
詳細情報	NNMi ヘルプに *トラップ転送を設定する*	508 ページの「NNMi ノースバウンド インタフェースの使用法」	• NNMi ヘルプの *SNMP トラップ インシデントのグローバル マネージャ設定への転送設定* • NNMi ヘルプの *リモート 6.x/7.x イベント インシデントのグローバル マネージャ設定への転送設定*

比較：サードパーティ SNMP トラップを別のアプリケーションに転送する

NNMi が管理デバイスから受信する SNMP トラップを別のアプリケーションに転送する場合は、以下のいずれかの方法を使用します。

- NNMi SNMP トラップ転送メカニズムを使用。NNMi SNMP トラップ転送の設定方法の詳細については、NNMi ヘルプの「*トラップ転送を設定する*」を参照してください。
- NNMi ノースバウンド インタフェース SNMP トラップ転送メカニズムを使用。受信した SNMP トラップを転送する NNMi ノースバウンド インタフェースの設定の詳細については、516 ページの表 56 の インシデント を参照してください。

受信側アプリケーションがトラップを識別する方法は、SNMP トラップ転送メカニズムでは以下のように異なります。

- *Windows (すべて) および UNIX (元のトラップ転送なし)*

  この説明は、デフォルトおよび SNMPv3 から SNMPv2c への変換転送オプションに該当します。

Windows NNMi 管理サーバー上の NNMi SNMP トラップ転送メカニズムにより、トラップ転送先へ転送する前に各 SNMP トラップが収集されます。トラップは NNMi 管理サーバーからのものと考えられます。(この情報は、**[トラップ転送先]** フォームで元のトラップ転送オプションが選択されていない UNIX NNMi 管理サーバーにも適用されます。)

受信側アプリケーションのトラップ送信デバイスとイベント間の関連付けを正しくするため、これらのトラップのルールを収集した varbind に対してカスタマイズする必要があります。originIPAddress (.1.3.6.1.4.1.11.2.17.2.19.1.1.3) varbind からの値を解釈します。originIPAddress の値は汎用タイプ InetAddress のバイト文字列で、originIPAddressType (.1.3.6.1.4.1.11.2.17.2.19.1.1.2) varbind の値によって決まる InetAddressIPv4 または InetAddressIPv6 です。ルールによって originIPAddressType varbind を読み取って、originIPAddress varbind のインターネット アドレス タイプ (ipv4(1)、ipv6(2)) の値を決定する必要があります。ルールによって originIPAddress の値を表示文字列に変換する必要もあります。

NNMi が転送されたトラップに追加する varbind の詳細については、NNMi ヘルプ、RFC 2851、および以下のファイルの「*NNMi が提供するトラップ varbind*」を参照してください。

— *Windows*: `%NNM_SNMP_MIBS¥Vendor¥Hewlett-Packard¥hp-nnmi.mib`

— *UNIX*: `$NNM_SNMP_MIBS/Vendor/Hewlett-Packard/hp-nnmi.mib`

- *元のトラップ転送が搭載された UNIX*

  UNIX NNMi 管理サーバー上の NNMi SNMP トラップ転送メカニズムにより、NNMi が受信するものと同じフォーマットでトラップを転送できます。各トラップは管理対象デバイスがトラップ転送先に直接送信したように表示されるため、受信側アプリケーションに設定された既存のトラップ処理は変更なしで動作する必要があります。

  詳細については、NNMi ヘルプの「*トラップ転送先フォーム*」の元のトラップ転送オプションを参照してください。

- *NNMi ノースバウンド インタフェース (全オペレーティング システム)*

  NNMi Northbound インタフェースは各 SNMP トラップを強化してから、トラップ転送先に転送します。トラップは NNMi 管理サーバーからのものと考えられます。受信側アプリケーションのトラップ送信デバイスとイベント間の関連付けを正しくするため、これらのトラップのルールを収集した varbind に対してカスタマイズする必要があります。IncidentNodeHostname（1.3.6.1.4.1.11.2.17.19.2.2.21）および IncidentNodeMgmtAddr（1.3.6.1.4.1.11.2.17.19.2.2.24）varbind によって元のトラップ ソースが識別されます。

MIB

NNMi では、以下の管理情報ベース (MIB) ファイルを NNMi データベースにロードする必要があります。

- Custom Poller 機能、折れ線グラフ、またはその両方の MIB 式で使用するすべての MIB 変数
- NNMi が稼動状態を監視するノード コンポーネント (ファン、または電源など)
- (NNM iSPI Performance for Metrics) しきい値監視で使用するすべての MIB 変数

NNMi では、以下の管理情報ベース (MIB) ファイル、または MIB ファイルで定義されているトラップを NNMi データベースにロードする必要があります。

- ノースバウンド宛先に転送するすべての SNMP トラップ
- (NNM iSPI NET) トラップ分析レポートからアクセスするすべての MIB 変数

カスタムインシデント属性

NNMi では、カスタム インシデント属性 (CIA) を使用して、インシデントに追加情報が追加されます。

- SNMP トラップ インシデントの場合、NNMi では元のトラップ varbind はインシデントの CIA として格納されます。
- 管理イベント インシデントの場合、NNMi では関連情報 (com.hp.ov.nms.apa.symptom など) はインシデントの CIA として追加されます。

インシデント CIA を使用すると、インシデント ライフサイクル移行アクション、抑制、重複解除、強化などの範囲を絞り込むことができます。CIA を使用して、インシデント ビューまたはフォームのアプリケーション メニュー項目の信頼性を絞り込むこともできます。

指定のインシデントに NNMi がどの CIA を追加するかを決定するには、インシデント ビューのサンプル インシデントを開き、[カスタム属性] タブの情報を確認します。

解決済み管理イベント インシデントに追加される CIA

管理イベント インシデントの原因となった状態が該当しなくなったと NNMi Causal Engine が判断すると、NNMi はそのインシデントのライフサイクル状態を [解決済み] に設定し、表 5 にリストされている CIA をインシデントに追加します。NNMi コンソール ユーザーは、**[インシデント]** フォームの **[相関処理の注]** フィールドでこの情報を確認できます。ライフサイクル移行アクションでは、CIA の値が直接使用されることがあります。

表 5　　解決済みインシデントのカスタム インシデント属性

名前	説明
cia.reasonClosed	NNMi がインシデントをキャンセルしたか解決済みにした理由。この理由は、NodeUp や InterfaceUp など、結果の名前にもなります。 このフィールドが設定されていない場合は、NNMi コンソール ユーザーがインシデントを解決済みにしたということになります。 cia.reasonClosed CIA の NNMi の期待値を判断するには、NNMi ヘルプの「*NNMi がインシデントを解決済みにする方法*」を参照してください。
cia.incidentDurationMs	機能停止の時間 (ミリ秒単位)。ステータスが停止中になってから動作中に戻るまで、NNMi が測定します。この値は、cia.timeIncidentDetectedMs と cia.timeIncidentResolvedMs の CIA の差です。停止中インシデントと動作中インシデントのタイムスタンプを比較するより正確な測定値です。
cia.timeIncidentDetectedMs	NNMi Causal Engine が最初に問題を検出したときのタイムスタンプ (ミリ秒単位)。
cia.timeIncidentResolvedMs	問題が解決したことを NNMi Causal Engine が検出したときのタイムスタンプ (ミリ秒単位)。

NNMi は、多くの一次的根本原因インシデントと二次的根本原因インシデントに、表 5 の示した CIA を追加します。たとえば NodeDown インシデントには、InterfaceDown インシデントと AddressDown インシデントが二次的根本原因として含まれることがあります。NNMi が NodeDown インシデントを解決済みにすると、NNMi は二次的インシデントも解決済みにして、それぞれのインシデントのコンテキストの値を含む CIA を二次的インシデントに追加します。

NNMi は、以下のデフォルト管理イベント インシデント タイプに、表 5 に示した CIA を追加しません。

- NNMi コンソール ユーザーが手動で解決済みにしたインシデント
- NNMi データベースから削除されたオブジェクトに応答して NNMi が解決済みにしたインシデント
- IslandGroupDown インシデント
- NnmClusterFailover、NnmClusterLostStandby、NnmClusterStartup、NnmClusterTransfer の各インシデント
- 以下のファミリーのインシデント
  - 相関処理
  - ライセンス
  - NNMi ヘルス
  - トラップ分析

インシデント数の削減

NNMi には、ネットワーク オペレータが NNMi コンソール で見るインシデント数を削減する以下のカスタマイズ可能相関処理が用意されています。

- Pairwise 相関処理 - あるインシデントが別のインシデントによってキャンセルされます。
- 重複解除相関処理 - 指定した時間ウィンドウ内に複数のインシデントのコピーを受信すると、重複解除インシデントの重複が相関処理されます。新たに受信した各重複インシデントの時間ウィンドが再開始されます。このように、NNMi では相関処理時間ウィンドウの全期間中、重複を受信しなくなるまで重複インシデントが相関処理されます。
- レート相関処理 - 指定時間帯内にインシデントに関する指定コピー数を受信すると、レート インシデントの重複が相関処理されます。時間ウィンドウの残り時間にかかわらず、指定数のインシデントを受信すると NNMi によってレート インシデントが生成されます。

インシデントの抑制、強化、およびダンプニング

NNMi には、インシデントからほとんどの値を取得する便利な機能セットが用意されています。各インシデント タイプに対して、以下のインシデント設定オプションでインシデントが関連する場合を具体的に指定することができます。

- 抑制 - インシデントが抑制設定に一致すると、そのインシデントは NNMi コンソール インシデント ビューに表示されません。インシデントの抑制は、あるノード (ルーター、スイッチなど) にとっては重要であるが、他にとっては重要ではないインシデント (SNMPLinkDown トラップなど) の場合に便利です。

- 強化 - インシデントが強化設定に一致すると、インシデントのコンテンツに応じて、NNMi によって 1 つ以上のインシデント値 (重大度、メッセージなど) が変更されます。インシデントの強化は、トラップ varbind (負荷量) に識別情報を継承するトラップ処理 (RMONFallingAlarm など) の場合に便利です。
- ダンプニング - インシデントがダンプニング設定に一致すると、ダンプニング周期中、NNMi によってそのインシデントのアクティビティが遅延されます。インシデントのダンプニングには、NNMi Causal Engine がインシデントの根本原因分析を実行する時間があり、NNMi コンソール 内のインシデント数を減らし、より意味のあるインシデントにする上で便利です。

NNMi には、各インシデント タイプに抑制、強化、ダンプニングに対する以下の設定レベルが用意されています。

- インタフェース グループ設定 - ソース オブジェクトが NNMi インシデント グループのメンバーである場合のインシデント動作が指定されます。各インタフェース グループに異なる動作を指定できます。
- ノード グループ設定 - ソース オブジェクトが NNMi ノード グループのメンバーである場合のインシデントの動作が指定されます。各ノード グループに異なる動作を指定できます。
- デフォルト設定 - デフォルトのインシデント動作が指定されます。

NNMi では、各インシデントの設定領域 (抑制、強化、ダンプニング) に対して、以下の手順を使用して特定のインシデントの動作が決定されます。

1 インタフェース グループ設定のチェック：
   - ソース オブジェクトが任意のインタフェース グループ設定に一致する場合は、一致内で最下位順序番号で定義された動作を実行し、一致検索を停止します。
   - ソース オブジェクトがどのインタフェース グループ設定とも一致しない場合は、手順 2 を続行します。
2 ノード グループ設定のチェック：
   - ソース オブジェクトが任意のノード グループ設定に一致する場合は、一致内で最下位順序番号で定義された動作を実行し、一致検索を停止します。
   - ソース オブジェクトがどのノード グループ設定とも一致しない場合は、手順 3 を続行します。
3 デフォルト設定で定義された動作を実行します (ある場合)。

ライフサイクル移行アクション

ライフサイクル移行アクションは管理者が提供するコマンドであり、インシデントのライフサイクル状態が変化してアクション設定と一致したときに実行されます。インシデントのアクション設定は、1 つのインシデント タイプの 1 つのライフサイクル状態に固有です。このインシデント タイプが特定のライフサイクル状態に移行すると、アクション設定により、実行するコマンドが特定されます。コマンドには引数を含めることができ、これによってインシデント情報がアクション コードに渡されます。

アクション コードは、NNMi 管理サーバーで正しく実行される Jython ファイル、スクリプト、実行可能ファイルのいずれかにすることができます。アクション コードは 1 つのインシデント タイプに固有のものにしたり、多くのインシデント タイプを処理するようにしたりできます。たとえば、ConnectionDown、NodeDown、NodeOrConnectionDown の

いずれかのインシデントを NNMi が作成したときにネットワーク オペレータを呼び出すアクション コードを作成できます。それぞれのインシデント タイプの [登録済み] ライフサイクル状態に 1 つのインシデント アクションというように、3 つのインシデント アクションを設定できます。

同じように、アクション コードを 1 つのライフサイクル状態の変化に固有にしたり、複数のライフサイクル状態の変化に対応させたりすることができます。たとえば、NNMi が InterfaceDown インシデントを作成したときにトラブル チケットを生成し、InterfaceDown インシデントがキャンセルされたときにトラブル チケットを解決済みにするアクション コードを作成できます。[登録済み] 状態に 1 つ、[解決済み] 状態に 1 つというように、InterfaceDown インシデントに 2 つのインシデント アクションを設定できます。

それぞれのアクション設定には、CIA に基づいて負荷量フィルタを組み込んで、アクションが実行されるときを制限できます。さらにフィルタリングするには、インシデントの強化を使用して CIA をインシデントに追加できます。NNMi はインシデント ソースからその属性の値を判別します。たとえば一部のノードにカスタム属性を追加した場合は、この情報をインシデントに CIA として追加し、インシデント アクションの負荷量フィルタをこの属性値に基づくようにすることができます。

インシデントの計画

以下の領域で決定します。

- NNMi が処理するデバイス トラップ？
- NNMi で表示するインシデント？
- インシデントに対する NNMi の対応方法？
- NNMi による NNM 管理ステーションからのトラップ受信の可否？
- NNMi による別のイベント レシーバへのトラップ転送の可否？

NNMi が処理するデバイス トラップ？

ネットワークに関連するデバイス トラップを識別し、各トラップのインシデント設定を計画します。NNMi では、MIB を NNMi にロードしないでトラップを処理できます。MIB に TRAP-TYPE または NOTIFICATION-TYPE マクロが含まれる場合は、MIB で定義されたトラップにスケルトン インシデント設定を作成できます。

NNMi トポロジにないデバイスからのトラップを表示するかどうかを決定します。

NNMi で表示するインシデント？

インシデントのデフォルト セットで開始することをお勧めします。インシデント設定は徐々に拡大および削減できます。

重複解除、レート設定、ペア相関処理によって削減できるインシデントを計画します。

インシデントに対する NNMi の対応方法？

インシデントが発生した場合の NNMi のアクション (ネットワーク オペレータへの電子メール送信など) 各アクションを実行するライフサイクルの状態？

NNMi による NNM 管理ステーションからのトラップ受信の可否？

NNMi と連動してネットワーク領域の管理を継続する 1 つ以上の NNM 6.x/7.x 管理ステーションが環境に含まれる場合は、NNMi オペレータのネットワーク管理をサポートする NNM 6.x/7.x イベントを識別します。NNMi コンソール で使用できる各 NNM 6.x/7.x イベントのインシデント設定を計画します。

NNMi による別のイベント レシーバへのトラップ転送の可否？

環境にサードパーティのトラップ統合が含まれる場合は、NNMi SNMP トラップ転送メカニズムを NNMi ノースバウンド インタフェース SNMP トラップ転送メカニズムと一緒に使用するかどうかを決定します。

NNMi ノースバウンド インタフェース SNMP トラップ転送メカニズムを選択する場合は、NNMi がイベント レシーバに転送するすべてのトラップの MIB をロードします。

インシデントの設定

ここでは、設定のヒントを一覧にし、いくつかの設定例について説明します。このセクションの情報を読んだ後で、具体的な手順の NNMi ヘルプの「*インシデントを設定する*」を参照してください。

大きな設定変更を行う前には、既存の設定のコピーを保存しておくことをお勧めします。詳細については、40 ページの「ベストプラクティス：既存の設定を保存」を参照してください。

- 計画したインシデント タイプを設定します。可能な場合は、MIB で定義したトラップのスケルトン インシデント設定から開始します。
- トラップ転送に必要な MIB をすべてロードします。
- NNMi 管理サーバーにトラップを送信するデバイスが設定されていることを確認します。

インシデントの抑制、強化、およびダンプニングの設定

インシデントの抑制、強化、ダンプニングを設定するときは、以下に注意してください。

- 各インタフェース グループ、ノード グループ、またはデフォルト設定に対して、設定を適用できる場合にさらに絞り込むための負荷量フィルタを指定できます。
- インシデント設定フォームの **[インタフェースの設定]** タブにインタフェース グループ設定を設定します。
- インシデント設定フォームの **[ノードの設定]** タブにノード グループ設定を設定します。
- インシデント設定フォームの **[抑制]**、**[強化]**、および **[ダンプニング]** タブにデフォルト設定を設定します。

ライフサイクル移行アクションの設定

ライフサイクル移行アクションを設定するときは、以下に注意してください。

- デフォルトでは、NNMi は以下の場所でアクションを実行します。
  - *Windows*: `%NnmDataDir%¥shared¥nnm¥actions`
  - *UNIX*: `$NNM_DATA/shared/nnm/actions`

  アクションがこの場所にない場合は、**[ライフサイクルの移行アクション]** フォームの **[コマンド]** フィールドでアクションの絶対パスを指定します。

  Jython ファイルは `actions` ディレクトリに配置する必要があります。

- アクション設定を変更するたびに、NNMi によって actions ディレクトリで Jython ファイルが再読み取りされて NNMi にロードされます。
- アクションは、グループとしてインシデント タイプに対して有効になります。
- アクションに渡すことができる NNMi 情報については、NNMi ヘルプの「*インシデント アクション設定の有効なパラメータ*」を参照してください。

インシデントの評価

このセクションでは、インシデント設定を評価する方法を説明します。

- NNMi がネットワークのすべての管理対象デバイスからトラップを受信したことを確認します。

  NNMi がトラップを受信していない場合は、NNMi 管理サーバーでファイアウォールの設定を確認します。

  一部のウイルス対策ソフトウェアにはファイアウォールが組み込まれており、システムのファイアウォールとは別に設定されています。

- 最も重要なトラップがインシデントに変換されることを確認します。
- 正しいライフサイクルの状態移行でインシデント アクションが実行されてることを確認します。
- NNMi がインシデントを期待どおり処理していることを確認します。

  [アクション] > [インシデント設定レポート] メニューには、既存のインシデントをそのインシデント タイプの現在の設定に対してテストする複数のオプションがあります。これらのメニュー項目のいずれかを使用しても、現在 NNMi コンソール にあるインシデントは変更されません。

インシデントの調整

NNMi コンソール インシデント ビューのインシデント数を削減します。以下のメソッドのいずれかを使用します。

- NNMi コンソール では必要のないインシデント タイプのインシデント設定を無効にします。
- [管理対象外] または [サービス停止中] を監視する必要がないネットワーク オブジェクトの管理モードを設定します。NNMi では、これらのノードとそのインタフェースからの受信トラップはすべて廃棄されます。
- NNMi でネットワーク オブジェクトが監視されないように設定します。NNMi では、監視されないトラップ ソースからの受信トラップはすべて廃棄されます。
- 受信インシデントの追加条件または関係を識別します。これらの条件または関係が発生すると、NNMi では受信管理イベントや SNMP トラップの条件またはパターンを識別して、関連するインシデントどうしを相関関係の子として入れ子にすることで、インシデントのフローが変更されます。

未定義トラップのインシデントの有効化および設定

NNMi は、デフォルトで未定義トラップをサイレントにドロップします。NNMi 9.01 以降、NNMi は、ドロップされる可能性がある未定義 SNMP トラップを特定できるようになります。

NNM iSPI NET が NNMi 管理サーバーでライセンス供与されている場合は、受信トラップ合計数 （ ノード別 ）レポートを使用して、ドロップされた SNMP トラップを調べます。詳細については、NNMi ヘルプの「*トラップ情報の分析 (NNM iSPI NET)*」を参照してください。

NNM iSPI NET が NNMi 管理サーバーでライセンス供与されておらず、インシデントとして欠落したトラップを確認する場合は、未定義 SNMP トラップ インシデントを以下のように設定します。

1. 以下のファイルを編集します。
   - *Windows*: `%NNM_PROPS%¥nms-jboss.properties`
   - *UNIX*: `$NNM_PROPS/nms-jboss.properties`
2. ファイルから、以下の行のようなセクションを特定します。

   ```
   #!com.hp.nnm.events.allowUndefinedTraps=false
   ```

   この行を以下のように変更します。

   ```
   com.hp.nnm.events.allowUndefinedTraps=true
   ```
3. *オプション*。nms-jboss.properties ファイルで説明されている値を使用し、インシデントの重大度を指定します。ファイルから、以下の行のようなセクションを特定します。

   ```
   #!com.hp.nnm.events.undefinedTrapsSeverity=NORMAL
   ```

   この行を以下のように変更し、定義した重大度の値を *YourSpecifiedSeverity* の代わりに使用します。

   ```
   com.hp.nnm.events.undefinedTrapsSeverity=YourSpecifiedSeverity
   ```

4 *オプション*。nms-jboss.properties ファイルで説明されている値を使用し、インシデントの特性を指定します。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.nnm.events.undefinedTrapsNature=INFO
```

この行を以下のように変更し、定義した特性の値を *YourSpecifiedNature* の代わりに使用します。

com.hp.nnm.events.undefinedTrapsNature=*YourSpecifiedNature*

5 以下のコマンドを実行して ovjboss を再開します。

a **ovstop ovjboss**

b **ovstart ovjboss**

6 未定義トラップのリストを検討し、制御するトラップ用に新しいインシデント設定を作成します。NNMi で新しいインシデントを表示する場合はそれを有効にして、NNMi で新しいインシデントを無視する場合はそれを無効にします。詳細については、NNMi ヘルプの「*SNMP トラップ インシデントを設定する*」を参照してください。

NNMi コンソール

この章の情報を読み、NNMi コンソールを使用して NNMi の機能を設定する具体的な方法について理解してください。

この章には、以下のトピックがあります。

- ノード グループの実際的な使用例
- ネットワーク概要マップに表示されるノードの最大数の削減
- ノード グループ マップの表示ノード数の削減

ノード グループの実際的な使用例

以下に、ノード グループを設定する場合の実際的な例を示します。

My Network: 他のノード グループを含んでいる最上位レベルの *コンテナ* ノード グループ。

USA: 他のノード グループを含んでいる中間レベルの *コンテナ* ノード グループ。

Colorado: Colorado に存在するノードを含んでいるノード グループ。

以下の項に注意してください。

- 事前にノード グループ マップのレイアウトを設計するのがベスト プラクティスです。
- ネットワーク監視のためにノード グループとインタフェース グループのセットを 1 つ設定するのがベスト プラクティスです。マップにより、ネットワーク可視化用に異なるノード グループのセットを設定します。
- この例において、**Colorado** はノードが含まれている唯一のノード グループです。
- NNMi では、いくつかの方法でノード グループとノード グループ マップを設定できます。このドキュメントで説明するステップに精通すれば、後続のノード グループやノード グループ マップをより効率よく作成する方法を見つけることもできます。

このドキュメントでは、ノード グループとノード グループ マップを設定する場合の以下のステップについて説明します。

ノード グループの作成

— ステップ 1: My Network ノード グループを作成する

— ステップ 2: USA ノード グループを作成する

— ステップ 3: フィルタを使用して Colorado ノード グループを作成する

— ステップ 4: ノード グループ メンバーを表示してノード グループのフィルタ結果を確認する

— ステップ 5: My Network ノード グループのノード グループ階層を設定する

— ステップ 6: USA ノード グループのノード グループ階層を作成する

親ノード グループには、ノードが含まれていない場合があります。その代わり、定義に子ノード グループのみが含まれています。この例では、My Network および USA ノード グループが、子ノード グループのみを含む親ノード グループです。

ノード グループ マップの設定

— ステップ 1: ノード グループ マップを作成する

— ステップ 2: ノード グループ マップを表示する

— ステップ 3: ノード グループのステータスを設定する

— ステップ 4: ノード グループ マップの順序の設定

— ステップ 5: ノード グループ マップに背景イメージを追加する

ノード グループの作成

ノード グループを作成してノード グループ マップに含める作業から説明を始めます。

ステップ 1: My Network ノード グループを作成する

My Network ノード グループを作成するには、以下の手順を実行します。

1 **[設定]** ワークスペースに移動します。

2 **[ノード グループ]** を選択します。

3 **[新規作成]** アイコンをクリックします。

4 [**名前**] 属性に、「**My Network**」と入力します。

5 **[ノート]** 属性に、「最上位のノード グループです」と入力します。

6 **[保存して閉じる]** をクリックしてこの設定を保存します。

ステップ 2: USA ノード グループを作成する

1 **[設定]** ワークスペースに移動します。

2 **[ノード グループ]** を選択します。

3 **[新規作成]** アイコンをクリックします。

4 [**名前**] 属性に、「**USA**」と入力します。

5 **[保存して閉じる]** をクリックしてこの設定を保存します。

ステップ 3: フィルタを使用して Colorado ノード グループを作成する

Colorado ノード グループを作成するには、フィルタ エディタを使用してノードを選択するフィルタを設定します。

可能であれば、**[追加のノード]** タブを使用して一連のノードを指定するのではなく、**[追加のフィルタ]** タブを使用してください。ノード グループ フィルタを使用すると、NNMi では、新規ノードがネットワークに追加されるときに、ノードを正しいノード グループに自動的に配置できます。

1 **[設定]** ワークスペースに移動します。

2 **[ノード グループ]** を選択します。

3 **[新規作成]** アイコンをクリックします。

4 **[名前]** 属性に、「**Colorado**」と入力します。

5 **[追加のフィルタ]** タブを選択します。

6 ノードが入力したホスト名値のいずれかと一致する場合に NNMi がノードを照合するよう指定するには、**[OR]** をクリックします。

7 フィルタ エディタの **[属性]** フィールドで、[hostname] を選択します。

   hostname を選択すると、ノードがこのノード グループに属するかどうかを判断するときに、NNMi がホスト名値を照合するように指定されます。

8 **[演算子]** フィールドで、[like] を選択します。

   [like] を選択すると、検索でワイルドカード文字を使用できます。

9 **[値]** フィールドに、ノード グループに含めるデバイスを表す値を入力します。たとえば、**cisco*.ntc.example.com** は、cisco< *このテキストで置き換える* >.<*network_domain*> という名前のデバイスを表します。

10 **[追加]** をクリックします。

11 **[属性]** フィールドで、[hostname] を選択します。

12 **[演算子]** フィールドで、[like] を選択します。

13 **[値]** フィールドに、Colorado ノード グループに追加する残りのデバイス名を表すワイルドカードを入力します。この例では、「**cisco?***」を使用します。

14 **[追加]** をクリックします。

15 **[保存]** をクリックして、ウィンドウを閉じずにノード グループを保存します。

ステップ 4: ノード グループ メンバーを表示してノード グループのフィルタ結果を確認する

ノード グループ フィルタをテストするため、作成したノード グループのメンバーを表示できます。

[アクション] → [ノード グループの詳細] → [メンバーの表示] を選択して、ノード グループ内のすべてのノードを含んだビューを開きます。

ノード グループ フィルタが正しく機能すると確信できるまで、ノード グループ フィルタ定義の結果を調べてください。

ステップ 5: My Network ノード グループのノード グループ階層を設定する

My Network ノード グループを最上位レベルにして、ノード グループの階層を作成します。

1 **[設定]** ワークスペースの **[ノード グループ]** オプションに戻り、作成したノード グループの一覧を表示します。

2 **My Network** ノード グループに移動して、**[開く]** をクリックします。

3 **[子ノード グループ]** タブをクリックします。

4 **[新規作成]** アイコンをクリックします。

5 **[子ノード グループ]** 属性で、**[検索]** アイコンをクリックして **[クイック検索]** を選択します。

[クイック検索] を使用して、ノード グループなどのオブジェクトがすでに存在する場合にはそれを選択します。

6 **[USA]** を子ノード グループとして選択します。

7 **[保存]** をクリックします。

8 **[保存して閉じる]** をクリックして変更を保存し、**[ノード グループの階層]** フォームを閉じます。

9 **[保存して閉じる]** をクリックして変更を保存し、**[ノード グループ]** フォームを閉じます。

ステップ 6: USA ノード グループのノード グループ階層を作成する

次に、**Colorado** を **USA** ノード グループの子ノード グループとして設定します。ステップ 5: My Network ノード グループのノード グループ階層を設定するの説明にあるのと同じステップを繰り返して行い、Colorado ノード グループを USA ノード グループの子に指定します。

これで、作成したノード グループごとにノード グループ マップを作成する準備ができました。

ノード グループ マップの設定

ステップ 1: ノード グループ マップを作成する

各ノード グループのノード グループ マップを作成するには、**[アクション]** メニューを使用します。

1 マップを作成するノード グループを開きます。

   a **[設定]** ワークスペースの **[ノード グループ]** オプションに戻り、作成したノード グループの一覧を表示します。

   b 対象のノード グループに移動し、**[開く]** アイコンをクリックします。

2 **[アクション]** → **[マップ]** → **[ノード グループ マップ]** を選択して、ノード グループ マップを表示します。

3 ノードおよびノード グループ マップのアイコンの位置を決めます。

4 **[レイアウトを保存]** アイコンをクリックして、ノード マップ アイコンを作成します。

ノードの位置を変更しない場合でも、ノード グループ マップを作成するときには、いつでも **[レイアウトを保存]** を使用してください。**[レイアウトを保存]** によりノード グループ マップが作成されます。

ノード グループ マップが正常に作成されたことを知らせるダイアログ ボックスが表示されます。

5 **[OK]** をクリックします。

6 作成した各ノード グループで、ステップ 1 ～ 5 までを繰り返します。

ステップ 2: ノード グループ マップを表示する

ノード グループ マップを作成できたので、今度はマップを表示して内容を確認します。

1 **[トポロジ マップ]** ワークスペースに移動します。

2 **[ノード グループの概要]** を選択します。

3 最上位レベル マップ **[My Network]** を選択します。

4 アイコンをダブルクリックして、子 nodegGroup マップに移動します。

5 **[戻る]** ボタンを使用して前のマップに戻ります。

ステップ 3: ノード グループのステータスを設定する

NNMi により、ノード グループのステータスの計算方法を設定できます。ノード グループのステータスを設定するときには、以下の中から NNMi で使用する方法を決めます。

- ノード グループ内で最も深刻なノードのステータスを使用する。
- NNMi で使用するパーセンテージの計算結果を指定する。

[ステータスの設定] はグローバル設定です。NNMi は、デフォルトでノード グループ内の最も深刻なノードのステータスを使用します。

1 **[設定]** ワークスペースに移動します。

2 **[ステータスの設定]** を選択します。

3 **[ステータスの設定]** フォームを調べ、デフォルトのパーセンテージを把握してください。パーセンテージを使用するには、**[ほとんどの重大なステータスを伝達]** チェックボックスをオフにしてから、変更を保存する必要があります。

ステップ 4: ノード グループ マップの順序の設定

ノード グループ マップの順序は、**[トポロジ マップ]** ワークスペースに表示されるマップの順序を判断するのに役立ちます。

この例では、ノード グループ マップの順序を使用して、**[トポロジ マップ]** ワークスペースのリストの最初に **My Network** ノード グループ マップが表示されるよう指定します。

1 **[設定]** ワークスペースに移動します。

2 **[ノード グループ マップの設定]** を選択します。

以下の例に示すように、デフォルトの **[トポロジ マップ順序]** の値は、すべてのユーザー定義マップで 50 です。

My Network を **[トポロジ マップ]** ワークスペースの最初のマップとして一覧に表示するよう NNMi に指示するには、**[トポロジ マップ順序]** の値を他のどのマップの **[トポロジ マップ順序]** の値よりも小さい数字 (たとえば **5**) にします。

3 **My Network** ノード グループ マップを開きます。

4 **[トポロジ マップ順序]** 属性で、値を **5** に変更します。

5 **[保存して閉じる]** をクリックして変更を保存し、フォームを閉じます。

マップを最初に NNMi コンソールに表示するかどうかも指定できます。それには、**[設定]** ワークスペースで **[ユーザー インタフェースの設定]** オプションを使用します。

1 **[設定]** ワークスペースに移動します。

2 **[ユーザー インタフェースの設定]** をクリックします。

3 **[初期ビュー]** 属性で、ドロップダウン メニューを使用して **[トポロジ マップワークスペース内の最初のノードグループ]** ワークスペースを選択します。

これにより、**My Network** マップが初期ビューに表示されます。

初期ビューを確認するには、NNMi からサインアウトしてからもう一度サインインします。**My Network** マップが NNMi コンソールに表示されるビューになります。

ステップ 5: ノード グループ マップに背景イメージを追加する

マップに背景グラフィックを含めるには、選択したノード グループ マップで **[ノード グループ マップの設定]** を使用します。

1 **[設定]** ワークスペースに移動します。

2 **[ユーザー インタフェース]** をクリックします。

3 **[ノード グループ マップの設定]** をクリックします。

4 **My Network** ノード グループ マップを開きます。

5 **[背景イメージ]** タブに移動します。

6 **[http://MACHINE:PORT/nnmdocs/images/]** をクリックします。

NNMi に、HP が提供するグラフィックの一覧が表示されます。

7 **world.png** リンクを右クリックします。

8 **[リンクの場所をコピー]** を選択します。

9 ディレクトリのリスト ウィンドウを閉じます。

コピーしたリンクを [背景イメージ] 属性に貼り付けます。

後で変更する場合のために、[背景イメージのスケール] の値をメモします。

10 **[保存して閉じる]** をクリックして変更を保存します。

11 **[トポロジ マップ]** ワークスペースに移動し、**[My Network]** を選択して、新しいマップを背景グラフィックと一緒に表示します。

ネットワーク概要マップに表示されるノードの最大数の削減

[ネットワークの概要] マップには、レイヤー 3 ネットワークで最も高度に接続された 250 までのノードを含むマップが表示されます。このマップに含まれるノード数が多すぎると、ノードを移動するときのマップの反応が遅くなったり、複雑すぎて実際の表示に適さなくなったりする可能性があります。**[ネットワークの概要]** マップに表示されるノードの最大数は、以下の例に示すようにして増減できます。

[ネットワークの概要] マップに表示されるノードの最大数を 250 から 100 に変更するとします。これを行うには、以下の手順を実行します。

1 以下のファイルを編集します。

- *Windows*: `%NNM_PROPS%¥nms-ui.properties`
- *UNIX*: `$NNM_PROPS/nms-ui.properties`

2 以下の行に似たテキストを特定します。

```
#!com.hp.nnm.ui.networkOverviewMaxNodes = 250
```

行を以下のように変更します。

```
com.hp.nnm.ui.networkOverviewMaxNodes = 100
```

行の始めにある **#!** 文字を必ず削除してください。

3 変更を保存します。

ノード グループ マップの表示ノード数の削減

数百単位のノードを含むようにノード グループ マップを設定すると、ノード グループを表示するマップには、予期される詳細なノード アイコンではなく、多くの小さいノード アイコンが表示されます。より詳細なマップを表示するには、ズーム機能を使用する必要があります。ズーム機能を使用すると、マップを表示するときの NNMi コンソールのパフォーマンスが低下する可能性があります。

解決方法は、以下の手順を実行して、表示されるノードまたは表示されるエンド ポイント、あるいはその両方の数を制限することです。

1 NNMi コンソールで、**[設定]** をクリックします。

2 **[ユーザー インタフェース]** の下にある **[ユーザー インタフェースの設定]** をクリックします。

3 **[デフォルトのマップ設定]** タブを選択します。

4 [表示するノードの最大数] フィールドに表示された値を変更します。

5 [表示するエンド ポイントの最大数] フィールドに表示された値を変更します。

6 **[保存して閉じる]** をクリックします。

詳細は、NNMi ヘルプの「*デフォルトのマップ設定を定義する*」を参照してください。

詳細設定

この項では以下の章について説明します。

- NNMi ライセンスの取得
- NNMi での証明書の使用
- NNMi とシングル サインオンの使用
- NNMi で使用する Telnet および SSH プロトコルを設定する
- NNMi と LDAP によるディレクトリ サービスの統合
- NNMi セキュリティおよびマルチテナント
- グローバル ネットワーク管理
- IPv6 用 NNMi Advanced の設定
- Solaris ゾーン環境での NNMi の実行

NNMi ライセンスの取得

恒久ライセンス キーをインストールしていない場合は、NNMi 製品には、NNMi のインストール後 60 日間有効な一時試用ライセンス キーが含まれています。この一時試用ライセンス キーを使用すると、NNMi Advanced 機能を使用できるようになります。できるだけ早く、恒久ライセンス キーを入手し、インストールしてください。

NNMi Advancedライセンスに含まれている機能のリストを表示するには、『HP NNMiソフトウェアリリースノート』の「ライセンス」のセクションを参照してください。

恒久ライセンス キーのインストール準備

試用ライセンスでは、250 ノードまでの制限が付けられています。試用ライセンス キーで NNMi を実行している場合、恒久ライセンスでサポートできる数以上のノードを管理できる場合があります。ただし、恒久ライセンスが有効になると、ライセンス制限を超えた分のノードは NNMi により自動的に管理対象外になります。

恒久ライセンスでは管理対象から除外するノードをご自身で決定する場合は、新規ライセンス キーをインストールする前に、あまり重要でないノードを NNMi コンソール を使用して削除してください。

ライセンスの種類および管理対象ノードの数の確認

現在、NNMi が使用しているライセンスの種類を確認するには、以下の手順に従います。

1. NNMi コンソール で、**[ヘルプ] > [HP Network Node Manager i Software について]** の順にクリックします。
2. **[HP Network Node Manager i Software について]** ウィンドウで、**[ライセンス情報]** をクリックします。

   (**[ライセンス情報]** は、[NNMi コンソールのサインイン] ページから入手することもできます。)
3. **[消費]** フィールドに表示されている値を探します。この値が、現在 NNMi が管理しているノードの数です。
4. 恒久ライセンスがサポートできるノード数が、現在 NNMi が管理しているノード数より少ない場合は、NNMi コンソール を使用して、あまり重要でないノードを削除します。詳細については、NNMi ヘルプの「*ノードの削除*」を参照してください。

恒久ライセンス キーの取得およびインストール

恒久ライセンス キーを申請するには、以下の情報が必要です。

- HP 製品番号や製造番号が明記されたエンタイトルメント証明書
- NNMi 管理サーバーの IP アドレス
- HA で動作する NNMi のライセンスの場合は、クラスタの仮想 IP アドレス

  NNMi を HA で実行する場合は、NNMi の商用ライセンスはクラスタの仮想 IP アドレスが対象になります。さらに、HA クラスタのいずれかのノードでは、NNMi の非商用ライセンスが必要です。

- お客様の企業情報もしくは団体情報

Autopass および HP 注文番号の使用 (ファイアウォール使用時は不可)

恒久ライセンス キーを入手してインストールするには、以下の手順に従ってください。

1. コマンドプロンプトで、以下のコマンドを入力し、Autopass ユーザーインタフェースを開きます。

   nnmlicense.ovpl NNM -gui

2. [Autopass] ウィンドウの左側にある **[ライセンス管理]** をクリックします。
3. **[ライセンス キーのインストール]** をクリックします。
4. **[ライセンス キーの取得 / インストール]** をクリックします。
5. HP 注文番号を入力し、Autopass プロンプトに従ってライセンスキーの取得プロセスを完了します。
6. NNMi のインストールは自動的に完了します。

コマンド行で、シードを追加する

自動プロセスが完了しない場合は (NNMi 管理サーバーがファイアウォールの背後にある場合など)、以下の手順を実行します。

1. ライセンスキーを取得するには、以下の HP パスワード配信サービスに移動します。

   https://webware.hp.com/welcome.asp

2. NNMi 管理サーバーのコマンドプロンプトで以下のコマンドを入力し、システムを更新して、ライセンスデータファイルを保存します。

   nnmlicense.ovpl NNM -f *license_file*

   (製品ライセンス ID (NNM) では大文字と小文字が区別されます。)

   詳細については、*nnmlicense.ovpl* のリファレンス ページまたは UNIX のマンページを参照してください。

3. NNMi のインストールは自動的に完了します。

追加のライセンスキーを取得する

HP 営業担当または Hewlett-Packard 認定代理店に、NNMi ライセンス構造に関する情報について問い合わせて、企業向けインストールにライセンス層を追加する方法を確認してください。

追加のライセンス キーを取得するには、HP ライセンス キー配信サービスに移動します。

https://webware.hp.com/welcome.asp

詳細については、NNMi ヘルプの「*ライセンス機能の拡張*」を参照してください。

開発者の方へ : NNMi 開発者ツールキットを使用すると、カスタム Web サービスクライアントを統合して NNMi の機能を拡張できます。NNMi 開発者ライセンスをインストールすると、NNMi により `doc` フォルダに `sdk-dev-kit.jar` ファイルが作成されます。`sdk-dev-kit.jar` ファイルを解凍すると、NNMi 開発者ツールキット ドキュメントやサンプル集を表示できます。

NNMi での証明書の使用

証明書は、Web サーバーの識別情報をブラウザに示すものです。この証明書には、自己署名するか、CA (認証機関) による署名を付けることができます。nnm.keystore ファイルでは、プライベート キーと証明書は対応するパブリック キーとともに格納されます。nnm.truststore ファイルには、通信する他者の証明書、または他者を識別するときに信頼する認証機関の証明書が保存されています。 NNMi は、nnm.keystore ファイルと nnm.truststore ファイルの両方に自己署名証明書を含めます。

特定の NNMi 機能を使用するため、NNMi 管理サーバーはそれぞれの証明書を相互に共有する必要があります。この章では、NNMi 管理サーバー 間でこれらの証明書をコピーする方法と、nnmcertmerge.ovpl スクリプトを使用して nnm.keystore および nnm.truststore ファイルに証明書をマージする方法について説明します。

この章には、以下のトピックがあります。

- すべてをまとめる
- 認証機関証明書を生成する
- 自己署名証明書を使用するようにアプリケーション フェイルオーバーを設定する
- 認証機関を使用するようにアプリケーション フェイルオーバーを設定する
- 自己署名証明書または CA 証明書を使用するように高可用性を設定する
- 自己署名証明書を使用するようにグローバル ネットワーク管理機能を設定する
- 認証機関を使用するようにグローバル ネットワーク管理機能を設定する
- 自己署名証明書を使用するようにアプリケーション フェイルオーバーが有効なグローバル ネットワーク管理を設定する
- ディレクトリ サービスへの SSL 接続を設定する
- HP BSM バージョン 9.xx への SSL 接続の設定

すべてをまとめる

以下の情報に従い、特別な要件に応じて証明書を設定します。

- CA 証明書を使用する場合は、121 ページの「認証機関証明書を生成する」の指示に従ってください。
- グローバル、リージョナル、またはその両方の NNMi 管理サーバーでアプリケーション フェイルオーバー機能を使用するように設定する場合は、追加の設定手順があります。124 ページの「自己署名証明書を使用するようにアプリケーション フェイルオーバーを設定する」の説明にあるグローバル ネットワーク管理設定を完了する前に、クラスタごとに NNMi 管理サーバーの nnm.keystore および nnm.truststore ファイルをマージします。
- 認証機関を使用する必要があり、グローバル、リージョナル、またはその両方の NNMi 管理サーバーでアプリケーション フェイルオーバー機能を使用するように設定した場合は、追加の設定手順があります。まず、121 ページの「認証機関証明書を生成する」の説明にある手順を実行し、次に 126 ページの「認証機関を使用するようにアプリケーション フェイルオーバーを設定する」の説明にあるグローバル ネットワーク管理設定を完了する前に、クラスタごとに NNMi 管理サーバーの nnm.keystore および nnm.truststore ファイルをマージします。
- グローバル、リージョナル、またはその両方の NNMi 管理サーバーで高可用性 (HA) を使用するように設定した場合は、128 ページの「自己署名証明書または CA 証明書を使用するように高可用性を設定する」の説明にあるグローバル ネットワーク管理設定を完了する前に、nnm.keystore および nnm.truststore ファイルで自己署名証明書を作成します。
- 各 HA またはアプリケーション フェイルオーバー クラスタを正しく設定したら、アクティブなリージョナル ノードからアクティブなグローバル ノードに nnm.truststore ファイルをコピーし、それからトラストストアをマージすることにより、グローバル ネットワーク管理機能を有効にします。この操作は、アクティブなリージョナル ノードごとに実行する必要があります。131 ページの「自己署名証明書を使用するようにアプリケーション フェイルオーバーが有効なグローバル ネットワーク管理を設定する」の情報を確認してください。NNMi 管理サーバーで 121 ページの「認証機関証明書を生成する」の説明にある手順を使用して生成した CA 証明書を使用する場合、グローバル トラストストアにマージする必要がある証明書はそれらの CA 証明書のみです。
- グローバル ネットワーク管理設定で NNMi 管理サーバーを設定し、その後、リージョナル、グローバル、またはその両方をアプリケーション フェイルオーバー クラスタに含めるよう変更する場合は、124 ページの「自己署名証明書を使用するようにアプリケーション フェイルオーバーを設定する」の指示に従ってください。そのセクションに示されているコマンドを使用して nnm.keystore および nnm.truststore ファイルを正しく設定し、変更された nnm.truststore ファイルをグローバル NNMi 管理サーバーにコピーし、そのファイルをグローバル NNMi 管理サーバーの nnm.truststore ファイルにマージする必要があります。
- グローバル ネットワーク管理設定で NNMi 管理サーバーを設定し、その後、リージョナル、グローバル、またはその両方で HA を使用するよう変更する場合は、128 ページの「自己署名証明書または CA 証明書を使用するように高可用性を設定する」の指示に従ってください。
- ディレクトリ サービス通信を有効にすると、NNMi は、ディレクトリ サービスからデータを取得するときに LDAP プロトコルを使用します。ディレクトリ サービスで SSL 接続が必要な場合は、132 ページの「ディレクトリ サービスへの SSL 接続を設定する」の指示に従ってください。

認証機関証明書を生成する

CA (認証機関) を使用する場合は、以下の手順で CA 証明書を生成します。

NNMi で CA を使用する場合は、RSA アルゴリズムを使用して証明書に署名します。DSA アルゴリズムはサポートされていません。

1 nnm.keystore および nnm.truststore ファイルが存在する NNMi 管理サーバーのディレクトリに変更します。
   - *Windows*: %NNM_DATA%¥shared¥nnm¥certificates
   - *UNIX*: $NNM_DATA/shared/nnm/certificates
2 nnm.keystore ファイルのバックアップ コピーを保存します。
3 システムからプライベート キーを生成します。このプライベート キーを生成するには、*keytool* コマンドを使用します。
   a 以下のコマンドを実行します。
      — *Windows*: **%NnmInstallDir%¥nonOV¥jdk¥nnm¥bin¥keytool.exe -genkeypair -validity 3650 -keyalg rsa -keystore nnm.keystore -storepass nnmkeypass -alias *myserver.mydomain***
      — *UNIX*: **$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -genkeypair -validity 3650 -keyalg rsa -keystore nnm.keystore -storepass nnmkeypass -alias *myserver.mydomain***

      別名 (この例では *myserver.mydomain*) は、この新規作成キーを識別する名前です。別名は任意の文字列にすることができますが、HP では、*myserver.mydomain* 別名の変数として、ご使用のシステムの完全修飾ドメイン名を使用するようお勧めします。

      Linux オペレーティングシステムには、この手順で使用される keytool コマンドまたはコマンドオプションと互換性のないkeytoolコマンドがあります。

   b 必要な情報を入力します。

      重要: 姓名の入力を求められたら、システムの FQDN (完全修飾ドメイン名) を入力してください。

4 以下のコマンドを実行して、CSR (証明書署名要求) ファイルを作成します。
      — *Windows*:**%NnmInstallDir%¥nonOV¥jdk¥nnm¥bin¥keytool.exe -keystore nnm.keystore -certreq -storepass nnmkeypass -alias *myserver.mydomain* -file CERTREQFILE**
      — *UNIX*: **$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -keystore nnm.keystore -certreq -storepass nnmkeypass -alias *myserver.mydomain* -file CERTREQFILE**

keytool コマンドの詳細については、**http://www.oracle.com/technetwork/java/index.html** で「鍵および証明書管理ツール」を検索してください。

5 CA 署名機関に CSR を送信します。以下のいずれかが発行されます。

- myserver.crt という名前の署名付き証明書。myserver.crt ファイルには、サーバー証明書 (ファイルに含まれている最上位の証明書) と、1 つ以上の CA (認証機関) 証明書の両方が含まれています。CA証明書を新しいファイルであるmyca.crt ファイルにコピーします。サーバー証明書を nnm.keystore ファイルにインポートする場合は myserver.crt ファイルを使用し、CA 証明書を nnm.truststore ファイルにインポートする場合は myca.crt ファイルを使用します。
- この手順における、myserver.crt と CA.crt という名前の 2 つのファイル。CA.crtファイルの内容をmyserver.crtファイルの最後に追加します。サーバー証明書をnnm.keystoreファイルにインポートする場合はmyserver.crt ファイルを使用し、CA 証明書を nnm.truststore ファイルにインポートする場合は myca.crt ファイルを使用します。

以下は、CA 署名機関から受け取るファイルの例です。

独立サーバーで、複数の CA 証明書ファイルがある場合

```
-----BEGIN CERTIFICATE-----
Sample/AVQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
.............................................................
.............................................................
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
```

結合サーバーで、1 つのファイルに複数の CA 証明書がある場合

```
-----BEGIN CERTIFICATE-----
Sample1/VQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
.............................................................
.............................................................
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Sample2/Gh0dHA6Ly9jb3JwMWRjc2cyLnNnLmludC5wc2FnbG9iYWwuY29tL0Nlc
RaOCApwwggKYMB0GA1UdDgQWBBSqaWZzCRcpvJWOFPZ/Be9b+QSPyDAfBgNVHSMC
.............................................................
.............................................................
Wp5Lz1ZJAOu1VHbPVdQnXnlBkx7V65niLoaT90Eqd6laliVlJHj7GBriJ90uvVGu
BQagggEChoG9bGRhcDovLy9DTj1jb3JwMWRjc2cyL==
-----END CERTIFICATE-----
```

6 これらの証明書が記録されているファイルを NNMi 管理サーバーのいずれかの場所にコピーします。この例では、以下の場所にファイルをコピーします。

- *Windows*: %NNM_DATA%¥shared¥nnm¥certificates
- *UNIX*: $NNM_DATA/shared/nnm/certificates

前の手順で生成した証明書を使用して、自己署名証明書を置き換えます。

1 nnm.keystore および nnm.truststore ファイルが存在する NNMi 管理サーバーのディレクトリに変更します。

- *Windows*: %NNM_DATA%¥shared¥nnm¥certificates
- *UNIX*: $NNM_DATA/shared/nnm/certificates

2 以下のコマンドを実行して、サーバー証明書およびCA証明書をNNMiのnnm.keystoreファイルにインポートします。

Windows:

- **%NnmInstallDir%¥nonOV¥jdk¥nnm¥bin¥keytool.exe -importcert -trustcacerts -keystore nnm.keystore -storepass nnmkeypass -alias** *myserver.mydomain* **-file myserver.crt**

UNIX:

- **$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -importcert -trustcacerts -keystore nnm.keystore -storepass nnmkeypass -alias** *myserver.mydomain* **-file myserver.crt**

-storepass オプションを使用し、パスワードを入力する場合、キーストア プログラムはキーストア パスワードの入力を要求しません。**-storepass** オプションを使用しない場合は、キーストア パスワードの入力を求められたときに **nnmkeypass** と入力してください。

3 証明書の信頼を確認するメッセージが表示されたら、**y** と入力します。

証明書をキーストアにインポートするときの出力例

このコマンドによる出力形式は以下のとおりです。

```
Owner: CN=NNMi_server.example.com
Issuer: CN=NNMi_server.example.com
Serial number: 494440748e5
Valid from: Tue Oct 28 10:16:21 MST 2008 until: Thu Oct 04
11:16:21 MDT 2108
Certificate fingerprints:
MD5:  29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
SHA1: C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03
Trust this certificate? [no]:  y
Certificate was added to keystore
```

4 以下のコマンドを実行して、CA 証明書を NNMi の nnm.truststore ファイルにインポートします。

— *Windows*:

%NnmInstallDir%¥nonOV¥jdk¥nnm¥bin¥keytool.exe -import -alias ***myca*** **-keystore nnm.truststore -file myca.crt**

— *UNIX*:

$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -import -alias ***myca*** **-keystore nnm.truststore -file myca.crt**

5 トラストストアのパスワードの入力を求められたら、**ovpass.** と入力します。

6 トラストストアの内容を確認します。

- *Windows*:
  %NnmInstallDir%¥nonOV¥jdk¥nnm¥bin¥keytool -list ¥
  -keystore nnm.truststore
- *UNIX*:
  $NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list ¥
  -keystore nnm.truststore

トラストストアのパスワードの入力を求められたら、**ovpass** と入力します。

トラストストアの出力例

トラストストアの出力形式は以下のとおりです。

```
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entry
nnmi_ldap, Nov 14, 2008, trustedCertEntry,
Certificate fingerprint (MD5):
29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
```

トラストストアには複数の証明書を含めることができます。

7 以下のファイルを編集します。

- *Windows*: `%NNM_CONF%¥nnm¥props¥nms-local.properties`
- *UNIX*: `$NNM_CONF/nnm/props/nms-local.properties`

8 `com.hp.ov.nms.ssl.KEY_ALIAS` 変数を、*myserver.mydomain* で使用した値に更新します。忘れずに設定内容を保存してください。

9 以下のコマンドを実行して `ovjboss` を再開始します。

a **ovstop ovjboss**

b **ovstart ovjboss**

10 構文 **https://<fully_qualified_domain_name>:<port_number>/nnm/** を使用して、NNMi コンソールへの HTTPS アクセスをテストします。ブラウザによって CA が信頼されると、NNMi コンソールへの HTTPS 接続が信頼されます。

自己署名証明書を使用するようにアプリケーション フェイルオーバーを設定する

図 2　アプリケーション フェイルオーバーでの自己署名証明書の使用法

アプリケーション フェイルオーバー機能を設定するときには、両方のノードの nnm.keystore *および* nnm.truststore *ファイルの内容をマージして、それぞれ 1 つの* nnm.keystore *および* nnm.truststore *ファイルにする必要があります。以下の手順を実行し、上の図に基づいてアプリケーション フェイルオーバー機能で自己署名証明書を使用するように設定します。*

NNMi でアプリケーション フェイルオーバー機能とともに自己署名証明書を使用する場合、以下の手順を完了しなければ、NNMi のプロセスがスタンバイ NNMi 管理サーバー (この例の Server Y) で正常に起動しません。

1 手順 2 を完了する前に、Server Y で以下のディレクトリに変更します。
   - *Windows*: %NNM_DATA%¥shared¥nnm¥certificates
   - *UNIX*: $NNM_DATA/shared/nnm/certificates
2 nnm.keystore および nnm.truststore ファイルを、Server Y から Server X の一時保存場所にコピーします。残りの手順では、これらのファイル保存場所は、**<*keystore*>** および <*truststore*> を指します。
3 Server X で以下のコマンドを実行し、Server Y の証明書を Server X の nnm.keystore および nnm.truststore ファイルにマージします。

   Windows:

   nnmcertmerge.ovpl -keystore <*keystore*> -truststore <*truststore*>

   UNIX:

   nnmcertmerge.ovpl -keystore <*keystore*> -truststore <*truststore*>
4 マージした nnm.keystore および nnm.truststore ファイルを server X から server Y にコピーし、どちらのノードにもマージ済みファイルがあるようにします。これらのファイル保存場所は、以下のとおりです。
   - *Windows*: %NNM_DATA%¥shared¥nnm¥certificates
   - *UNIX*: $NNM_DATA/shared/nnm/certificates
5 Server X と Server Y の両方で以下のコマンドを実行します。完全修飾ドメイン名を含め、両方のサーバーからの表示結果が一致することを確認します。一致しない場合は続行せずに、手順 1 から手順 7 までをやり直します。

   Windows:

   %NnmInstallDir%¥nonOV¥jdk¥nnm¥bin¥keytool.exe -list -keystore %NnmDataDir%¥shared¥nnm¥certificates¥nnm.keystore -storepass nnmkeypass

   UNIX:

   $ NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list -keystore $NnmDataDir/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass
6 Server X と Server Y の両方で以下のコマンドを実行します。完全修飾ドメイン名を含め、両方のサーバーからの表示結果が一致することを確認します。一致しない場合は続行せずに、手順 1 から手順 7 までをやり直します。

   Windows:

   %NnmInstallDir%¥nonOV¥jdk¥nnm¥bin¥keytool.exe -list -keystore %NnmDataDir%¥shared¥nnm¥certificates¥nnm.truststore -storepass ovpass

UNIX:

```
$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list -keystore
$NnmDataDir/shared/nnm/certificates/nnm.truststore
-storepass ovpass
```

7 271 ページの手順 6 から、アプリケーション フェイルオーバー機能の設定を続行します。

手順 4で以下の自動アクションを手動で実行しましたが、アプリケーションフェイルオーバー機能を実行すると、NNMi は、マージされたキーストアとトラストストアの情報を NNMi_active から NNM_standby へ自動的に複製します。

認証機関を使用するようにアプリケーション フェイルオーバーを設定する

図 3　アプリケーション フェイルオーバーでの CA 証明書の使用法

アプリケーション フェイルオーバー機能を設定するときには、両方のノードの nnm.keystore *および* nnm.truststore *ファイルの内容をマージして、それぞれ 1 つの* nnm.keystore *および* nnm.truststore *ファイルにする必要があります。*以下の手順に従い、上記図に基づき CA 証明書を使用するアプリケーション フェイルオーバー機能を設定します。

NNMi でアプリケーション フェイルオーバー機能とともに CA 証明書を使用する場合、以下の手順を完了しなければ、NNMi のプロセスがスタンバイ NNMi 管理サーバー (この例の Server Y) で正常に起動しません。

1 NNMi_standby については、121 ページの「認証機関証明書を生成する」の手順に従います。

2 手順 3 を完了する前に、Server Y で以下のディレクトリに変更します。

- *Windows*: %NNM_DATA%¥shared¥nnm¥certificates
- *UNIX*: $NNM_DATA/shared/nnm/certificates

3 nnm.keystore ファイルと nnm.truststore ファイルを Server Y から Server X の一時ファイル保管場所にコピーします。これ以降の手順では、これらのファイルの保管場所は **<*keystore*>** および <*truststore*> と呼びます。

4 Server X で以下のコマンドを実行し、Server Y の証明書を Server X の nnm.keystore および nnm.truststore ファイルにマージします。

Windows:

```
nnmcertmerge.ovpl -keystore <keystore> -truststore
<truststore>
```

UNIX:

```
nnmcertmerge.ovpl -keystore <keystore> -truststore
<truststore>
```

5 マージした nnm.keystore および nnm.truststore ファイルを server X から server Y にコピーし、どちらのノードにもマージ済みファイルがあるようにします。これらのファイル保存場所は、以下のとおりです。

- *Windows*: %NNM_DATA%¥shared¥nnm¥certificates
- *UNIX*: $NNM_DATA/shared/nnm/certificates

6 Server X と Server Y の両方で以下のコマンドを実行します。hp.com 完全修飾ドメイン名を含め、両方のサーバーからの表示結果が一致することを確認します。一致しない場合は続行せずに、手順 1 から手順 7 までをやり直します。

Windows:

```
%NnmInstallDir%¥nonOV¥jdk¥nnm¥bin¥keytool.exe -list
-keystore %NnmDataDir%¥shared¥nnm¥certificates¥nnm.keystore
-storepass nnmkeypass
```

UNIX:

```
$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list -keystore
$NnmDataDir/shared/nnm/certificates/nnm.keystore -storepass
nnmkeypass
```

7 Server X と Server Y の両方で以下のコマンドを実行します。hp.com 完全修飾ドメイン名を含め、両方のサーバーからの表示結果が一致することを確認します。一致しない場合は続行せずに、手順 1 から手順 7 までをやり直します。

Windows:

```
%NnmInstallDir%¥nonOV¥jdk¥nnm¥bin¥keytool.exe -list
-keystore
%NnmDataDir%¥shared¥nnm¥certificates¥nnm.truststore
-storepass ovpass
```

UNIX:

```
$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list -keystore
$NnmDataDir/shared/nnm/certificates/nnm.truststore
-storepass ovpass
```

8 271 ページの手順 6 から、アプリケーション フェイルオーバー機能の設定を続行します。

➤ 127 ページの手順 5 で以下の自動アクションを手動で実行しましたが、アプリケーションフェイルオーバー機能を実行すると、NNMi は、マージされたキーストアとトラストストア情報を Server X から Server Y へ自動的に複製します。

自己署名証明書または CA 証明書を使用するように高可用性を設定する

図 4　HA での証明書の使用法

自己署名証明書を使用するように高可用性を設定する

NNMi HA を正しく設定するプロセスでは、プライマリ ノードとセカンダリ ノードの間で自己署名証明書を共有します。HA 下で実行される NNMi でデフォルトの証明書を使用するために、追加の手順を実行する必要はありません。

新規証明書を使用するように高可用性を設定する

新規の自己署名証明書または CA 証明書を作成し、newcert と呼ぶとします。以下の手順を実行して、この新規の CA 証明書または自己署名証明書を使用するように HA を設定します。

この手順は、305 ページの「HA の設定」での説明に従って、NNMi に HA を設定する前または後に実行できます。

1. 手順 2 を完了する前に、NNMi_HA1 で以下のディレクトリに変更します。
   - *Windows*: %NNM_DATA%¥shared¥nnm¥certificates
   - *UNIX*: $NNM_DATA/shared/nnm/certificates
2. NNMi_HA1 で、以下のコマンドを実行して newcert を nnm.keystore ファイルにインポートします。
   - *Windows*: **%NnmInstallDir%¥nonOV¥jdk¥nnm¥bin¥keytool -import -alias *newcert_Alias* -keystore nnm.keystore -file newcert**
   - *UNIX*: **$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -import -alias *newcert_Alias* -keystore nnm.keystore -file newcert**
3. アクティブ ノード (NNMi_HA1) とスタンバイ ノード (NNMi_HA2) の両方で以下のファイルを編集します。
   - *Windows*: %NNM_DATA%¥conf¥nnm¥props¥nms-local.properties
   - *UNIX*: $NNM_DATA/conf/nnm/props/nms-local.properties
4. NNMi_HA1 と NNMi_HA2 の両方の nms-local.properties ファイルで、以下の行を変更します。

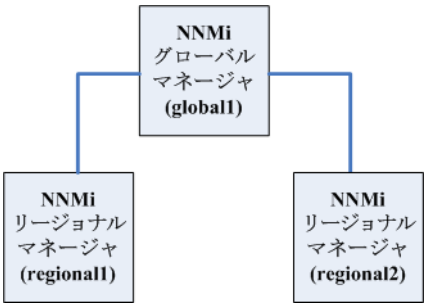
   com.hp.ov.nms.ssl.KEY_ALIAS = newcert_Alias
5. 変更を保存します。

自己署名証明書を使用するようにグローバル ネットワーク管理機能を設定する

NNMi のインストール時には、インストール スクリプトによって NNMi 管理サーバー の自己署名証明書が作成されます。この証明書には、ノードの完全修飾ドメイン名を含む別名が記録されています。インストール スクリプトは、この自己署名証明書を NNMi 管理サーバー の nnm.keystore および nnm.truststore ファイルに追加します。

グローバル ネットワーク管理設定で図 5 のモデルを実現するとします。

図 5　　グローバル ネットワーク管理



以下の手順を実行し、図 5 に基づいて自己署名証明書を使用するようにグローバル ネットワーク管理機能を設定します。

1. 手順 2 を完了する前に、regional1 および regional2 で以下のディレクトリに変更します。
   - *Windows*: %NNM_DATA%¥shared¥nnm¥certificates
   - *UNIX*: $NNM_DATA/shared/nnm/certificates
2. nnm.truststore ファイルを、上記の regional1 および regional2 の場所から、global1 の任意の一時保管場所にコピーします。
3. global1 で以下のコマンドを実行し、regional1 および regional2 の証明書を global1 の nnm.truststore ファイルにマージします。

   Windows:

   a. **nnmcertmerge.ovpl -truststore *regional1_nnm.truststore_location***
   b. **nnmcertmerge.ovpl -truststore *regional2_nnm.truststore_location***

   UNIX

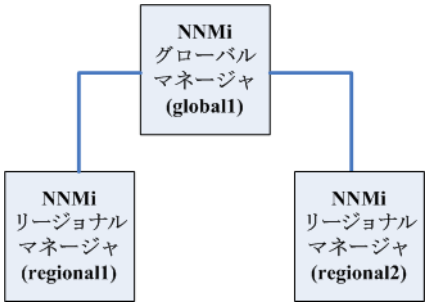
   a. **nnmcertmerge.ovpl -truststore *regional1_nnm.truststore_location***
   b. **nnmcertmerge.ovpl -truststore *regional2_nnm.truststore_location***
4. global1 で、以下のコマンドを以下の順序で実行します。
   a. **ovstop ovjboss**
   b. **ovstart ovjboss**

認証機関を使用するようにグローバル ネットワーク管理機能を設定する

NNMi のインストール時には、インストール スクリプトによって NNMi 管理サーバー の自己署名証明書が作成されます。この証明書には、ノードの完全修飾ドメイン名を含む別名が記録されています。インストール スクリプトは、この自己署名証明書を NNMi 管理サーバー の nnm.keystore および nnm.truststore ファイルに追加します。

グローバル ネットワーク管理設定で図 6 のモデルを実現するとします。

図 6　グローバル ネットワーク管理での証明書の使用法



1. regional1 および regional2 については、121 ページの「認証機関証明書を生成する」の手順に従います。
2. regional1 および regional2 の以下のディレクトリを変更してから、手順を実行します手順 3。
   - *Windows*: %NNM_DATA%¥shared¥nnm¥certificates
   - *UNIX*: $NNM_DATA/shared/nnm/certificates
3. nnm.truststore ファイルを、上記の regional1 および regional2 の場所から、global1 の任意の一時保管場所にコピーします。
4. global1 で以下のコマンドを実行し、regional1 および regional2 の証明書を global1 の nnm.truststore ファイルにマージします。

   Windows:

   a. **nnmcertmerge.ovpl -truststore *regional1_nnm.truststore_location***

   b. **nnmcertmerge.ovpl -truststore *regional2_nnm.truststore_location***

   UNIX

   a. **nnmcertmerge.ovpl -truststore *regional1_nnm.truststore_location***

   b. **nnmcertmerge.ovpl -truststore *regional2_nnm.truststore_location***
5. global1 で、以下のコマンドを以下の順序で実行します。

   a. **ovstop ovjboss**

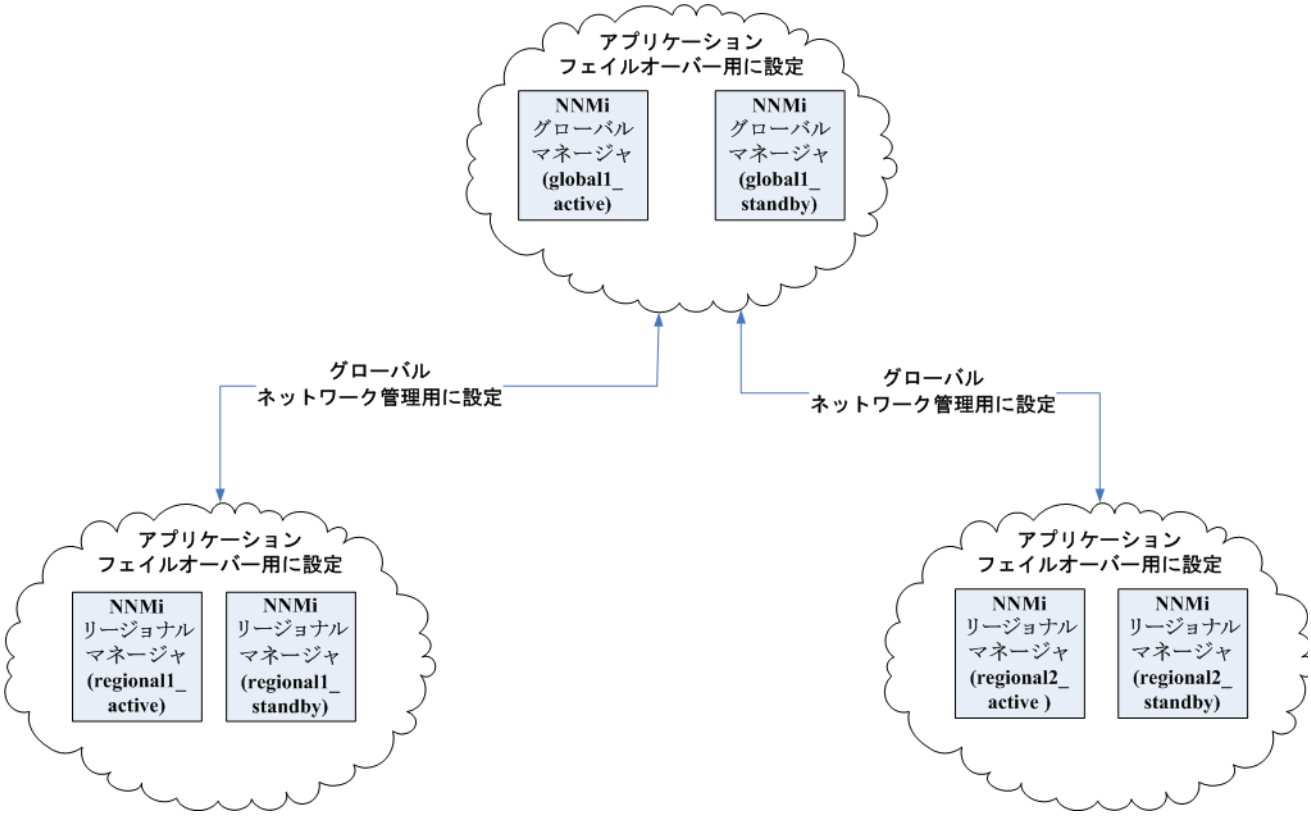
   b. **ovstart ovjboss**

自己署名証明書を使用するようにアプリケーション フェイルオーバーが有効なグローバル ネットワーク管理を設定する

上の説明にあるように、NNMi のインストール時には、インストール スクリプトによって NNMi 管理サーバーの自己署名証明書が作成されます。この証明書には、ノードの完全修飾ドメイン名を含む別名が記録されています。インストール スクリプトは、この自己署名証明書を NNMi 管理サーバー の nnm.keystore および nnm.truststore ファイルに追加します。

グローバル ネットワーク管理設定で、図 7 に示すアプリケーション フェイルオーバー機能のモデルを実現するとします。

図 7　　アプリケーション フェイルオーバーが有効なグローバル ネットワーク管理



以下の手順を実行し、上の図に基づいてアプリケーション フェイルオーバーが有効なグローバル ネットワーク管理機能を設定します。

1. 上の図に示すアプリケーション フェイルオーバー クラスタごとに、124 ページの「自己署名証明書を使用するようにアプリケーション フェイルオーバーを設定する」に示す指示に従ってください。
2. 268 ページの「アプリケーション フェイルオーバーの基本セットアップ」の指示に従ってアプリケーション フェイルオーバーを設定します。
3. 129 ページの「自己署名証明書を使用するようにグローバル ネットワーク管理機能を設定する」に示す regional1_active and regional2_active に関する指示に従ってください。

ディレクトリ サービスへの SSL 接続を設定する

デフォルトでは、ディレクトリ サービス通信を有効にすると、NNMi は、ディレクトリ サービスからデータを取得するときに LDAP プロトコルを使用します。ディレクトリ サービスで SSL 接続が必要な場合は、SSL プロトコルを有効にして、NNMi とディレクトリ サービスの間を流れるデータを暗号化する必要があります。

SSL では、ディレクトリ サービス ホストと NNMi 管理サーバーの間で信頼関係を確立する必要があります。この信頼関係を確立するには、証明書を NNMi トラストストアに追加します。証明書は、ディレクトリ サービス ホストの識別情報を NNMi 管理サーバーに示すものです。

SSL 通信用のトラストストア証明書をインストールするには、以下の手順を実行します。

1. ディレクトリ サーバーから会社のトラストストア証明書を取得します。ディレクトリ サービス管理者からこの証明書のテキスト ファイルのコピーを入手できます。
2. NNMi トラストストアが格納されているディレクトリに変更します。
   - *Windows*: `%NNM_DATA%¥shared¥nnm¥certificates`
   - *UNIX*: `$NNM_DATA/shared/nnm/certificates`

   `certificates` ディレクトリから、この手順のコマンドすべてを実行します。
3. 会社のトラストストア証明書を NNMi トラストストアにインポートします。
   a. 以下のコマンドを実行します。
      — *Windows*:
      ```
      %NnmInstallDir%¥nonOV¥jdk¥b¥bin¥keytool -import
      -alias nnmi_ldap -keystore nnm.truststore
      -file <Directory_Server_Certificate.txt>
      ```
      — *UNIX*:
      ```
      $NnmInstallDir/nonOV/jdk/b/bin/keytool -import ¥
      -alias nnmi_ldap -keystore nnm.truststore ¥
      -file <Directory_Server_Certificate.txt>
      ```
      <Directory_Server_Certificate.txt> は、会社のトラストストア証明書です。
   b. キーストアのパスワードの入力を求められたら、**ovpass** と入力します。
   c. 証明書の信頼を確認するメッセージが表示されたら、**y** と入力します。

      このコマンドによる出力形式は以下のとおりです。

証明書をトラストストアにインポートするときの出力例

```
Owner: CN=NNMi_server.example.com
Issuer: CN=NNMi_server.example.com
シリアル番号 : 494440748e5
Valid from: Tue Oct 28 10:16:21 MST 2008 until: Thu Oct 04
11:16:21 MDT 2108
Certificate fingerprints:
MD5:  29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
SHA1: C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03
Trust this certificate? [no]:  y
Certificate was added to keystore
```

4 トラストストアの内容を確認します。

- *Windows*:
  %NnmInstallDir%¥nonOV¥jdk¥b¥bin¥keytool.exe -list -keystore nnm.truststore
- *UNIX*:
  $NnmInstallDir/nonOV/jdk/b/bin/keytool -list -keystore nnm.truststore

キーストアのパスワードの入力を求められたら、**ovpass** と入力します。

トラストストアの出力例

トラストストアの出力形式は以下のとおりです。

```
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entry
nnmi_ldap, Nov 14, 2008, trustedCertEntry,
Certificate fingerprint (MD5):
29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
```

トラストストアには複数の証明書を含めることができます。

5 以下のコマンドを実行して ovjboss を再開始します。

a **ovstop ovjboss**

b **ovstart ovjboss**

keytool コマンドの詳細については、**http://www.oracle.com/technetwork/java/index.html** で「鍵および証明書管理ツール」を検索してください。

HP BSM バージョン 9.xx への SSL 接続の設定

HP 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¥b¥bin¥keytool.exe -export -alias *hostname*.selfsigned -file C:¥temp¥cert -keystore %NnmDataDir%¥shared¥nnm¥certificates¥nnm.keystore -storepass nnmkeypass
- *UNIX*:
  $NnmInstallDir/nonOV/jdk/b/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 以下のコマンドを実行します。**keytool.exe -import -keystore *<directory>*:¥HPBSM¥odb¥conf¥security¥server.keystore -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
```

7 次のように、手順 6 に示されているコマンドの server.truststore を server.keystore で置き換えて実行します。**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 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 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?」と尋ねられたら、必ず「yes」と回答してください。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 9.01 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 9.01 キートストア証明書は <*directory*>:¥keystore ファイルに保存されます。

c truststore 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、残りのコマンドで、NNMi 管理サーバーの *<directory>*:¥temp¥keystore、*<directory>*:¥temp¥truststore、/*tmp*/keystore and /tmp/truststore の各保存場所に存在するものとして示します。

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 -import -alias hpcert -keystore %NnmDataDir%¥shared¥nnm¥certificates¥nnm.keystore -storepass nnmkeypass -file *<directory>*:¥temp¥keystore

— *UNIX*:
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 -import -alias clientcert -keystore %NnmDataDir%¥shared¥nnm¥certificates¥nnm.truststore -storepass ovpass -file *<directory>:*/temp/truststore

— *UNIX*:
keytool -import -alias clientcert -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass -file
/tmp**/truststore**

11 *オプション*: 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 *オプション*: 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**

— *UNIX*: **keytool -list -keystore $NnmDataDir/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass**

- *BSM サーバー*: **keytool.exe -list -keystore *<directory>*:¥HPBSM¥odb¥conf¥security¥server.keystore -storepass hppass**

13 *オプション*: 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*:
  - *Windows*: **keytool.exe -list -keystore %NnmDataDir%¥shared¥nnm¥certificates¥nnm.truststore -storepass ovpass**
  - *UNIX*: **keytool -list -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass**
- *BSM サーバー*: **keytool.exe -list -keystore *<directory>*:¥HPBSM¥odb¥conf¥security¥server.truststore -storepass hppass**

NNMi とシングル サインオンの使用

HP Network Node Manager i Software (NNMi) シングル サインオン (SSO) を設定すると、NNMi コンソールから簡単に NNM iSPI にアクセスできるようになります。SSO を使用して NNMi コンソールにログオンすれば、NNM iSPI や他の HP アプリケーションにアクセスできます。再度ログインする必要はありません。SSO は、安全なアクセス レベルを維持しながら、より簡単に NNM iSPI や他の HP アプリケーションにアクセスできるようにする機能です。NNMi コンソールからサインアウト (または NNMi コンソール セッションがタイムアウト) した後に NNMi コンソールとは異なる NNM iSPI や他のアプリケーションの URL にアクセスするには、サインイン資格証明を再入力する必要があります。

インストール中に SSO は無効になっています。SSO が有効になっていても、ある NNMi 管理サーバーから別の NNMi 管理サーバーへと参照すると、最初の NNMi 管理サーバーからログアウトされ、利益はほとんどありません。これが起こらないようにするために、SSO は無効に初期設定されており、この章で説明されているように、NNMi 管理サーバー間で `initString` パラメータと `protectedDomains` パラメータの設定を調整できます。

この章には、以下のトピックがあります。

- 140 ページの「NNMi への SSO アクセス」
- 141 ページの「1 つのドメインに対する SSO の有効化」
- 141 ページの「異なるドメインに配置されている NNMi 管理サーバーに対する SSO の有効化」
- 142 ページの「NNMi と NNM iSPI の SSO アクセス」
- 143 ページの「NNMi と HP BSM または HP BAC 間のシングル サインオンの設定」
- 144 ページの「NNMi と HP UCMDB 間のシングル サインオンの設定」
- 145 ページの「NNMi と HP NA 間のシングル サインオンの設定」
- 148 ページの「SSO の無効化」
- 148 ページの「SSO セキュリティに関する注意」

NNMi への SSO アクセス

複数の NNMi 管理サーバー間を移動するには、以下のいずれかを実行します。

- nms-ui.properties ファイルを編集して、com.hp.nms.ui.sso.initString と com.hp.nms.ui.sso.protectedDomains のパラメータ値を NNMi 管理サーバー間で同じ値にします。com.hp.nms.ui.sso.domain パラメータを、NNMi 管理サーバーが配置されているドメインと一致するように設定してください。
  - NNMi 管理サーバーを 1 つのネットワークドメインにしか配置していない場合は、141 ページの「1 つのドメインに対する SSO の有効化」の説明に従ってください。
  - NNMi 管理サーバーを複数のネットワークドメインに配置している場合、詳細については、141 ページの「異なるドメインに配置されている NNMi 管理サーバーに対する SSO の有効化」の説明に従ってください。
- nms-ui.properties file を編集し、SSO が無効になっていることを確認します。詳細については、148 ページの「SSO の無効化」を参照してください。

これらのアクションのいずれかが完了していないと、別の NNMi 管理サーバーに移動するたびに、直前の NNMi 管理サーバーから自動的にサインアウトします。

SSO と NNMi グローバル ネットワーク管理機能を併用する場合、特別な考慮事項があります。詳細については、223 ページの「SSO およびアクション メニュー」および 223 ページの「グローバル ネットワーク管理用にシングル サインオンを設定する」を参照してください。

NNMi 管理サーバーのドメイン名が mycompany のように短く、ドット (.) がない場合、NNMi コンソールによりただちにサインアウトされます。SSO ブラウザ クッキーの制限には、mycompany.com のように、ドット (.) が少なくとも 1 つ付いているドメイン名が必要です。この状況を解決するには、以下の手順を実行します。

1. 以下のファイルをテキスト エディタで開きます。
   - *Windows*: %NNM_PROPS%/nms-ui.properties
   - *UNIX*: $NNM_PROPS/nms-ui.properties
2. この例では、以下の文字列を検索します。

   com.hp.nms.ui.sso.domain = mycompany

   これを以下の文字列で置き換えます。

   com.hp.nms.ui.sso.domain = mycompany.com
3. 以下のコマンドを実行し、変更をコミットします。

   nnmsso.ovpl -reload

1 つのドメインに対する SSO の有効化

1 つのドメインで SSO を使用可能にするには、以下の手順を実行します。

1 以下のファイルを編集します。
   - *Windows*: `%NNM_PROPS%¥nms-ui.properties`
   - *UNIX*: `$NNM_PROPS/nms-ui.properties`
2 ファイルから、以下のようなセクションを見つけます。

   `com.hp.nms.ui.sso.isEnabled = false`

   これを以下のように変更します。

   `com.hp.nms.ui.sso.isEnabled = true`
3 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.domain = mycompany.com`

   mycompany.com を、NNMi 管理サーバーが配置されているドメインに変更します。1 つのドメインで SSO を有効にするときは、1 つのドメインのみがリストされていることを確認してください。
4 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.protectedDomains = mycompany.com`

   mycompany.com を、NNMi 管理サーバーが配置されているドメインに変更します。1 つの保護ドメインで SSO を有効にするときは、1 つの保護ドメインのみがリストされていることを確認してください。
5 以下のコマンドを実行し、変更をコミットします。

   `nnmsso.ovpl -reload`

異なるドメインに配置されている NNMi 管理サーバーに対する SSO の有効化

SSO を使用できるように複数の NNMi 管理サーバーを設定できます。この例では、異なるドメインに配置されている 3 つの NNMi 管理サーバーに対して SSO を設定する方法を説明します。SSO を使用できるように複数の NNMi 管理サーバーを設定する必要がある場合に、これらのシステムが異なるドメインに配置されているときは、以下の手順を実行します。

1 以下のファイルを編集します。
   - *Windows*: `%NNM_PROPS%¥nms-ui.properties`
   - *UNIX*: `$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 = false`

   これを以下のように変更します。

   `com.hp.nms.ui.sso.isEnabled = true`
3 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.domain = group1.mycompany.com`

ドメイン名に 1 つ以上のドット (.) があることを確認します。

4 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.protectedDomains=group1.mycompany.com
```

これを以下のように変更します。

```
com.hp.nms.ui.sso.protectedDomains=group1.mycompany.com,
group2.yourcompany.com, group3.yourcompany.com
```

5 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.initString = Initialization String
```

1 つの SSO 設定で機能するように各 NNMi 管理サーバーの初期化ストリングを共有する必要があります。SSO 設定に含まれるすべての NNMi 管理サーバーの初期化ストリングを同じ値に変更します。

6 以下のコマンドを実行し、変更をコミットします。

```
nnmsso.ovpl -reload
```

7 手順 1 から手順 6 までをさらに 2 回繰り返し、残りの 2 つの NNMi 管理サーバーを設定します。残りの各 NNMi 管理サーバーについては、手順 3 で、 *group2* または *group3* を *group1* に置き換えてください。

NNMi と NNM iSPI の SSO アクセス

NNMi と NNM iSPI 間の SSO には `initString` 設定は必要*ありません*。

SSO を使用するには、以下のように NNMi にアクセスします。

- 以下の形式の正しい URL を使用します。
  <protocol>://<fully_qualified_domain_name>:<port_number>/nnm/
  <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、NNMi コンソールに接続するためのポートです。これは、NNMi のインストール時に割り当てられ、以下のファイルで指定されます。
  - *Windows*: `%NnmDataDir%¥conf¥nnm¥props¥nms-local.properties`
  - *UNIX*: `$NnmDataDir/conf/nnm/props/nms-local.properties`
- 有効なアカウントを使用して NNMi にログオンします。

SSO が機能するには、NNMi と NNM iSPI への URL アクセスに共通するネットワークドメイン名が使用されている必要があります。さらに、IP アドレスが含まれていない URL である必要があります。NNMi 管理サーバー用の FQDN がない場合は、代わりに NNMi 管理サーバーの IP アドレスを使用できますが、その場合、NNM iSPI のシングルサインオンが無効になるため、次回 NNM iSPI にアクセスするときにもう一度ログオンする必要があります。

NNMi 管理サーバー の正式な FQDN を判別するには、以下のいずれかの方法を使用します。

- **`nnmofficialfqdn.ovpl`** コマンドを使用して、インストール中に設定した正式な FQDN の値を表示します。詳細については、*nnmofficialfqdn.ovpl* リファレンス ページまたは UNIX のマンページを参照してください。
- NNMi コンソールで、**[ヘルプ] > [システム情報]** をクリックします。**[サーバー]** タブで、正式な FQDN ステートメントを特定します。

インストール中に設定された正式な FQDN を変更する必要がある場合は、**nnmsetofficialfqdn.ovpl** コマンドを使用します。詳細については、*nnmsetofficialfqdn.ovpl* リファレンス ページまたは UNIX のマンページを参照してください。

インストール後、システム アカウントは有効なままになっています。システム アカウントは、コマンドラインのセキュリティと復旧の目的のみに使用します。

NNM iSPI への SSO には、ユーザーが正式な FQDN を含む URL で NNMi コンソールにアクセスすることが要求されます。IP アドレスや短縮されたドメイン名など、正式ではないドメイン名を使用して NNMi コンソールにアクセスした場合に NNMi URL を正式な FQDN にリダイレクトするように NNMi を設定できます。URL をリダイレクトするように NNMi を設定する前に、該当する正式な FQDN が設定されている必要があります。詳細については、NNMi ヘルプを参照してください。

NNMi で URL へのリダイレクトを可能にした後、以下の点に注意してください。

- アクセスする NNMi 管理サーバーに適したホスト名を使用して、NNMi コンソールにログオンできます。たとえば、ユーザーが http://localhost/nnm を要求している場合、NNMi は http://host.mydomain.com/nnm などの URL にそれをリダイレクトします。
- http://host.mydomain.com/nnm を使用して NNMi コンソールにアクセスできない場合、以下の URL を使用して、NNMi コンソールに直接アクセスしてください。
  <protocol>:**//**
  <fully_qualified_domain_name>:***<port_number>***launch?cmd=showMain.**
  <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、NNMi コンソールに接続するためのポートです。これは、NNMi のインストール時に割り当てられ、以下のファイルで指定されます。
  - *Windows*: `%NnmDataDir%¥conf¥nnm¥props¥nms-local.properties`
  - *UNIX*: `$NnmDataDir/conf/nnm/props/nms-local.properties`

NNMi と HP BSM または HP BAC 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、NNMi と HP Business Service Management (BSM) または HP Business Availability Center (BAC) 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、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 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、BSM または BAC では通常の権限、NNMi では管理者権限を有する場合があります。

BSM または BAC 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。

BSM または BAC 初期化ストリング

以下のようにして、BSM または BAC 初期化ストリングを特定します。

1 BSM または BAC 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_BAC_hostname*>:<*BSM_BAC_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** パラメータの値です。

3 **InitString** パラメータ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 エディタで開きます。

- *Windows*: `%NNM_PROPS%¥nms-ui.properties`
- *UNIX*: `$NNM_PROPS/nms-ui.properties`

2 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
```

3 手順 2 に示されている `initString` パラメータ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。

```
nnmsso.ovpl -reload
```

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、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、UCMDB にログオンすることなく 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。NNMi と UCMDB 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、NNMi では通常の権限、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** パラメータの値です。

3 **InitString** パラメータ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 エディタで開きます。

- *Windows*: `%NNM_PROPS%¥nms-ui.properties`
- *UNIX*: `$NNM_PROPS/nms-ui.properties`

2 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
```

3 `initString` パラメータ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。

```
nnmsso.ovpl -reload
```

NNMi と HP NA 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、NNMi と HP Network Automation (NA) 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、NA にログオンすることなく NA ページを表示できます。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。NNMi と NA 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、NNMi ではオペレータ レベル 1 の権限、NA では管理者権限を有する場合があります。

NNMi から NA 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

NNMi 管理サーバーで、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 エディタで開きます。

- *Windows*: `%NNM_PROPS%¥nms-ui.properties`
- *UNIX*: `$NNM_PROPS/nms-ui.properties`

2 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
```

3 initString パラメータ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。

```
nnmsso.ovpl -reload
```

NA 初期化ストリング

NA サーバーで、以下のようにして NA 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 エディタで開きます。

- *Windows*: %NA_HOME%¥server¥ext¥jboss¥server¥default¥conf¥lwssofmconf.xml
- *UNIX*: $NA_HOME/server/ext/jboss/server/default/conf/lwssofmconf.xml

NA_HOME 環境変数のデフォルト値は以下のとおりです。

- *Windows*: C:/na
- *UNIX*: /opt/NA

2 enableLWSSO タグで、enableLWSSOFramework 属性を true に設定します。

```
enableLWSSOFramework="true"
```

3 lwssoValidation ブロックで、以下を実行します。

- domain タグの値を NA サーバーの完全ドメイン名に設定します。たとえば、NA サーバーのホスト名が na.location.example.com の場合、<domain>location.example.com</domain> に設定します。

  この手順では、NNMi 管理サーバーが NA サーバーと同じドメインにあることを想定しています。同じドメインにない場合、NNMi 管理サーバーのドメインの DNSDomain エレメントを trustedHosts ブロックに追加する必要があります。

- crypto タグで、initString 属性を NNMi nms-ui.properties ファイルの initString プロパティの値に設定します。

  crypto ブロック内の設定は、SSO を使用するすべてのアプリケーションで同一である必要があります。

4 trustedHosts ブロックで、DNSDomain タグを lwssoValidation ブロックの domain タグの値に設定します。たとえば、以下のようになります。

```
<DNSDomain>location.example.com</DNSDomain>
```

この手順では、NNMi 管理サーバーが NA サーバーと同じドメインにあることを想定しています。NA サーバーが、NNMi 管理サーバーとは異なるドメインにある場合、両方のドメインに DNSDomain エントリを追加します。

5 SSO を使用するすべてのアプリケーションが、最大 15 分の差異の範囲で GMT (グリニッジ標準時) 時間に設定されていることを確認してください。これらのアプリケーションのタイムゾーンは異なる場合がありますが、GMT に変換すると同じになります。

6 NA jboss サーバーを再起動します。

- *Windows*: NA ユーザー インタフェースの **[管理者] > [サービスの開始 / 停止]** ページで、管理エンジンを再起動します。
- *UNIX*: 以下のコマンドを実行します。

```
/etc/init.d/truecontrol restart
```

SSO の無効化

SSO を無効にする必要がある場合は、以下の手順を実行します。

1 以下のファイルを編集します。

- *Windows*: `%NNM_PROPS%¥nms-ui.properties`
- *UNIX*: `$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 = true
```

これを以下のように変更します。

com.hp.nms.ui.sso.isEnabled = false

3 以下のコマンドを実行し、変更をコミットします。

```
nnmsso.ovpl -reload
```

SSO セキュリティに関する注意

1 SSO セキュリティの機密 `initString` パラメータ。

SSO は、*対象鍵暗号方式*を使用して SSO トークンの検証と作成を行います。設定内の `initString` パラメータは、秘密鍵の初期化に使用されます。アプリケーションはトークンを作成し、`initString` パラメータを使用する各アプリケーションはそのトークンを検証します。

以下は、非常に重要な情報です。

— `initString` パラメータを設定せずに、SSO を使用することはできません。

— `initString` パラメータは機密情報であり、公開、移動、永続性において、機密情報として取り扱う必要があります。

— 相互に統合するアプリケーションは、SSO を使用して `initString` を共有できます。

— `initString` は最低 12 文字の長さです。

2 特に必要でない限り、SSO を無効にします。

3 最も弱い認証フレームワークを使用するアプリケーションやほかの統合アプリケーションに信頼される SSO トークンを発行するアプリケーションは、すべてのアプリケーションの認証セキュリティ レベルを判断します。

HP は、強力で安全な認証フレームワークを使用するアプリケーションのみが SSO トークンを発行するように設定することを推奨します。

4 対象鍵暗号方式による影響について

SSO は、SSO トークンの発行と検証に対象鍵暗号方式を使用します。そのため、SSO を使用するアプリケーションは、同一の `initString` を共有しているその他のすべてのアプリケーションによって信頼されるトークンを発行できます。

`initString` を共有するアプリケーションが信頼されない場所にある、または信頼できない場所にアクセスできる場合に、この潜在的なリスクが浮上します。

5 ユーザーロール

SSO では、統合されたアプリケーション間でユーザーロールは共有されません。このため、統合されたアプリケーションはユーザーロールを監視する必要があります。HP は、すべての統合アプリケーションで、同一のユーザー レジストリ (LDAP/AD として) を共有することを推奨します。

ユーザーロールを管理できないと、セキュリティ違反やアプリケーション エラーが発生する場合があります。たとえば、複数のアプリケーションで異なるロールに同じユーザー名が割り当てられることがあります。

ユーザーがアプリケーション A にログオンし、コンテナやアプリケーション認証を使用するアプリケーション B にアクセスするとします。ユーザーロールを管理できないと、そのユーザーはアプリケーション B に手動でログオンし、ユーザー名を入力しなければならなくなります。このとき、ユーザーがアプリケーション A とは異なるユーザー名を入力すると、その後に、アプリケーション A または B から 3 つ目のアプリケーション (アプリケーション C) にアクセスすると、アプリケーション A または B に使用したユーザー名でアプリケーション C にアクセスするという予期しない動作が発生することになります。

6 認証に Identity Manager が使用される

Identity Manager 内の保護されていないすべてのリソースは、SSO 設定に非セキュア URL 設定として設定されている必要があります。

7 SSO デモ モード

— デモの目的のみに SSO デモ モードを使用します。

— セキュアでないネットワークでのみデモ モードを使用します。

— デモ モードを本番に使用しないでください。デモ モードと本番モードを混ぜて使用しないでください。

NNMi で使用する Telnet および SSH プロトコルを設定する

[アクション] > [Telnet... (クライアントから)] メニュー項目によって、選択したノードに対する telnet コマンドが呼び出されます (NNMi コンソールを現在実行中の Web ブラウザから)。**[アクション] > [Secure Shell... (クライアントから)]** メニュー項目によって、選択したノードに対する secure shell (SSH) コマンドが呼び出されます (NNMi コンソールを現在実行中の Web ブラウザから)。デフォルトでは、Microsoft Internet Explorer と Mozilla Firefox のどちらでも telnet コマンドや SSH コマンドは定義されていないため、どちらのメニュー項目を使用する場合でもエラー メッセージが生成されます。telnet、SSH、または両方のプロトコルを各 NNMi ユーザーに設定して (システムごとに)、NNMi コンソール メニュー項目を変更できます。

この章には、以下のトピックがあります。

- 151 ページの「Telnet または SSH メニュー項目の無効化」
- 152 ページの「Windows 上のブラウザへの Telnet または SSH クライアントの設定」
- 158 ページの「Linux で Telnet または SSH を使用する Firefox の設定」
- 160 ページの「Windows レジストリを変更するファイル例」

Telnet または SSH メニュー項目の無効化

導入環境の NNMi ユーザーが、NNMi コンソールから telnet または SSH 接続する必要がない場合は、それぞれのメニュー項目を無効化して NNMi コンソールから削除できます。

NNMi コンソールのメニュー項目の無効化は、NNMi 管理サーバー上で NNMi コンソールにログオンするすべてのユーザーに適用されます。**[Telnet]** または **[Secure Shell]** メニュー項目を無効にするには、以下の手順を実行します。

1. **[設定]** ワークスペースで **[ユーザー インタフェース]** を展開して、**[メニュー項目]** を選択します。
2. **[メニュー項目]** ビューで、**[Telnet... (クライアントから)]** 行または **[Secure Shell... (クライアントから)]** 行を選択して、**[開く]** をクリックします。

3 **[メニュー項目]** フォームで、**[有効にする]** チェックボックスをオフにしてから、**[作成者]** フィールドを適切な値に設定します。

作成者値を変更すると、このメニュー項目は NNMi をアップグレードしても無効化されたままです。

4 フォームを保存し、閉じます。

詳細については、NNMi ヘルプの「*アクション メニューの制御*」を参照してください。

Windows 上のブラウザへの Telnet または SSH クライアントの設定

NNMi ユーザーの Web ブラウザにオペレーティング システム提供の telnet コマンドを設定します。この手順は、**[アクション] > [Telnet... (クライアントから)]** メニュー項目を実行する必要がある NNMi ユーザーの各コンピュータおよび Web ブラウザで実行する必要があります。

NNMi ユーザーの Web ブラウザにサードパーティの ssh コマンドを設定します。この手順は、**[アクション] > [Secure Shell... (クライアントから)]** メニュー項目を実行する必要がある NNMi ユーザーの各コンピュータおよび Web ブラウザで実行する必要があります。

このセクションの手順を完了するには、コンピュータの管理権限が必要です。特定の手順は、ブラウザおよびオペレーティング システムのバージョン (32 ビットまたは 64 ビット) によって異なります。

Internet Explorer のバージョンを確認するには、**[ヘルプ]> [Internet Explorer のバージョン情報]** をクリックします。バージョン情報にテキスト **[64 ビット版]** が含まれない場合、この Internet Explorer は 32 ビットです。

Firefox は 32 ビット バージョンでのみ使用可能です。

表 6 は、各ブラウザとオペレーティング システムの組み合わせで使用する手順を示したものです。

表 6　Windows での Telnet および SSH 設定手順のマトリクス

Web ブラウザ	Windows オペレーティング システム アーキテクチャ	適用手順
Internet Explorer 32 ビット	32 ビット	• 153 ページの「Windows オペレーティング システム提供の Telnet クライアント」 • 155 ページの「サードパーティ Telnet クライアント (標準 Windows)」 • 157 ページの「サードパーティ SSH クライアント (標準 Windows および Windows 上のウィンドウ)」
	64 ビット Windows 7	• 155 ページの「サードパーティ Telnet クライアント (標準 Windows)」 • 157 ページの「サードパーティ SSH クライアント (標準 Windows および Windows 上のウィンドウ)」
	64 ビット Windows 7 以外	• 156 ページの「サードパーティ Telnet クライアント (Windows 上のウィンドウ)」 • 157 ページの「サードパーティ SSH クライアント (標準 Windows および Windows 上のウィンドウ)」

表 6　Windows での Telnet および SSH 設定手順のマトリクス (続く)

Web ブラウザ	Windows オペレーティング システム アーキテクチャ	適用手順
Internet Explorer 64 ビット	64 ビット	• 153 ページの「Windows オペレーティング システム提供の Telnet クライアント」 • 155 ページの「サードパーティ Telnet クライアント (標準 Windows)」 • 157 ページの「サードパーティ SSH クライアント (標準 Windows および Windows 上のウィンドウ)」
Firefox	32 ビット	• 153 ページの「Windows オペレーティング システム提供の Telnet クライアント」 • 155 ページの「サードパーティ Telnet クライアント (標準 Windows)」 • 157 ページの「サードパーティ SSH クライアント (標準 Windows および Windows 上のウィンドウ)」
	64 ビット Windows 7	• 155 ページの「サードパーティ Telnet クライアント (標準 Windows)」 • 157 ページの「サードパーティ SSH クライアント (標準 Windows および Windows 上のウィンドウ)」
	64 ビット Windows 7 以外	• 156 ページの「サードパーティ Telnet クライアント (Windows 上のウィンドウ)」 • 157 ページの「サードパーティ SSH クライアント (標準 Windows および Windows 上のウィンドウ)」

このセクションのタスクの多くでは Windows レジストリの編集が必要です。レジストリを直接編集せずにシステム上で各ユーザーが実行できる .reg ファイルを作成できます。.reg ファイルの例は、160 ページの「Windows レジストリを変更するファイル例」を参照してください。

このセクションで説明するタスクの詳細については、以下の Microsoft の記事を参照してください。

- Microsoft 提供の telnet クライアントをインストールする
  http://technet.microsoft.com/en-us/library/cc771275%28WS.10%29.aspx
- Windows レジストリの概要
  http://support.microsoft.com/kb/256986
- Windows レジストリをバックアップおよびリストアする
  http://support.microsoft.com/kb/322756

Windows オペレーティング システム提供の Telnet クライアント

この手順は、以下の場合に適用されます。

- 32 ビット オペレーティング システム上の 32 ビット Internet Explorer
- 32 ビット オペレーティング システム上の 32 ビット Firefox
- 64 ビット オペレーティング システム上の 64 ビット Internet Explorer

Web ブラウザで使用するオペレーティング システム提供の telnet クライアントを設定するには、以下の手順を実行します。

1 (Microsoft Windows 7、Microsoft Vista、または Microsoft Windows Server 2008 専用) オペレーティング システムに該当する手順に従い、コンピュータにオペレーティング システム telnet クライアントをインストールします。

Windows 7 または Vista:

a [コントロール パネル] で、**[プログラム]** をクリックしてから、**[プログラムと機能]** をクリックします。

b [タスク] で、**[Windows の機能の有効化または無効化]** をクリックします。

c [Windows の機能] ダイアログボックスで、**[Telnet クライアント]** チェックボックスをオンにして、**[OK]** をクリックします。

Windows Server 2008:

a [サーバー マネージャ] の [機能の概要] で、**[機能の追加]** をクリックします。

b [機能の追加ウィザード] で、**[Telnet クライアント]** チェックボックスをオンにして、**[次へ]**、**[インストール]** の順にクリックします。

2 (Internet Explorer 専用) telnet を使用する Internet Explorer を有効化します。

a Windows レジストリをバックアップします。

b Windows レジストリ エディタを使用して、[HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Internet Explorer¥MAIN¥FeatureControl¥FEATURE_DISABLE_TELNET_PROTOCOL] キーに以下の値を追加します。

名前	タイプ	データ
iexplore.exe	REG_DWORD	0

3 URL:Telnet プロトコル ファイル タイプのファイル関連付けを設定します。

a Windows レジストリをバックアップします。

b Windows レジストリ エディタを使用して、[HKEY_CLASSES_ROOT¥telnet¥shell¥open¥command] キーを以下の値で変更します。

名前	タイプ	データ
(デフォルト)	REG_SZ	rundll32.exe url.dll,TelnetProtocolHandler %l

`%l` (小文字の L) は telnet に渡される引数で、通常はノードの IP アドレスまたは完全修飾ドメイン名。

制御を厳しくするには、キーのバイナリへのパスを 1 行としてコード化できます。たとえば、以下のようにします。

```
"C:¥Windows¥system32¥rundll32.exe"
"C:¥Windows¥system32¥url.dll",TelnetProtocolHandler %l
```

4 Web ブラウザを再起動してから、ブラウザのアドレス バーに telnet コマンドを入力します。

telnet://<node>

<node> は telnet サーバーを実行するノードの IP アドレスまたは完全修飾ドメイン名です。

セキュリティ警告が表示される場合は、アクションを許可します。

Firefox で、**[Remember my choice for telnet links (今後 telnet リンクを同様に処理する)]** チェックボックスをオンにします。

サードパーティ Telnet クライアント (標準 Windows)

この手順は、以下の場合に適用されます。

- 32 ビット オペレーティング システム上の 32 ビット Internet Explorer
- 64 ビット Windows 7 オペレーティング システム上の 32 ビット Internet Explorer
- 32 ビット オペレーティング システム上の 32 ビット Firefox
- 64 ビット オペレーティング システム上の 64 ビット Internet Explorer

Web ブラウザで使用するサードパーティ telnet クライアントを設定するには、以下の手順に従います。

1 サードパーティ telnet クライアントを取得してインストールします。

この手順では、`C:¥Program Files¥PuTTY¥putty.exe` にインストールした PuTTY クライアントを例にあげます。PuTTY クライアントは、以下から使用できます。**http://www.putty.org**。

2 (Internet Explorer 専用) telnet を使用する Internet Explorer を有効化します。

a Windows レジストリをバックアップします。

b Windows レジストリ エディタを使用して、[HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Internet Explorer¥MAIN¥FeatureControl¥FEATURE_DISABLE_TELNET_PROTOCOL] キーに以下の値を追加します。

名前	タイプ	データ
iexplore.exe	REG_DWORD	0

3 URL:Telnet プロトコル ファイル タイプのファイル関連付けを設定します。

a Windows レジストリをバックアップします。

b Windows レジストリ エディタを使用して、[HKEY_CLASSES_ROOT¥telnet¥shell¥open¥command] キーを以下の値で変更します。

名前	タイプ	データ
(デフォルト)	REG_SZ	"C:¥Program Files¥PuTTY¥putty.exe" %l

`%l` (小文字の L) は telnet に渡される引数で、通常はノードの IP アドレスまたは完全修飾ドメイン名。

.reg ファイルでは、各引用符 (") とバックスラッシュ (¥) 文字はバックスラッシュ (¥) 文字でエスケープします。

4 Web ブラウザを再起動してから、ブラウザのアドレス バーに telnet コマンドを入力します。

telnet://<node>

<node> は telnet サーバーを実行するノードの IP アドレスまたは完全修飾ドメイン名です。

セキュリティ警告が表示される場合は、アクションを許可します。

Firefox で、**[Remember my choice for telnet links (今後 telnet リンクを同様に処理する)]** チェックボックスをオンにします。

サードパーティ Telnet クライアント (Windows 上のウィンドウ)

この手順は、以下の場合に適用されます。

- 64 ビット オペレーティング システム上の 32 ビット Internet Explorer (Windows 7 以外)
- 32 ビット オペレーティング システム上の 64 ビット Firefox

Web ブラウザで使用するサードパーティ telnet クライアントを設定するには、以下の手順に従います。

1 サードパーティ telnet クライアントを取得してインストールします。

この手順では、`C:¥Program Files¥PuTTY¥putty.exe` にインストールした PuTTY クライアントを例にあげます。PuTTY クライアントは **http://www.putty.org** から使用できます。

2 (Internet Explorer 専用) telnet を使用する Internet Explorer を有効化します。

a Windows レジストリをバックアップします。

b Windows レジストリ エディタを使用して、[HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Microsoft¥Internet Explorer¥MAIN¥FeatureControl¥FEATURE_DISABLE_TELNET_PROTOCOL] キーに以下の値を追加します。

名前	タイプ	データ
iexplore.exe	REG_DWORD	0

3 URL:Telnet プロトコル ファイル タイプのファイル関連付けを設定します。

a Windows レジストリをバックアップします。

b Windows レジストリ エディタを使用して、[HKEY_CLASSES_ROOT¥Wow6432Node¥telnet¥shell¥open¥command] キーを以下の値で変更します。

名前	タイプ	データ
(デフォルト)	REG_SZ	"C:¥Program Files¥PuTTY¥putty.exe" %l

`%l` (小文字の L) は telnet に渡される引数で、通常はノードの IP アドレスまたは完全修飾ドメイン名。

.reg ファイルでは、各引用符 (") とバックスラッシュ (¥) 文字はバックスラッシュ (¥) 文字でエスケープします。

4 Web ブラウザを再起動してから、ブラウザのアドレス バーに telnet コマンドを入力します。

telnet://<*node*>

<node> は telnet サーバーを実行するノードの IP アドレスまたは完全修飾ドメイン名です。

セキュリティ警告が表示される場合は、アクションを許可します。

Firefox で、**[Remember my choice for telnet links (今後 telnet リンクを同様に処理する)]** チェックボックスをオンにします。

サードパーティ SSH クライアント (標準 Windows および Windows 上のウィンドウ)

この手順は、以下の場合に適用されます。

- 32 ビットまたは 64 ビット オペレーティング システム上の 32 ビット Internet Explorer
- 32 ビットまたは 64 ビット オペレーティング システム上の 32 ビット Firefox
- 64 ビット オペレーティング システム上の 64 ビット Internet Explorer

Web ブラウザで使用するサードパーティ SSH クライアントを設定するには、以下の手順を実行します。

1 サードパーティ SSH クライアントを取得してインストールします。

この手順では、`C:¥Program Files¥PuTTY¥putty.exe` にインストールした PuTTY クライアントを例にあげます。PuTTY クライアントは **http://www.putty.org** から使用できます。

2 PuTTY は 「ssh://<node>」入力を正しく構文解析できないため、この例には入力引数から「ssh://」を取り除くスクリプトが含まれています。スクリプト `C:¥Program Files¥PuTTY¥ssh.js` には、以下のコマンドが含まれます。

```
host = WScript.Arguments(0).replace(/ssh:/,"").replace(/¥//g,"");
shell = WScript.CreateObject("WScript.Shell");
shell.Run("¥"c:¥¥Program Files¥¥PuTTY¥¥putty.exe¥" -ssh " + host);
```

このスクリプトはこの例のために作成されたもので、PuTTY には含まれません。

3 ssh プロトコルを定義します。

a Windows レジストリをバックアップします。

b Windows レジストリ エディタを使用して、[HKEY_CLASSES_ROOT¥ssh] キーに以下の値を追加します。

名前	タイプ	データ
(デフォルト)	REG_SZ	URL:ssh プロトコル
EditFlags	REG_DWORD	2
FriendlyTypeName	REG_SZ	セキュア シェル
URL プロトコル	REG_SZ	*値なし*

4 URL:ssh プロトコル ファイル タイプのファイル関連付けを設定します。

a Windows レジストリをバックアップします。

b Windows レジストリ エディタを使用して、[HKEY_CLASSES_ROOT¥ssh¥shell¥open¥command] キーを以下の値で変更します。

名前	タイプ	データ
(デフォルト)	REG_SZ	"C:¥Windows¥System32¥WScript.exe" "C:¥Program Files¥PuTTY¥ssh.js" %l

`%l` (小文字の L) は完全 ssh 引数で、プロトコル指定が含まれます。ssh.js スクリプトは ssh ターゲットを PuTTY に渡します。

.reg ファイルでは、各引用符 (") とバックスラッシュ (¥) 文字はバックスラッシュ (¥) 文字でエスケープします。

5 Web ブラウザを再起動してから、ブラウザのアドレス バーに ssh コマンドを入力します。

ssh://<node>

<node> は telnet サーバーを実行するノードの IP アドレスまたは完全修飾ドメイン名です。

セキュリティ警告が表示される場合は、アクションを許可します。

Firefox で、**[Remember my choice for ssh links (今後 ssh リンクを同様に処理する)]** チェックボックスをオンにします。

Linux で Telnet または SSH を使用する Firefox の設定

Linux オペレーティング システムに telnet または ssh プロトコルを定義してから、新規プロトコルを使用するように Firefox を設定します。

このセクションの手順を完了するには、コンピュータの管理権限が必要です。

詳細については、**http://kb.mozillazine.org/Register_protocol** を参照してください。

Linux 上の Telnet

Linux オペレーティング システムで telnet プロトコルを使用するように Firefox を設定するには、以下の手順に従います。

1 telnet プロトコルを定義します。

a `/usr/local/bin/nnmtelnet` ファイルを以下の内容で作成します。

```
#!/bin/bash
#
# Linux shell script called by Firefox in response to
# telnet:// URLs for the NNMi telnet menu.
#
```

```
address=`echo $1 | cut -d : -f 2 | sed 's;/;;g'`
port=`echo $1 | cut -d : -f 3`
exec /usr/bin/xterm -e telnet $address $port
```

b 誰でも実行可能なスクリプト権限を設定します。

```
chmod 755 /usr/local/bin/nnmtelnet
```

2 telnet 用の Firefox プリファレンスを設定します。

a Firefox アドレス バーに、**about:config** と入力します。

b プリファレンス リスト内を右クリックし、**[新規]** をクリックしてから、**[ブール値]** をクリックします。

c プリファレンス名 **network.protocol-handler.expose.telnet** を入力します。

d プリファレンス値 **false** を選択します。

3 新規に定義されたプロトコルを使用するように Firefox を設定します。

a telnet リンクを参照します。

リンクを含む簡易 HTML ファイルを作成、または NNMi コンソールで **[アクション] > [Telnet... (クライアントから)** を使用できます。アドレス バーに直接リンクを入力しても、同じ結果にはなりません。

b [アプリケーションの起動] ウィンドウで、**[選択]** をクリックしてから、/usr/local/bin/nnmtelnet を選択します。

c **[Remember my choice for telnet links (今後 telnet リンクを同様に処理する)]** チェックボックスをオンにします。

Linux 上のセキュア シェル

Linux オペレーティング システムで ssh プロトコルを使用するように Firefox を設定するには、以下の手順に従います。

1 ssh プロトコルを定義します。

a /usr/local/bin/nnmssh ファイルを以下の内容で作成します。

```
#!/bin/bash
#
# Linux shell script called by Firefox in response to
# ssh:// URLs for the NNMi SSH menu.
#
address=`echo $1 | cut -d : -f 2 | sed 's;/;;g'`
port=`echo $1 | cut -d : -f 3`
exec /usr/bin/xterm -e ssh $address $port
```

b 誰でも実行可能なスクリプト権限を設定します。

```
chmod 755 /usr/local/bin/nnmssh
```

2 SSH 用の Firefox プリファレンスを設定します。

a Firefox アドレス バーに、**about:config** と入力します。

b プリファレンス リスト内を右クリックし、**[新規]** をクリックしてから、**[ブール値]** をクリックします。

c プリファレンス名 **network.protocol-handler.expose.ssh** を入力します。

d プリファレンス値 **false** を選択します。

3 新規に定義されたプロトコルを使用するように Firefox を設定します。

a SSH リンクを参照します。

リンクを含む簡易 HTML ファイルを作成、または NNMi コンソールで定義した新規 SSH メニュー項目を使用できます。アドレス バーに直接リンクを入力しても、同じ結果にはなりません。

b [アプリケーションの起動] ウィンドウで、**[選択]** をクリックしてから、`/usr/local/bin/nnmssh` を選択します。

c **[Remember my choice for ssh links (今後 ssh リンクを同様に処理する)]** チェックボックスをオンにします。

Windows レジストリを変更するファイル例

多くの NNMi ユーザーが telnet または ssh プロトコルを使用して NNMi コンソールから管理対象ノードにアクセスする必要がある場合は、Windows レジストリ更新を 1 つ以上の .reg ファイルで自動化することができます。このセクションには、独自の .reg ファイル作成の基準にできる .reg ファイル例が含まれます。レジストリ キーは、アプリケーションとオペレーティング システムが一致する場合と、64 ビットの Windows バージョンで 32 ビットのアプリケーションを実行する場合では異なるパスにあります。

詳細については、**http://support.microsoft.com/kb/310516** の Microsoft の記事を参照してください。

nnmtelnet.reg の例

このレジストリの内容例は、153 ページの「Windows オペレーティング システム提供の Telnet クライアント」に適用されます。

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Internet
Explorer¥MAIN¥FeatureControl¥FEATURE_DISABLE_TELNET_PROTOCOL]
"iexplore.exe"=dword:00000000

[HKEY_CLASSES_ROOT¥telnet¥shell¥open¥command]
@="¥"C:¥¥Windows¥¥system32¥¥rundll32.exe¥"
¥"C:¥¥Windows¥¥system32¥¥url.dll¥",TelnetProtocolHandler %l"
```

nnmputtytelnet.reg の例

このレジストリの内容例は、155 ページの「サードパーティ Telnet クライアント (標準 Windows)」に適用されます。

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Internet
Explorer¥MAIN¥FeatureControl¥FEATURE_DISABLE_TELNET_PROTOCOL]
"iexplore.exe"=dword:0c0000000

[HKEY_CLASSES_ROOT¥telnet¥shell¥open¥command]
@="¥"C:¥¥Program Files¥¥PuTTY¥¥putty.exe¥" %l"
```

nnmtelnet32on64.reg の例

このレジストリの内容例は、156 ページの「サードパーティ Telnet クライアント (Windows 上のウィンドウ)」に適用されます。

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Microsoft¥Internet
Explorer¥MAIN¥FeatureControl¥FEATURE_DISABLE_TELNET_PROTOCOL]
"iexplore.exe"=dword:00000000

[HKEY_CLASSES_ROOT¥Wow6432Node¥telnet¥shell¥open¥command]
@="¥"C:¥¥Program Files¥¥PuTTY¥¥putty.exe¥" %l"
```

nnmssh.reg の例

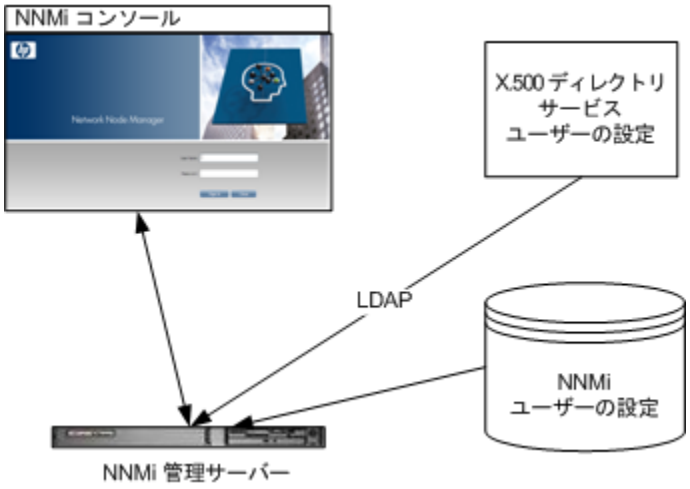
このレジストリの内容例は、157 ページの「サードパーティ SSH クライアント (標準 Windows および Windows 上のウィンドウ)」に適用されます。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT¥ssh]
@="URL:ssh Protocol"
"EditFlags"=dword:00000002
"FriendlyTypeName"="Secure Shell"
"URL Protocol"=""

[HKEY_CLASSES_ROOT¥ssh¥shell¥open¥command]
@="¥"C:¥¥Windows¥¥System32¥¥WScript.exe¥" ¥"c:¥¥Program Files¥¥PuTTY¥¥ssh.js¥" %l"
```

NNMi と LDAP によるディレクトリ サービスの統合



この章では、NNMi とディレクトリ サービスを統合することにより、ユーザー名、パスワード、およびオプションとして NNMi ユーザー グループの割り当ての保存場所を統合する方法について説明します。内容は以下のとおりです。

- 163 ページの「NNMi ユーザーのアクセス情報と設定オプション」
- 167 ページの「ディレクトリ サービスにアクセスする NNMi の設定」
- 174 ページの「ディレクトリ サービスのアクセス設定を変更し、NNMi のセキュリティ モデルをサポートする」
- 176 ページの「ディレクトリ サービスのクエリ」
- 186 ページの「NNMi ユーザー グループを保存するディレクトリ サービスの設定」
- 187 ページの「ディレクトリ サービス統合のトラブルシューティング」
- 188 ページの「ldap.properties 設定ファイル リファレンス」

NNMi ユーザーのアクセス情報と設定オプション

NNMi ユーザーは、以下の項目によって定義されます。

- **ユーザー名**は、NNMi ユーザーを一意に識別します。ユーザー名によって NNMi へのアクセスが許可され、インシデント割り当てを受け取ることができます。
- **パスワード**は、ユーザー名と関連付けられ、NNMi コンソールまたは NNMi コマンドへのアクセスを制御するために使用されます。
- **NNMi ユーザー グループ**メンバーシップにより、提供する情報および NNMi コンソールでユーザーが実行可能なアクションのタイプを制御します。ユーザー グループのメンバーシップに従って、ユーザーが使用可能な NNMi コマンドの制御も行われます。

NNMi には、以下の説明にあるように、NNMi ユーザー アクセス情報の保存先としていくつかのオプションが用意されています。表 7 に、NNMi ユーザー アクセス情報を保存するデータベースを設定オプションごとに示します。

表 7　ユーザー情報の保存オプション

項目	ユーザー名	パスワード	ユーザーグループ	ユーザーグループメンバーシップ
1	NNMi	NNMi	NNMi	NNMi
2	両方	ディレクトリサービス	NNMi	NNMi
3	ディレクトリサービス	ディレクトリサービス	両方	ディレクトリサービス

NNMi を、ユーザー アクセス情報の一部またはすべてを保存するディレクトリ サービスと統合すると、**[システム情報]** ウィンドウの **[サーバー]** タブのユーザー アカウントおよびユーザー グループ定義ステートメントに、LDAP クエリによって取得した情報のタイプが示されます。

NNMi と他のアプリケーションの間のシングル サインオン (SSO) は、NNMi ユーザー アクセス情報の設定やその保存場所に関係なく機能します。

オプション 1: NNMi データベースにすべての NNMi ユーザー情報を保存

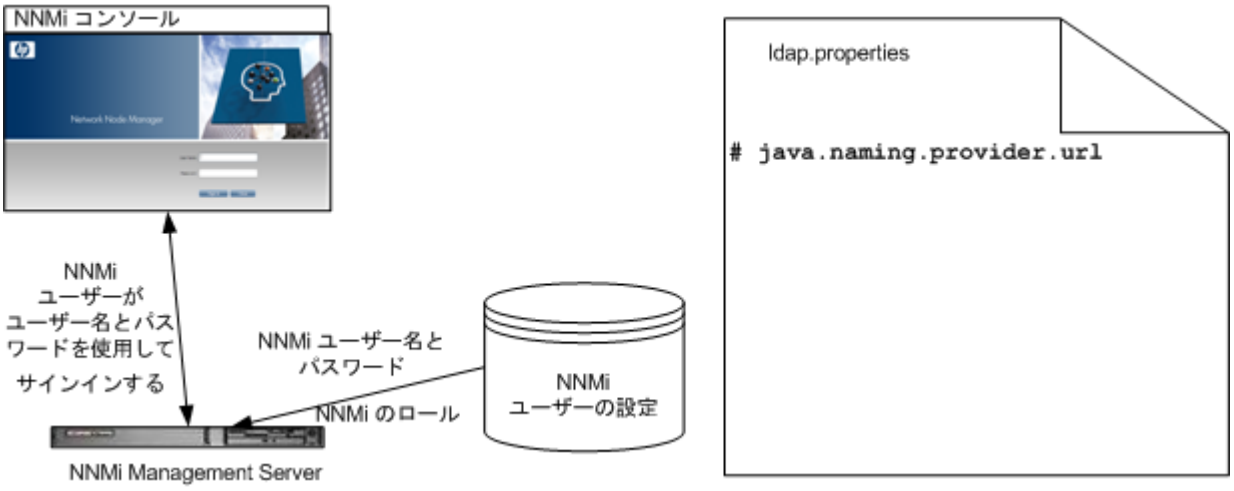
設定オプション 1 では、NNMi が、すべてのユーザー アクセス情報を取得するために NNMi データベースにアクセスします。それらの情報は、NNMi 管理者が NNMi コンソールで定義およびメンテナンスします。ユーザー アクセス情報は、NNMi にとってローカルの情報となります。NNMi はディレクトリ サービスにアクセスせず、NNMi は (図 8 のコメント行に示されている) `ldap.properties` ファイルを無視します。

図 8 に、このオプションの情報フローを示します。この情報フローは、以下のような状況に適しています。

- NNMi ユーザーの数が少ない。
- ディレクトリ サービスを使用していない。

NNMi データベースですべてのユーザー情報を設定する方法の詳細については、NNMi ヘルプの「*Control Access with NNMi Accounts*」を参照してください。この章を読む必要はありません。

図 8　オプション 1 における NNMi ユーザー サインインの情報フロー



オプション 2: 一部の NNMi ユーザー情報を NNMi データベースに、一部の NNMi ユーザー情報をディレクトリ サービスに保存

設定オプション 2 では、NNMi が、ユーザー名とパスワードを取得するためにディレクトリ サービスにアクセスします。それらの情報は、NNMi の外部で定義され、他のアプリケーションでも使用できます。ユーザーから NNMi ユーザー グループへのマッピングは、NNMi コンソールでメンテナンスします。NNMi ユーザー アクセス情報の設定およびメンテナンスは、以下で説明するように共同で行われます。

- ディレクトリ サービス管理者は、ディレクトリ サービス内のユーザー名とパスワードをメンテナンスします。
- NNMi 管理者は、(ディレクトリ サービスで定義されている) ユーザー名、ユーザー グループ定義、ユーザー グループのマッピングを NNMi コンソールで入力します。
- NNMi 管理者は、NNMi に対するユーザー名のディレクトリ サービス データベース スキーマを記述する NNMi `ldap.properties` ファイルを設定します (図 9 のコマンド ラインは、NNMi がユーザー グループ情報をディレクトリ サービスから引き出さないことを示しています)。

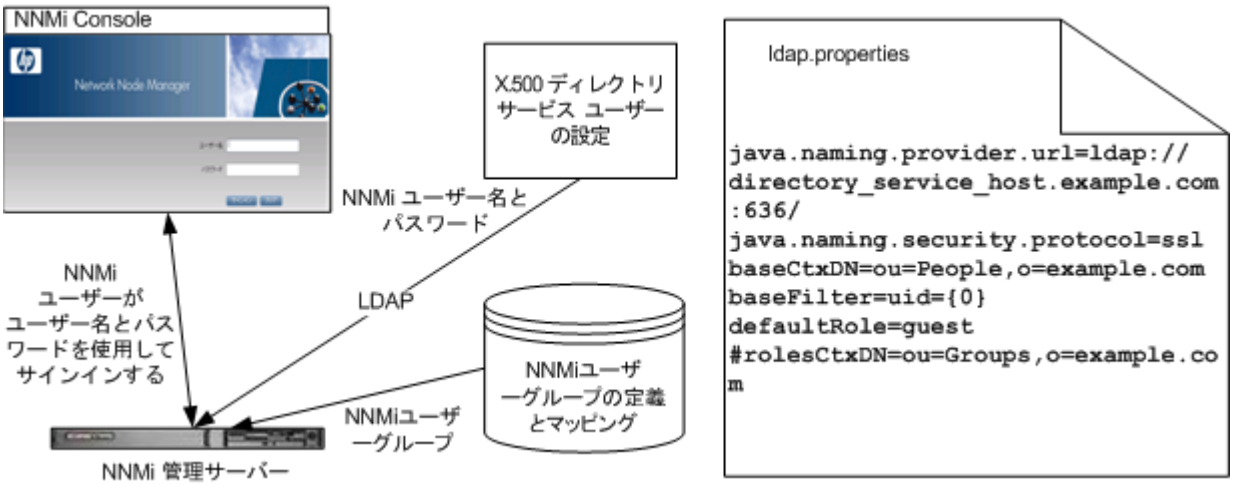
ユーザー名は、2 か所で入力する必要があるため、両方の場所でユーザー名のメンテナンスを行う必要があります。

図 9 に、このオプションの情報フローを示します。この情報フローは、以下のような状況に適しています。

- NNMi ユーザーの数が少なく、ディレクトリ サービスを使用できる。
- ユーザー グループの変更ごとにディレクトリ サービスの変更を必要とするのではなく、NNMi 管理者がユーザー グループを管理する。
- ディレクトリ サービスのグループ定義を簡単には拡張できない。

ユーザー名とパスワードを保存するディレクトリ サービスとの統合に関する詳細については、この章の以降の説明と、NNMi ヘルプの「*Control Access Using Both Directory Service and NNMi*」を参照してください。

図 9　　オプション 2 における NNMi ユーザー サインインの情報フロー



オプション 3: すべての NNMi ユーザー情報をディレクトリ サービスに保存

設定オプション 3 では、NNMi が、すべてのユーザー アクセス情報を取得するためにディレクトリ サービスにアクセスします。それらの情報は、NNMi の外部で定義され、他のアプリケーションが使用できます。1 つ以上のディレクトリ サービス グループでのメンバーシップにより、ユーザーの NNMi ユーザー グループが決まります

NNMi ユーザー アクセス情報の設定およびメンテナンスは、以下で説明するように共同で行われます。

- ディレクトリ サービス管理者は、ディレクトリ サービス内のユーザー名、パスワード、グループ メンバーシップをメンテナンスします。
- NNMi 管理者は、ディレクトリ サービス グループを NNMi ユーザー グループに NNMi コンソールでマッピングします。
- NNMi 管理者は、NNMi に対するユーザー名およびグループのディレクトリ サービス データベース スキーマを記述する NNMi `ldap.properties` ファイルを設定します

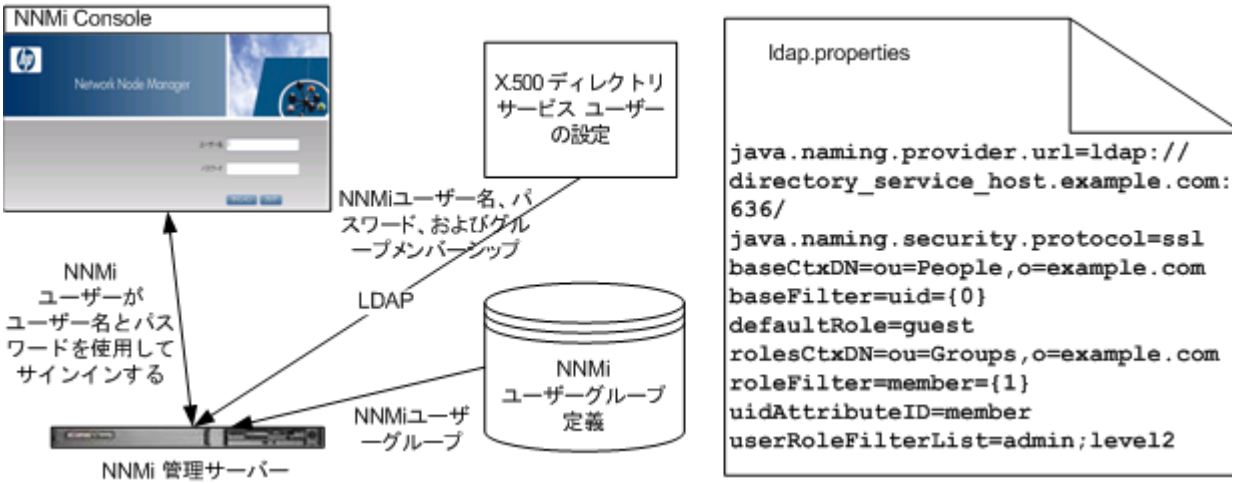
図 10 に、このオプションでの情報フローを示します。これは、NNMi にアクセスする必要があるユーザーで構成されるユーザー グループを含めるようにディレクトリ サービスを変更することが可能な環境に適しています。

このオプションはオプション 2 の例を拡張した形態であるため、HP では以下の設定プロセスを推奨します。

1. ディレクトリ サービスから NNMi ユーザー名とパスワードを取得するよう設定して検証する。
2. ディレクトリ サービスから NNMi ユーザー グループを取得するよう設定する。

すべてのユーザー情報を保存するディレクトリ サービスとの統合に関する詳細については、この章の以降の説明と、NNMi ヘルプの「*Control Access with a Directory Service*」を参照してください。

図 10　　オプション 3 における NNMi ユーザー サインインの情報フロー



ディレクトリ サービスにアクセスする NNMi の設定

ディレクトリ サービスへのアクセスは、以下のフィルで設定されています。

- *Windows*: `%NNM_SHARED_CONF%¥ldap.properties`
- *UNIX*: `$NNM_SHARED_CONF/ldap.properties`

このファイルの詳細については、188 ページの「ldap.properties 設定ファイル リファレンス」を参照してください。192 ページの「例」も参照してください。

ディレクトリ サービスの一般的な構造の詳細については、176 ページの「ディレクトリ サービスのクエリ」を参照してください。

設定オプション 2 の場合は、以下のタスクを実行します。

- タスク 1: 現在の NNMi ユーザー情報をバックアップする
- タスク 2: オプション。ディレクトリ サービスへのセキュア接続を設定する
- タスク 3: ディレクトリ サービスからのユーザー アクセスを設定する
- タスク 4: ユーザー名とパスワードの設定をテストする
- タスク 9: クリーンアップして NNMi への予期せぬアクセスを防止する
- タスク 10: オプション。ユーザー グループをセキュリティ グループにマッピングする

設定オプション 3 の場合は、以下のタスクを実行します。

- タスク 1: 現在の NNMi ユーザー情報をバックアップする
- タスク 2: オプション。ディレクトリ サービスへのセキュア接続を設定する
- タスク 3: ディレクトリ サービスからのユーザー アクセスを設定する
- タスク 4: ユーザー名とパスワードの設定をテストする
- タスク 5: (設定オプション 3 のみ) ディレクトリサービスからのグループの取得を設定する

  ディレクトリ サービスに NNMi ユーザー グループを保存する場合は、NNMi ユーザー グループによってディレクトリ サービスを設定する必要があります。詳細については、186 ページの「NNMi ユーザー グループを保存するディレクトリ サービスの設定」を参照してください。

- タスク 6: (設定オプション 3 のみ) ディレクトリサービスグループを NNMi ユーザーグループにマッピングする
- タスク 7: (設定オプション 3 のみ) NNMi ユーザーグループ設定をテストする
- タスク 8: (設定オプション 3 のみ) インシデント割り当ての NNMi ユーザーグループを設定する
- タスク 9: クリーンアップして NNMi への予期せぬアクセスを防止する
- タスク 10: オプション。ユーザー グループをセキュリティ グループにマッピングする

タスク 1: 現在の NNMi ユーザー情報をバックアップする

NNMi データベースのユーザー情報をバックアップします。

```
nnmconfigexport.ovpl -c account -u <user> ¥
-p <password> -f NNMi_database_accounts.xml
```

タスク 2: オプション。ディレクトリ サービスへのセキュア接続を設定する

ディレクトリ サービスで Secure Socket Layer (SSL) を使用する必要がある場合は、132 ページの「ディレクトリ サービスへの SSL 接続を設定する」の説明に従って、自社の証明書を NNMi トラスト ストアにインポートします。

タスク 3: ディレクトリ サービスからのユーザー アクセスを設定する

このタスクは、設定オプション 2 および 3 の場合に実行します。ディレクトリ サービスに応じた適切な手順に従ってください。このタスクには、以下のセクションが含まれます。

- Microsoft Active Directory の場合の簡単な方法
- 他のディレクトリ サービスの場合の簡単な方法

(設定の詳細な手順については、181 ページの「ユーザー識別」を参照してください。)

Microsoft Active Directory の場合の簡単な方法

1 NNMi に付属する ldap.properties ファイルをバックアップしてから、そのファイルを任意のテキスト エディタで開きます。

2 ファイルの内容を以下のテキストで上書きします。

```
java.naming.provider.url=ldap://<myldapserver>:389/

bindDN=<mydomain>¥¥<myusername>
bindCredential=<mypassword>

baseCtxDN=CN=Users,DC=<myhostname>,DC=<mycompanyname>,DC=<mysuffix>
baseFilter=CN={0}

defaultRole=guest

#rolesCtxDN=CN=Users,DC=<myhostname>,DC=<mycompanyname>,DC=<mysuffix>
roleFilter=member={1}
uidAttributeID=member
userRoleFilterList=admin;level2;level1
```

3 ディレクトリ サービスにアクセスするときの URL を指定します。上のテキストには以下の行があります。

```
java.naming.provider.url=ldap://<myldapserver>:389/
```

<myldapserver> を、Active Directory サーバーの完全修飾ホスト名 (例 : myserver.example.com) で置き換えます。

複数のディレクトリ サービス URL を指定するには、各 URL をスペース文字 1 つ ( ) で区切ります。

4 有効なディレクトリ サービス ユーザーの資格証明を指定します。上のテキストには以下の行があります。

```
bindDN=<mydomain>¥¥<myusername>
bindCredential=<mypassword>
```

以下のように置き換えます。

- *<mydomain>* を Active Directory ドメインの名前で置き換えます。
- *<myusername>* および *<mypassword>* を Active Directory サーバーにアクセスするときに使用するユーザー名とパスワードで置き換えます。パスワードは平文で保存されるため、ディレクトリ サービスへの読み取り専用アクセス権を付与してユーザー名を指定してください。

5 ディレクトリ サーバー ドメインの中でユーザー レコードを保存する部分を指定します。上のテキストには以下の行があります。

```
baseCtxDN=CN=Users,DC=<myhostname>,DC=<mycompanyname>,
  DC=<mysuffix>
```

<myhostname>、*<mycompanyname>*、および *<mysuffix>* を Active Directory サーバーの完全修飾ホスト名のコンポーネントで置き換えます (たとえばホスト名 myserver.example.com の場合は、DC=myserver,DC=example,DC=com と指定します)。

他のディレクトリ サービスの場合の簡単な方法

1. NNMi に付属する ldap.properties ファイルをバックアップしてから、そのファイルを任意のテキスト エディタで開きます。
2. ディレクトリ サービスにアクセスするときの URL を指定します。上のテキストには以下の行があります。

   ```
   #java.naming.provider.url=ldap://<myldapserver>:389/
   ```

   以下を実行します。

   - 行のコメントを解除します (# 文字を削除します)。
   - *<myldapserver>* をディレクトリ サーバーの完全修飾ホスト名で置き換えます (例 : myserver.example.com)。

   複数のディレクトリ サービス URL を指定するには、各 URL をスペース文字 1 つ ( ) で区切ります。

3. ディレクトリ サーバー ドメインの中でユーザー レコードを保存する部分を指定します。上のテキストには以下の行があります。

   ```
   baseCtxDN=ou=People,o=myco.com
   ```

   ou=People,o=myco.com をユーザー レコードを保存するディレクトリ サービス ドメインの部分で置き換えます。

4. NNMi にサインインするユーザー名の形式を指定します。 上のテキストには以下の行があります。

   ```
   baseFilter=uid={0}
   ```

   uid をディレクトリ サービス ドメインのユーザー名属性で置き換えます。

タスク 4: ユーザー名とパスワードの設定をテストする

1. ldap.properties ファイルで、テスト用に defaultRole=guest と設定します (この値はいつでも変更できます)。
2. ldap.properties ファイルを保存します。
3. 以下のコマンドを実行して、NNMi に ldap.properties を再読み込みさせます。

   nnmldap.ovpl -reload

4. ディレクトリ サービスで定義されているユーザー名とパスワードを使用して、NNMi コンソールにログオンします。

   このテストは、NNMi データベースでまだ定義されていないユーザー名を使用して実行してください。

5. NNMi コンソールのタイトル バーで、ユーザー名と NNMi ロール (ゲスト) を確認します。
   - ユーザー サインインが正しく動作したら、このタスクの手順 8 に進みます。
   - ユーザー サインインが正しく動作しない場合は、次は手順 6 に進みます。

   各テストの後で、NNMi コンソールからサインアウトしてセッション資格証明をクリアします。

6 以下のコマンドを実行し、あるユーザーの設定をテストします。

```
nnmldap.ovpl -diagnose <NNMi_user>
```

<NNMi_user> は、ディレクトリ サービスで定義した NNMi ユーザーのサインイン名で置き換えます。

コマンド出力を検討し、適切に応答します。推奨事項は以下のとおりです。

- 168 ページのタスク 3 が正常に完了したことを確認します。
- 181 ページの「ユーザー識別」の詳細な設定プロセスに従います。

7 NNMi コンソールへのサインイン時に期待する結果が表示されるまで、手順 1 から手順 5 を繰り返します。

8 ログオンできたら、設定方法を選択します。

- NNMi ユーザー グループ メンバーシップを NNMi データベースに保存する (設定オプション 2) 場合は、173 ページのタスク 9 に進みます。
- NNMi ユーザー グループ メンバーシップをディレクトリ サービスに保存する (設定オプション 3) 場合は、次はタスク 5 に進みます。

タスク 5: (設定オプション 3 のみ) ディレクトリサービスからのグループの取得を設定する

このタスクは、設定オプション 3 の場合に実行します。ディレクトリ サービスに応じた適切な手順に従ってください。このタスクには、以下のセクションが含まれます。

- Microsoft Active Directory の場合の簡単な方法
- 他のディレクトリ サービスの場合の簡単な方法

(設定の詳細な手順については、183 ページの「ユーザー グループの識別」を参照してください。)

Microsoft Active Directory の場合の簡単な方法

1 `ldap.properties` ファイルをバックアップしてから、そのファイルを任意のテキスト エディタで開きます。

2 ディレクトリ サーバー ドメインの中でグループ レコードを保存する部分を指定します。上のテキストには以下の行があります。

```
#rolesCtxDN=CN=Users,DC=<myhostname>,DC=<mycompanyname>,
  DC=<mysuffix>
```

以下を実行します。

- 行のコメントを解除します (# 文字を削除します)。
- *<myhostname>*、*<mycompanyname>*、および *<mysuffix>* を Active Directory サーバーの完全修飾ホスト名のコンポーネントで置き換えます (たとえばホスト名 `myserver.example.com` の場合は、`DC=myserver,DC=example,DC=com` と指定します)。

他のディレクトリ サービスの場合の簡単な方法

1 `ldap.properties` ファイルをバックアップしてから、そのファイルを任意のテキスト エディタで開きます。

2 ディレクトリ サーバー ドメインの中でグループ レコードを保存する部分を指定します。上のテキストには以下の行があります。

```
#rolesCtxDN=ou=Groups,o=myco.com
```

以下を実行します。

- 行のコメントを解除します (# 文字を削除します)。
- `ou=Groups,o=myco.com` を、ディレクトリ サービス ドメインのグループ レコードを保存する部分で置き換えます。

3 ディレクトリ サービスのグループ定義でグループ メンバー名の形式を指定します。上のテキストには以下の行があります。

```
roleFilter=member={1}
```

`member` を、ディレクトリ サービス ドメインのディレクトリ サービス ユーザー ID を保存するグループ属性の名前で置き換えます。

タスク 6: (設定オプション3のみ) ディレクトリサービスグループをNNMiユーザーグループにマッピングする

1 NNMi コンソールで、定義済みの NNMi ユーザー グループをディレクトリ サービスのユーザー グループにマッピングします。

a **[ユーザー グループ]** ビューを開きます。

[設定] ワークスペースで **[セキュリティ]** を展開してから **[ユーザー グループ]** をクリックします。

b **[管理者]** 行をダブルクリックします。

c **[ディレクトリ サービス名]** フィールドに、NNMi 管理者のディレクトリ サービス グループの完全識別名を 入力します。

d **[保存して閉じる]** をクリックします。

e **guest**、**level1**、**level2** の行ごとに手順 b から手順 d を繰り返します。

このマッピングにより、NNMi コンソールにアクセスできるようになります。NNMi コンソールにアクセスするすべてのユーザーは、この手順で指定した、定義済みの NNMi ユーザー グループのうちいずれかにマッピングされているディレクトリ サービス グループに含まれている必要があります。

2 ディレクトリ サービスで 1 人以上の NNMi ユーザーを含むその他のグループに、NNMi コンソールで新しいユーザー グループを作成します。

a **[ユーザー グループ]** ビューを開きます。

[設定] ワークスペースで **[セキュリティ]** を展開してから **[ユーザー グループ]** をクリックします。

b **[新規作成]** をクリックしてから、グループの情報を入力します。

— **[名前]** は一意の値に設定します。短い名前にすることをお勧めします。

— **[表示名]** は、ユーザーに表示される値に設定します。

— **[ディレクトリ サービス名]** は、ディレクトリ サービス グループの完全識別名に設定します。

— **[説明]** は、この NNMi ユーザー グループの目的を説明するテキストに設定します。

c **[保存して閉じる]** をクリックします。

d NNMi ユーザーのディレクトリ サービス グループごとに手順 b と手順 c を繰り返します。

このマッピングにより、NNMi コンソールのトポロジ オブジェクトにアクセスできるようになります。各ディレクトリ サービス グループは、複数の NNMi ユーザー グループにマッピングできます。

タスク 7: (設定オプション 3 のみ) NNMi ユーザーグループ設定をテストする

1 `ldap.properties` ファイルを保存します。

2 以下のコマンドを実行して、NNMi に `ldap.properties` を再読み込みさせます。

```
nnmldap.ovpl -reload
```

3 ディレクトリ サービスで定義されているユーザー名とパスワードを使用して、NNMi コンソールにログオンします。

NNMi データベースでまだ定義されておらず、admin、level1、level2 の NNMi ユーザー グループにマッピングされているディレクトリ サービス グループのメンバーであるユーザー名で、このテストを実行します。

4 ユーザー名と NNMi ロール (**[ユーザー グループ]** ビューの **[表示名]** フィールドで定義したもの) を NNMi コンソールのタイトル バーで確認します。

- ユーザー サインインが正しく動作したら、172 ページのタスク 8 に進みます。
- ユーザー サインインが正しく動作しない場合は、次は手順 5 に進みます。

各テストの後で、NNMi コンソールからサインアウトしてセッション資格証明をクリアします。

5 以下のコマンドを実行し、あるユーザーの設定をテストします。

```
nnmldap.ovpl -diagnose <NNMi_user>
```

<NNMi_user> は、ディレクトリ サービスで定義した NNMi ユーザーのサインイン名で置き換えます。

コマンド出力を検討し、適切に応答します。推奨事項は以下のとおりです。

- 170 ページのタスク 5 が正常に完了したことを確認します。
- 定義済みの NNMi ユーザー グループごとに、171 ページのタスク 6 が正常に完了したことを確認します。
- 183 ページの「ユーザー グループの識別」の詳細な設定プロセスに従います。

6 NNMi コンソールへのサインイン時に期待する結果が表示されるまで、手順 1 から手順 4 を繰り返します。

タスク 8: (設定オプション 3 のみ) インシデント割り当ての NNMi ユーザーグループを設定する

1 `ldap.properties` ファイルをバックアップしてから、そのファイルを任意のテキスト エディタで開きます。

2 インシデントを割り当てることができる NNMi ロールを NNMi オペレータが指定するように、`userRoleFilterList` パラメータ値を変更します。

1 つ以上の定義済み NNMi ユーザー グループ名の一意の名前 (184 ページの表 10 で定義) をセミコロンで区切ったリストという形式です。

3 `ldap.properties` ファイルを保存します。

4 以下のコマンドを実行して、NNMi に `ldap.properties` を再読み込みさせます。

```
nnmldap.ovpl -reload
```

5 ディレクトリ サービスで定義されているユーザー名とパスワードを使用して、NNMi コンソールにログオンします。

6 任意のインシデント ビューでインシデントを選択し、**[アクション] > [割り当て] > [インシデントの割り当て]** をクリックします。`userRoleFilterList` パラメータによって指定されている各 NNMi ロールのユーザーに、インシデントを割り当てることができることを確認します。

7 設定した各 NNMi ロールにインシデントを割り当てることができるまで、手順 1 から手順 6 の操作を繰り返してください。

タスク 9: クリーンアップして NNMi への予期せぬアクセスを防止する

1 オプション。`ldap.properties` ファイルで、`defaultRole` パラメータの値を変更するか、またはコメントを解除します。

2 (設定オプション 2 のみ) NNMi データベースにユーザーグループメンバーシップを保存するには、以下の手順を実行して、NNMi データベースのユーザーアクセス情報をリセットします。

   a 既存のユーザー アクセス情報すべてを削除します (**[ユーザー アカウント]** ビューのすべての行を削除します)。

   詳細については、NNMi ヘルプの「*ユーザーアカウントの削除*」を参照してください。

   b NNMi ユーザーごとに、ユーザー名の **[ユーザーアカウント]** ビューに新しいオブジェクトを作成します。

   — **[名前]** フィールドに、ディレクトリサービスに定義されているユーザー名を入力します。

   — **[ディレクトリサービスアカウント]** チェックボックスを選択します。

   — パスワードは指定しないでください。

   詳細については、NNMi ヘルプの「*ユーザーアカウントタスク*」を参照してください。

   c NNMi ユーザーごとに、1 つ以上の NNMi ユーザー グループにユーザー アカウントをマッピングします。

   詳細については、NNMi ヘルプの「*ユーザーアカウントマッピングタスク*」を参照してください。

   d インシデント所有権を更新して、各割り当てインシデントが有効なユーザー名と関連付けられるようにします。

   詳細については、NNMi ヘルプの「*インシデント割り当ての管理*」を参照してください。

3 (設定オプション 3 のみ) ディレクトリサービスのユーザーグループメンバーシップを使用するには、以下の手順を実行して、NNMi データベースのユーザーアクセス情報をリセットします。

   a 既存のユーザー アクセス情報すべてを削除します (**[ユーザー アカウント]** ビューのすべての行を削除します)。

   詳細については、NNMi ヘルプの「*ユーザーアカウントの削除*」を参照してください。

   b インシデント所有権を更新して、各割り当てインシデントが有効なユーザー名と関連付けられるようにします。

   詳細については、NNMi ヘルプの「*インシデント割り当ての管理*」を参照してください。

タスク 10: オプション。ユーザー グループをセキュリティ グループにマッピングする

詳細については、NNMi ヘルプの「*セキュリティグループマッピングタスク*」を参照してください。

ディレクトリ サービスのアクセス設定を変更し、NNMi のセキュリティ モデルをサポートする

ここでは、ldap.properties ファイルを NNMi 8.1x または 9.0x から改訂して、ユーザーごとに複数の NNMi ユーザー グループをサポートする方法について説明します。この改訂は、以下の条件の*両方*で必要となります。

- ldap.properties ファイルにより、NNMi ユーザー アクセス設定オプション 3 (ディレクトリ サービスにすべての NNMi ユーザー情報) が現在有効になっている。
- NNMi をカスタム セキュリティ グループで設定したか、設定することになっている。

NNMi 8.1x および 9.0x の場合、NNMi ユーザーは、定義済みの NNMi ロールのうちいずれかに割り当てられていました。各ユーザーは、NNMi トポロジのすべてのオブジェクトにアクセスできました。

NNMi 9.10 では、定義済みの NNMi ユーザー グループで NNMi ロールが置き換わります。各 NNMi ユーザーは最低 1 つの定義済み NNMi ユーザー グループに属する必要があり、これによって NNMi ユーザーが NNMi コンソールで実行できる事項が定義されます。追加のユーザー グループが存在する場合は、以下のように NNMi トポロジ オブジェクトへのアクセスを制限します。

- カスタム ユーザー グループが存在しない場合、すべての NNMi コンソール ユーザーはすべてのトポロジ オブジェクトにアクセスできます。
- 1 つ以上のカスタム ユーザー グループが存在する場合、各ユーザー グループは NNMi トポロジのオブジェクトのサブセットにアクセスできます。

NNMi 8.1x および 9.0x では、各ディレクトリ サービス グループ定義に、NNMi ロールを指定するグループ属性を含める必要がありました。ldap.properties 設定ファイルの以下のパラメータで、このグループ属性を指定していました。

- roleAttributeID
- roleAttributeIsDN
- roleNameAttributeID

NNMi 9.10 では、このパラメータが廃止されます。今後のリリースではサポートされなくなります。

NNMi 9.10 では、各ユーザー グループを NNMi コンソールで定義する必要があります。ユーザー グループ定義には外部名を含めます。これが、ディレクトリ サービスにおけるグループの識別名になります。

ディレクトリ サービスのアクセス設定を変更して NNMi セキュリティ モデルをサポートするには、以下の手順を実行します。

1. NNMi データベースのユーザー情報をバックアップします。

```
nnmconfigexport.ovpl -c account -u <user> ¥
-p <password> -f NNMi_database_accounts.xml
```

2. ldap.properties ファイルをバックアップしてから、そのファイルを任意のテキスト エディタで開きます。

ldap.properties ファイルの詳細については、188 ページの「ldap.properties 設定ファイル リファレンス」を参照してください。廃止されたパラメータの詳細については、前バージョンの NNMi の『NNMi デプロイメント リファレンス』を参照してください。

3 以下のパラメータが存在する場合は、コメント アウトするか削除します。

- `roleAttributeID`
- `roleAttributeIsDN`
- `roleNameAttributeID`

`roleAttributeID` パラメータは、NNMi ユーザー グループの識別にどの方法を使用するかを NNMi に指示するフラグです。`roleAttributeID` を設定すると、NNMi では NNMi 8.1x および 9.0x の方法が使用されます。`roleAttributeID` を設定しないと、NNMi では NNMi 9.10 の方法が使用されます。

4 NNMi コンソールで、定義済みの NNMi ユーザー グループをディレクトリ サービスのユーザー グループにマッピングします。

a **[ユーザー グループ]** ビューを開きます。

[設定] ワークスペースで **[セキュリティ]** を展開してから **[ユーザー グループ]** をクリックします。

b **[管理者]** 行をダブルクリックします。

c **[ディレクトリ サービス名]** フィールドに、NNMi 管理者のディレクトリ サービス グループの完全識別名を 入力します。

d **[保存して閉じる]** をクリックします。

e **guest**、**level1**、**level2** の行ごとに手順 b から手順 d を繰り返します。

このマッピングにより、NNMi コンソールにアクセスできるようになります。NNMi コンソールにアクセスするすべてのユーザーは、この手順で指定した、定義済みの NNMi ユーザー グループのうちいずれかにマッピングされているディレクトリ サービス グループに含まれている必要があります。

5 ディレクトリ サービスで NNMi ユーザーの追加グループを識別します。必要に応じて新しいグループを定義します。

6 手順 5 で追加された新しいグループごとに、NNMi コンソールで新しいユーザー グループを作成します。

a **[ユーザー グループ]** ビューを開きます。

[設定] ワークスペースで **[セキュリティ]** を展開してから **[ユーザー グループ]** をクリックします。

b **[新規作成]** をクリックしてから、グループの情報を入力します。

— **[名前]** は一意の値に設定します。短い名前にすることをお勧めします。

— **[表示名]** は、ユーザーに表示される値に設定します。

— **[ディレクトリ サービス名]** は、ディレクトリ サービス グループの完全識別名に設定します。

— **[説明]** は、この NNMi ユーザー グループの目的を説明するテキストに設定します。

c **[保存して閉じる]** をクリックします。

d NNMi ユーザーの新しいディレクトリ サービス グループごとに手順 b と手順 c を繰り返します。

このマッピングにより、NNMi コンソールのトポロジ オブジェクトにアクセスできるようになります。各ディレクトリ サービス グループは、複数の NNMi ユーザー グループにマッピングできます。

7 オプション。ユーザー グループをセキュリティ グループにマッピングします。

詳細については、NNMi ヘルプの「*セキュリティの設定*」を参照してください。

ディレクトリ サービスのクエリ

NNMi は、LDAP を使用してディレクトリ サービスと通信します。NNMi が要求を送信すると、ディレクトリ サービスは保存されている情報を返します。NNMi は、ディレクトリ サービスに保存されている情報を変更できません。

この項では以下の内容について説明します。

- ディレクトリ サービス アクセス
- ディレクトリ サービスの情報
- ディレクトリ サービス管理者が所有する情報
- ユーザー識別
- ユーザー グループの識別

ディレクトリ サービス アクセス

LDAP は、以下の形式でディレクトリ サービスに対してクエリを実行します。

ldap://*<directory_service_host>*:*<port>*/*<search_string>*

- `ldap` はプロトコル指定子です。この指定子は、ディレクトリ サービスへの標準接続と SSL 接続の両方で使用してください。
- *<directory_service_host>* は、ディレクトリ サービスをホストするコンピュータの完全修飾名です。
- *<port>* は、LDAP 通信でディレクトリ サービスが使用するポートです。非 SSL 接続のデフォルト ポートは 389 です。SSL 接続のデフォルト ポートは 636 です。
- *<search_string>* には要求情報が指定されます。詳細については、「ディレクトリ サービスの情報」と、以下のサイトにある RFC 1959「*An LDAP URL Format*」を参照してください。
  labs.apache.org/webarch/uri/rfc/rfc1959.txt

Web ブラウザで LDAP クエリを URL として入力し、アクセス情報が正しく、検索文字列の構造が正しいことを確認できます。

ディレクトリ サービス (たとえば、Active Directory) が匿名アクセスを許可しない場合、そのディレクトリは Web ブラウザからの LDAP クエリを拒否します。この場合は、サードパーティ製の LDAP ブラウザ (Apache Directory Studio に含まれる LDAP ブラウザなど) を使用し、設定パラメータの有効性を検証できます。

ディレクトリ サービスの情報

ディレクトリ サービスには、ユーザー名、パスワード、およびグループ メンバーシップなどの情報が保存されています。ディレクトリ サービス内の情報にアクセスするには、情報の保存場所を参照する識別名を知っている必要があります。サインイン アプリケーションの場合の識別名は、可変情報 (ユーザー名など) と固定情報 (ユーザー名の保存場所など) の組み合わせです。識別名を構成するエレメントは、ディレクトリ サービスの構造と内容によって決まります。

以下の例は、USERS-NNMi-Admin というユーザー グループの場合に考えられる定義を示しています。このグループは、NNMi への管理アクセス権限を持つディレクトリ サーバーのユーザー ID のリストで構成されます。以下の情報は、これらの例に関係しています。

- Active Directory の例は、Windows オペレーティング システムの場合です。
- 他のディレクトリ サービスの例は、UNIX オペレーティング システムの場合です。
- それぞれの例に示すファイルは、LDIF (lightweight directory interchange format) ファイルの一部です。LDIF ファイルにより、ディレクトリ サービスの情報を共有できます。
- それぞれの例の図は、ディレクトリ サービス ドメインをグラフィカルに表現したものです。この図は、引用した LDIF ファイルに含まれる情報を拡張して表示したものです。

Active Directory の情報構造例

この例での関心の対象は以下の項目です。

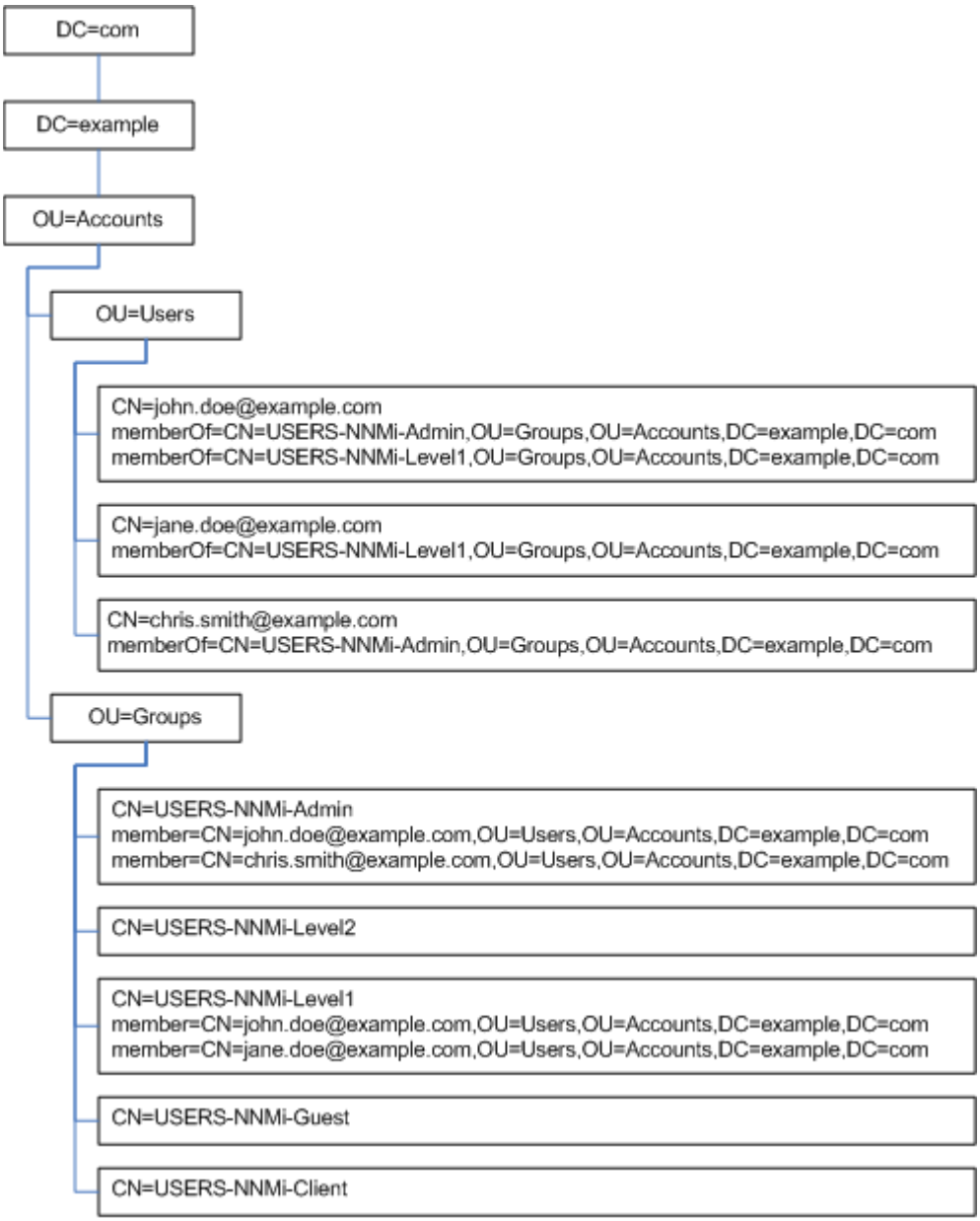
- ユーザー John Doe の識別名：
  `CN=john.doe@example.com,OU=Users,OU=Accounts,DC=example,DC=com`
- USERS-NMi-Admin グループの識別名：
  `CN=USERS-NNMi-Admin,OU=Groups,OU=Accounts,DC=example,DC=com`
- ディレクトリ サービス ユーザー ID を保存するグループ属性：`member`

LDIF ファイルの引用例：

```
groups |USERS-NNMi-Admin
dn: CN=USERS-NNMi-Admin,OU=Groups,OU=Accounts,DC=example,DC=com
cn: USERS-NNMi-Admin
description: Group of users for NNMi administration.
member: CN=john.doe@example.com,OU=Users,OU=Accounts,
  DC=example,DC=com
member: CN=chris.smith@example.com,OU=Users,OU=Accounts,
  DC=example,DC=com
```

178 ページ の図 11 に、このディレクトリ サービス ドメインを例示します。

図 11　　Active Directory のドメイン例



他のディレクトリ サービスの情報構造例

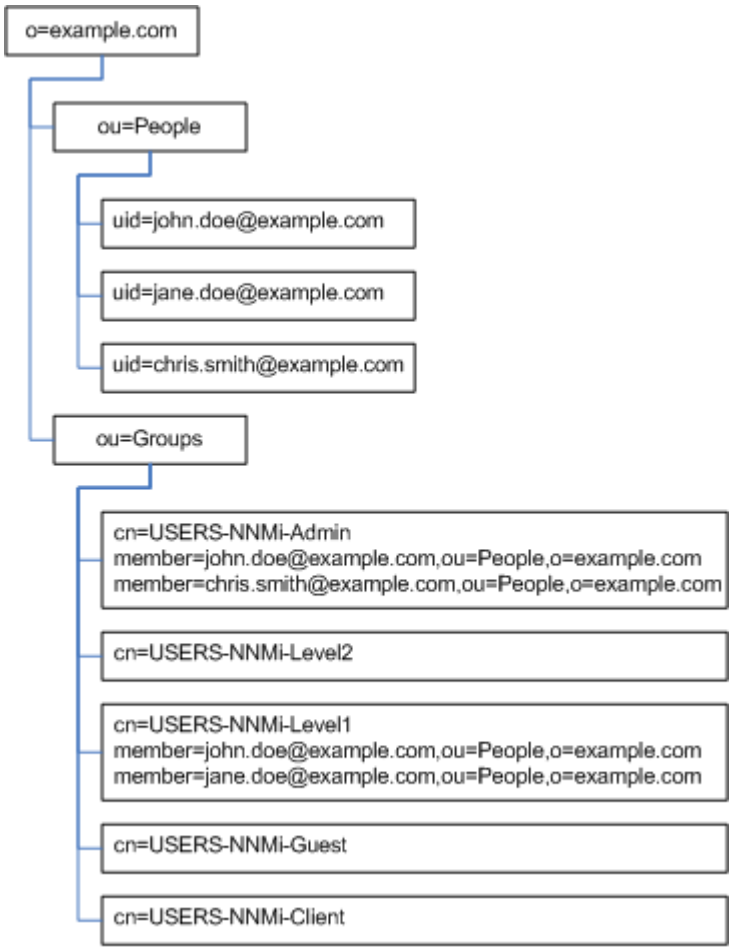
この例での関心の対象は以下の項目です。

- ユーザー John Doe の識別名：
  `uid=john.doe@example.com,ou=People,o=example.com`
- USERS-NMi-Admin グループの識別名：
  `cn=USERS-NNMi-Admin,ou=Groups,o=example.com`
- ディレクトリ サービス ユーザー ID を保存するグループ属性：`member`

LDIF ファイルの引用例：

```
groups |USERS-NNMi-Admin
dn: cn=USERS-NNMi-Admin,ou=Groups,o=example.com
cn: USERS-NNMi-Admin
description: Group of users for NNMi administration.
member: uid=john.doe@example.com,ou=People,o=example.com
member: uid=chris.smith@example.com,ou=People,o=example.com
```

図 12　他のディレクトリ サービスのドメインの例



ディレクトリ サービス管理者が所有する情報

表 8 と表 9 には、ディレクトリ サービスに LDAP アクセスするように NNMi を設定する前に、ディレクトリ サービス管理者から取得する情報をリストしています。

- ユーザー名とパスワードのみにディレクトリ サービスを使用する場合は (設定オプション 2)、表 8 の情報を収集します。
- すべての NNMi アクセス情報にディレクトリ サービスを使用する場合は (設定オプション 3)、表 8 と表 9 の情報を収集します。

表 8　ユーザー名およびパスワードをディレクトリ サービスから取得するための情報

情報	Active Directory の例	その他のディレクトリ サービスの例
ディレクトリ サービスをホストするコンピュータの完全修飾名	directory_service_host.example.com	
LDAP 通信でディレクトリ サービスが使用するポート	• 非 SSL 接続の場合は 389 • SSL 接続の場合は 636	
ディレクトリ サービスでの SSL 接続情報	SSL 接続が必要な場合は、会社のトラスト ストア証明書のコピーを取得し、132 ページの「ディレクトリ サービスへの SSL 接続を設定する」を参照します。	
ディレクトリ サービスに保存される 1 つのユーザー名の識別名 (ディレクトリ サービス ドメインを示す)	CN=john.doe@example.com, OU=Users,OU=Accounts, DC=example,DC=com	uid=john.doe@example.com, ou=People,o=example.com

表 9　グループ メンバーシップをディレクトリ サービスから取得するための情報

情報	Active Directory の例	その他のディレクトリ サービスの例
ユーザーが割り当てられているグループを識別する識別名	memberOf ユーザー属性によりグループを識別します。	• ou=Groups,o=example.com • cn=USERS-NNMi-*, ou=Groups,o=example.com
グループ内のユーザーを識別する方法	• CN=john.doe@example.com, OU=Users,OU=Accounts, DC=example,DC=com • CN=john.doe@example.com	• cn=john.doe@example.com, ou=People,o=example.com • cn=john.doe@example.com
ディレクトリ サービス ユーザー ID を保存するグループ属性	member	member

表 9　グループ メンバーシップをディレクトリ サービスから取得するための情報（続く）

情報	Active Directory の例	その他のディレクトリ サービスの例
NNMi アクセスに適用するディレクトリ サービスのグループの名前	• CN=USERS-NNMi-Admin, OU=Groups,OU=Accounts, DC=example,DC=com • CN=USERS-NNMi-Level2, OU=Groups,OU=Accounts, DC=example,DC=com • CN=USERS-NNMi-Level1, OU=Groups,OU=Accounts, DC=example,DC=com • CN=USERS-NNMi-Client, OU=Groups,OU=Accounts, DC=example,DC=com • CN=USERS-NNMi-Guest, OU=Groups,OU=Accounts, DC=example,DC=com	• cn=USERS-NNMi-Admin, ou=Groups,o=example.com • cn=USERS-NNMi-Level2, ou=Groups,o=example.com • cn=USERS-NNMi-Level1, ou=Groups,o=example.com • cn=USERS-NNMi-Client, ou=Groups,o=example.com • cn=USERS-NNMi-Guest, ou=Groups,o=example.com

ユーザー識別

ユーザー識別は、設定オプション 2 および 3 に適用されます。

ユーザー識別のための識別名は、1 人のユーザーをディレクトリ サービスで特定するための完全に修飾する方法です。NNMi はユーザー識別名を LDAP 要求でディレクトリ サービスに渡します。

`ldap.properties` ファイルでのユーザー識別名は、`baseFilter` 値と `baseCtxDN` 値を連結した値です。ディレクトリ サービスによって返されたパスワードが、NNMi コンソールにユーザーが入力したサインイン パスワードと一致する場合、ユーザー サインインが続行されます。

設定オプション 2 の場合は、以下の情報が適用されます。

- NNMi コンソール アクセスの場合、NNMi は以下の情報を検討し、可能な限り高い権限をユーザーに与えます。
  - `ldap.properties` ファイルの `defaultRole` パラメータの値
  - NNMi コンソールで定義済みの NNMi ユーザー グループにおける、このユーザーのメンバーシップ
- NNMi トポロジ オブジェクト アクセスの場合、NNMi は、NNMi コンソールでこのユーザーが属する NNMi ユーザー グループのセキュリティ グループ マッピングに従ってアクセス権を与えます。

設定オプション 3 の場合は、以下の情報が適用されます。

- NNMi コンソール アクセスの場合、NNMi は以下の情報を検討し、可能な限り高い権限をユーザーに与えます。
  - `ldap.properties` ファイルの `defaultRole` パラメータの値
  - NNMi コンソールで定義済みの NNMi ユーザー グループにマッピングされている（**[ディレクトリ サービス名]** フィールド）ディレクトリ サービス グループにおける、このユーザーのメンバーシップ

- NNMi トポロジ オブジェクト アクセスの場合、NNMi は、このユーザーがディレクトリ サービス (NNMi コンソールで NNMi ユーザーがマッピングされている) で属するグループのセキュリティ グループ マッピングに従ってアクセス権を与えます。

Active Directory でのユーザー識別例

`baseFilter` を `CN={0}` に設定し、`baseCtxDN` を `OU=Users,OU=Accounts,DC=example,DC=com` に設定し、ユーザーが `john.doe` として NNMi にサインインする場合、ディレクトリサービスに渡される文字列は以下のとおりです。

```
CN=john.doe,OU=Users,OU=Accounts,DC=example,DC=com
```

その他のディレクトリ サービスでのユーザー識別例

`baseFilter` を `uid={0}@example.com` に設定し、`baseCtxDN` を `ou=People,o=example.com` に設定し、ユーザーが `john.doe` として NNMi にサインインする場合、ディレクトリサービスに渡される文字列は以下のとおりです。

```
uid=john.doe@example.com,ou=People,o=example.com
```

ディレクトリ サービスからの NNMi ユーザー アクセスの設定 (詳細な方法)

168 ページのタスク 3 で説明した単純な方法が正しく動作しない場合は、以下の手順を実行します。

1. 180 ページの表 8 にリストされている情報をディレクトリ サービス管理者から取得します。
2. 適切な手順を完了し、ディレクトリ サービスにおけるユーザー名の形式を確認します。
   - *Active Directory およびその他のディレクトリ サービスの場合に LDAP ブラウザを使用する方法*: 183 ページの「ディレクトリ サービスでユーザーを識別する方法の判別 (LDAP ブラウザを使用する方法)」を参照してください。
   - *他のディレクトリ サービスの場合に Web ブラウザを使用する方法*: 183 ページの「ディレクトリ サービスでユーザーを識別する方法の判別 (Web ブラウザを使用する方法)」を参照してください。
3. 任意のテキスト エディタで `ldap.properties` ファイルを開きます。

   `ldap.properties` ファイルの詳細については、188 ページの「ldap.properties 設定ファイル リファレンス」を参照してください。

4. `java.naming.provider.url` パラメータを、LDAP によってディレクトリ サービスにアクセスする場合の URL に設定します。
   - *LDAP ブラウザを使用する方法*: LDAP ブラウザ設定からこの情報を入手します。
   - *Web ブラウザを使用する方法*: 183 ページの「ディレクトリ サービスでユーザーを識別する方法の判別 (Web ブラウザを使用する方法)」から、< *ディレクトリ サービス ホスト* > と < *ポート* > の値を含めます。

   複数のディレクトリ サービス URL を指定するには、各 URL をスペース文字 1 つで区切ります。

5. ディレクトリ サービスへのセキュア通信を設定した場合は、以下の行のコメントを解除 (または追加) します。

   ```
   java.naming.security.protocol=ssl
   ```

6 (Active Directory のみ) bindDN および bindCredential パラメータを以下のように設定します。

- *<mydomain>* を Active Directory ドメインの名前で置き換えます。
- *<myusername>* および *<mypassword>* を Active Directory サーバーにアクセスするときに使用するユーザー名とパスワードで置き換えます。パスワードは平文で保存されるため、ディレクトリ サービスへの読み取り専用アクセス権を付与してユーザー名を指定してください。

7 baseCtxDN パラメータを、複数のユーザーで同じになっている、識別ユーザー名のエレメントに設定します。

8 NNMi のサインインで入力するときのユーザー名が、ディレクトリ サービスでユーザー名が保存されるときの方法と相関するように、baseFilter パラメータを設定します。

この値は、ユーザーごとに変更される識別ユーザー名のエレメントです。実際のユーザー名を式 {0} で置き換えます。

9 169 ページのタスク 4 の説明に従って設定をテストします。

ディレクトリ サービスでユーザーを識別する方法の判別 (LDAP ブラウザを使用する方法)

サードパーティの LDAP ブラウザで、以下の手順を実行します。

1 ディレクトリ サーバー ドメインの中でグループ情報を保存する領域にナビゲートします。

2 ユーザーのグループを識別し、そのグループに関連付けられているユーザーの識別名の形式を調べます。

ディレクトリ サービスでユーザーを識別する方法の判別 (Web ブラウザを使用する方法)

1 サポートされる Web ブラウザで、以下の URL を入力します。

ldap://*<directory_service_host>*:*<port>*/*<user_search_string>*

- *<directory_service_host>* は、ディレクトリ サービスをホストするコンピュータの完全修飾名です。
- *<port>* は、LDAP 通信でディレクトリ サービスが使用するポートです。
- *<user_search_string>* は、ディレクトリ サービスに保存される 1 つのユーザー名の識別名です。

2 ディレクトリ サービスのアクセス テストの結果を評価します。

- 要求が時間切れになったり、ディレクトリ サービスに到達できなかったことを示すメッセージが表示される場合は、*<directory_service_host>* と *<port>* の値を確認してから、手順 1 を繰り返してください。
- ディレクトリ　サービスに要求されたエントリが存在しないことを示すメッセージが表示された場合は、*<user_search_string>* の値を確認してから、手順 1 の操作を繰り返してください。
- 該当するユーザー レコードが表示された場合、そのアクセス情報は正しいことになります。*<user_search_string>* の値は、識別ユーザー名です。

ユーザー グループの識別

ユーザー グループ識別は、設定オプション 3 に適用されます。

NNMi は、NNMi ユーザーのユーザー グループを以下のように判断します。

1 NNMi は、NNMi コンソールで設定されているすべてのユーザー グループの外部名の値をディレクトリ サービス グループの名前と比較します。

2 ユーザー グループが一致する場合、NNMi は、NNMi ユーザーがディレクトリ サービスのそのグループのメンバーであるかどうかを判断します。

NNMi コンソールで、短いテキスト文字列により、NNMi コンソール アクセスを許可する、定義済みの NNMi ユーザー グループの一意の名前が識別されます。`ldap.properties` 設定ファイルの `defaultRole` および `userRoleFilterList` パラメータも、このテキスト文字列を必要とします。表 10 では、このグループの一意の名前を表示名にマッピングしています。

表 10　NNMi ユーザー グループ名のマッピング

NNMi コンソールの NNMi のロール名	NNMi 設定ファイルのユーザー グループの一意の名前およびテキスト文字列
管理者	`admin`
オペレータ レベル 2	`level2`
オペレータ レベル 1	`level1`
ゲスト	`guest`
Web サービス クライアント	`client`

ディレクトリ サービスからのユーザー グループ取得の設定 (詳細な方法)

170 ページのタスク 5 で説明した単純な方法が正しく動作しない場合は、以下の手順を実行します。

1 180 ページの表 9 にリストされている情報をディレクトリ サービス管理者から取得します。

2 適切な手順を完了し、ディレクトリ サービスにおけるグループ名およびグループ メンバーの形式を確認します。

- *Active Directory の場合に LDAP ブラウザを使用する方法* : 185 ページの「ディレクトリ サービスでグループおよびグループ メンバーシップを識別する方法の判別 (Active Directory の場合に LDAP ブラウザを使用する方法)」を参照してください。
- *他のディレクトリ サービスの場合に LDAP ブラウザを使用する方法*: 185 ページの「ディレクトリ サービスでグループおよびグループ メンバーシップを識別する方法の判別 (他のディレクトリ サービスの場合に LDAP ブラウザを使用する方法)」を参照してください。
- *他のディレクトリ サービスの場合に Web ブラウザを使用する方法*: 185 ページの「ディレクトリ サービスでグループを識別する方法の判別 (Web ブラウザを使用する方法)」を参照してください。

3 任意のテキスト エディタで `ldap.properties` ファイルを開きます。

`ldap.properties` ファイルの詳細については、188 ページの「ldap.properties 設定ファイル リファレンス」を参照してください。

4 `rolesCtxDN` パラメータを、複数のグループで同じになっている、識別グループ名のエレメントに設定します。

5 ディレクトリ サービスでグループにユーザー名が保存されるときの方法とユーザー名が相関するように、roleFilter パラメータを設定します。実際のユーザー名を以下の式のいずれかで置き換えます。

- サインインのために入力されたユーザー名を意味する場合は {0} を使用します (たとえば、john.doe)。
- ディレクトリ サービスによって返された認証済みユーザーの識別名を意味する場合は、{1} を使用します (たとえば、uid=john.doe@example.com,ou=People,o=example.com)。

6 uidAttributeID パラメータを、ユーザー ID を保存するグループ属性の名前に設定します。

7 172 ページのタスク 7 の説明に従って設定をテストします。

ディレクトリ サービスでグループおよびグループ メンバーシップを識別する方法の判別 (Active Directory の場合に LDAP ブラウザを使用する方法)

サードパーティの LDAP ブラウザで、以下の手順を実行します。

1 ディレクトリ サーバー ドメインの中でユーザー情報を保存する領域にナビゲートします。

2 NNMi にアクセスする必要があるユーザーを識別し、そのユーザーに関連付けられているグループの識別名の形式を調べます。

3 ディレクトリ サーバー ドメインの中でグループ情報を保存する領域にナビゲートします。

4 NNMi ユーザー グループに対応するグループを識別して、グループに関連付けられているユーザーの名前の形式を調べます。

ディレクトリ サービスでグループおよびグループ メンバーシップを識別する方法の判別 (他のディレクトリ サービスの場合に LDAP ブラウザを使用する方法)

サードパーティの LDAP ブラウザで、以下の手順を実行します。

1 ディレクトリ サーバー ドメインの中でグループ情報を保存する領域にナビゲートします。

2 NNMi ユーザー グループに対応するグループを識別して、それらのグループの識別名の形式を調べます。

3 また、グループに関連付けられているユーザーの名前の形式も調べます。

ディレクトリ サービスでグループを識別する方法の判別 (Web ブラウザを使用する方法)

1 サポートされる Web ブラウザで、以下の URL を入力します。

ldap://*<directory_service_host>*:*<port>*/*<group_search_string>*

- *<directory_service_host>* は、ディレクトリ サービスをホストするコンピュータの完全修飾名です。
- *<port>* は、LDAP 通信でディレクトリ サービスが使用するポートです。
- *<group_search_string>* は、ディレクトリ サービスに保存されるグループ名の識別名です (例 : cn=USERS-NNMi-Admin,ou=Groups,o=example.com)。

2 ディレクトリ サービスのアクセス テストの結果を評価します。

- ディレクトリ　サービスに要求されたエントリが存在しないことを示すメッセージが表示された場合は、*<group_search_string>* の値を確認してから、手順 1 の操作を繰り返してください。
- 該当するグループのリストが表示された場合、そのアクセス情報は正しいことになります。

3 グループのプロパティを調べ、そのグループに関連付けられえているユーザーの名前の形式を判断してください。

NNMi ユーザー グループを保存するディレクトリ サービスの設定

NNMi ユーザー グループをディレクトリ サービスに保存する場合 (設定オプション 3) は、NNMi ユーザー グループ情報を使用してディレクトリ サービスを設定する必要があります。原則として、ディレクトリ サービスには適切なユーザー グループがすでに含まれています。含まれていない場合、ディレクトリ サービス管理者は、特に NNMi ユーザー グループ割り当て用の新規ユーザー グループを作成できます。

ディレクトリ サービスの設定およびメンテナンス手順は、特定のディレクトリ サービス ソフトウェアと企業のポリシーに応じて異なるため、ここではそれらの手順について説明していません。

ディレクトリ サービス統合のトラブルシューティング

1 以下のコマンドを実行して NNMi LDAP 設定を検証します。

```
nnmldap.ovpl -info
```

報告された設定が期待どおりの設定ではない場合は、`ldap.properties` ファイルで設定を確認してください。

2 以下のコマンドを実行して、NNMi に `ldap.properties` を再読み込みさせます。

```
nnmldap.ovpl -reload
```

3 以下のコマンドを実行し、あるユーザーの設定をテストします。

```
nnmldap.ovpl -diagnose <NNMi_user>
```

<NNMi_user> は、ディレクトリ サービスで定義した NNMi ユーザーのサインイン名で置き換えます。

コマンド出力を検討し、適切に応答します。

4 ディレクトリ サービスに期待されるレコードが含まれていることを確認します。Web ブラウザまたはサードパーティの LDAP ブラウザ (Apache Directory Studio に含まれる LDAP ブラウザなど) を使用して、ディレクトリ サービスの情報を調べます。

ディレクトリ サービスに対するクエリの形式に関する詳細については、以下のサイトの RFC 1959「*An LDAP URL Format*」を参照してください。

http://labs.apache.org/webarch/uri/rfc/rfc1959.txt

5 `%NnmDataDir%¥log¥nnm¥jbossServer.log` (*Windows*) または `/var/opt/OV/log/nnm/jbossServer.log` (*UNIX*) のログファイルを表示し、サインイン要求が正しいことを確認して、エラーが発生しているかどうかを判断します。

- 以下の行のようなメッセージは、ディレクトリ サービスで HTTPS 通信が必要であることを示しています。この場合は、132 ページの「ディレクトリ サービスへの SSL 接続を設定する」の説明に従って SSL を有効にします。

```
javax.naming.AuthenticationNotSupportedException: [LDAP:
error code 13 - confidentiality required]
```

- 以下の行のようなメッセージは、ディレクトリ サービスとのやり取り中にタイムアウトが発生したことを示します。この場合は、`nms-ldap.properties` ファイルの `searchTimeLimit` の値を増やします。

```
javax.naming.TimeLimitExceededException: [LDAP: error code 3
- Timelimit Exceeded]
```

ldap.properties 設定ファイル リファレンス

ldap.properties ファイルには、ディレクトリ サービスと通信し、それに対する LDAP クエリを作成する場合の設定が保存されています。このファイルは以下の場所にあります。

- *Windows*: %NNM_SHARED_CONF%¥ldap.properties
- *UNIX*: $NNM_SHARED_CONF/ldap.properties

ldap.properties ファイルでは、以下の規則が適用されます。

- 行をコメント アウトするには、その行の先頭を番号記号文字 (#) にします。
- 特殊文字には、以下のルールが適用されます。
  - バックスラッシュ文字 (¥)、カンマ (,)、セミコロン (;)、プラス記号 (+)、小なり記号 (<)、大なり記号 (>) を指定するには、バックスラッシュ文字でエスケープします。たとえば、¥¥ や ¥+ のように指定します。
  - 文字列の*先頭*文字または*末尾*文字としてスペース文字 ( ) を含めるには、バックスラッシュ文字 (¥) でエスケープします。
  - 文字列の*先頭*文字としてシャープ記号 (#) を含めるには、バックスラッシュ文字 (¥) でエスケープします。

  ここで言及していない文字をエスケープしたり、引用符で囲んだりする必要はありません。

ldap.properties ファイルを編集したら、以下のコマンドを実行して NNMi に LDAP 設定を再読み込みさせます。

```
nnmldap.ovpl -reload
```

表 11 に、ldap.properties ファイルのパラメータの説明を示します。

初期の ldap.properties ファイルには、表 11 のリストにあるパラメータの一部が含まれていない場合があります。必要なパラメータを追加してください。

表 11　ldap.properties ファイルのパラメータ

パラメータ	説明
java.naming.provider.url	ディレクトリ サービスにアクセスするときの URL を指定します。 URL は、プロトコル (ldap) の後にディレクトリ サービスの完全修飾ホスト名が続き、オプションとしてさらにポート番号が続く形式で指定します。たとえば、以下のようにします。 java.naming.provider.url=ldap://ldap.example.com:389/ ポート番号を省略すると、以下のデフォルト値が適用されます。 • 非 SSL 接続の場合、デフォルト値は 389 です。 • SSL 接続の場合、デフォルト値は 636 です。 複数のディレクトリ サービスの URL を指定すると、NNMi は可能な限り最初のディレクトリ サービスを使用します。そのディレクトリ サービスにアクセスできない場合、NNMi はリスト内の次のディレクトリ サービスにクエリを実行し、以下同様に対処します。各 URL は 1 つのスペース文字で区切ります。たとえば、以下のようにします。 java.naming.provider.url=ldap://ldap1.example.com/ ldap://ldap2.example.com/ このパラメータを設定すると、NNMi とディレクトリ サービス間の LDAP 通信が有効になります。LDAP 通信を無効にするには、このパラメータをコメント アウトしてからファイルを保存します。これにより NNMi は、ldap.properties ファイルの設定を無視します。

表 11　ldap.properties ファイルのパラメータ (続く)

パラメータ	説明
java.naming.security.protocol	接続プロトコル指定を指定します。 • LDAP over SSL を使用するようにディレクトリ サーバーが設定されている場合は、このパラメータを ssl に設定します。たとえば、以下のようにします。 java.naming.security.protocol=ssl • ディレクトリ サービスで SSL が不要な場合は、このパラメータをコメントアウトしたままにします。 詳細については、132 ページの「ディレクトリ サービスへの SSL 接続を設定する」を参照してください。
bindDN	匿名アクセスを許可しない (Active Directory などの) ディレクトリ サービスの場合は、そのディレクトリ サービスにアクセスするユーザー名を指定します。このユーザー名のパスワードは ldap.properties ファイルに平文で保存されるため、ディレクトリ サービスへの読み取り専用アクセス権を持つユーザー名を選択してください。 たとえば、以下のようにします。 bindDN=region1¥¥john.doe@example.com
bindCredential	bindDN が設定されている場合は、その bindDN によって識別されるユーザー名のパスワードを指定します。たとえば、以下のようにします。 bindCredential=PasswordForJohnDoe
baseCtxDN	ディレクトリ サーバー ドメインの中でユーザー レコードを保存する部分を指定します。 形式は、ディレクトリ サービスの属性名と値のカンマ区切りリストです。たとえば、以下のようにします。 • baseCtxDN=CN=Users,DC=ldapserver,DC=example,DC=com • baseCtxDN=ou=People,o=example.com 詳細については、181 ページの「ユーザー識別」を参照してください。
baseFilter	NNMi にサインインするユーザー名の形式を指定します。 形式は、ディレクトリ サービスのユーザー名属性の名前と、入力したユーザー サインイン名をディレクトリ サービス内の名前の形式に関連付ける文字列で構成されます。ユーザー名文字列には、式 {0} (サインインで入力されたユーザー名を示す) と、ユーザー名のディレクトリ サービス形式を照合するために必要な他の文字が含まれます。 • NNMi のサインインで入力されたユーザー名がディレクトリ サービスに保存されているユーザー名と同じ場合、値は置換表現になります。たとえば、以下のようにします。 – baseFilter=CN={0} – baseFilter=uid={0} • NNMi のサインインで入力したユーザー名がディレクトリ サービスに保存されているユーザー名のサブセットになっている場合は、値に追加の文字を含めます。たとえば、以下のようにします。 – baseFilter=CN={0}@example.com – baseFilter=uid={0}@example.com 詳細については、181 ページの「ユーザー識別」を参照してください。

表 11　**ldap.properties** ファイルのパラメータ (続く)

パラメータ	説明
defaultRole	オプション。LDAP に従って NNMi にサインインするディレクトリ サービス ユーザーすべてに適用されるデフォルト ロールを指定します。このパラメータの値は、(NNMi データベースまたはディレクトリ サービスでの) ユーザー グループ マッピングの保存場所に関係なく適用されます。 定義済みの NNMi ユーザー グループにユーザーが直接設定されている場合、NNMi は、デフォルト ロールおよび割り当て済みユーザー グループの権限のスーパーセットをユーザーに付与します。 有効な値は、`admin`、`level2`、`level1`、または `guest` です。 この名前は、定義済み NNMi ユーザー グループ名の一意の名前です (184 ページの表 10 で定義)。 たとえば、以下のようにします。 `defaultRole=guest` コメント アウトまたは省略すると、NNMi はデフォルト値を使用しません。
rolesCtxDN	ディレクトリ サーバー ドメインの中でグループ レコードを保存する部分を指定します。 形式は、ディレクトリ サービスの属性名と値のカンマ区切りリストです。たとえば、以下のようにします。 • `rolesCtxDN=CN=Users,DC=ldapserver,DC=example,DC=com` • `rolesCtxDN=ou=Groups,o=example.com` 他のディレクトリ サービス (Active Directory 以外) では、検索速度を高めるため、NNMi ユーザー グループを含むディレクトリ サービス グループを 1 つ以上指定できます。グループ名にパターンがある場合は、ワイルドカードを指定できます。たとえば、ディレクトリ サービスに `USERS-NNMi-administrators` や `USERS-NNMi-level1Operators` などの名前のグループが含まれる場合は、以下のような検索コンテキストを使用できます。 `rolesCtxDN=cn=USERS-NNMi-*,ou=Groups,o=example.com` このパラメータを設定すると、LDAP を介した NNMi ユーザー グループ割り当てのディレクトリ サービスのクエリが有効になります。 LDAP を介した NNMi ユーザー グループ割り当てのディレクトリ サービスのクエリを無効にするには、このパラメータをコメント アウトしてからファイルを保存します。NNMi は、`ldap.properties` ファイルにある残りのユーザー グループ関連の値を無視します。 詳細については、183ページの「ユーザー グループの識別」を参照してください。

表 11　ldap.properties ファイルのパラメータ (続く)

パラメータ	説明
roleFilter	ディレクトリ サービスのグループ定義でグループ メンバー名の形式を指定します。 形式は、ユーザー ID のディレクトリ サービス グループ属性の名前と、入力したユーザー サインイン名をディレクトリ サービス内のユーザー ID の形式に関連付ける文字列で構成されます。ユーザー名文字列には、以下の式の 1 つと、グループ メンバー名のディレクトリ サービス形式を照合するために必要な他の文字が含まれています。 • 式 `{0}` は、サインインで入力されたユーザー名を示します (たとえば、`john.doe`)。 サインインで入力される (短い) ユーザー名で照合するロール フィルタ例 : `roleFilter=member={0}` • 式 `{1}` は、ディレクトリ サービスによって返された認証済みユーザーの識別名を意味します (たとえば、 `CN=john.doe@example.com,OU=Users,OU=Accounts,DC=example,DC=com` または `uid=john.doe@example.com,ou=People,o=example.com`)。 (完全に) 認証されたユーザー名で照合するロール フィルタ例 : `roleFilter=member={1}` 詳細については、183ページの「ユーザー グループの識別」を参照してください。
uidAttributeID	ディレクトリ サービス ユーザー ID を保存するグループ属性を指定します。 たとえば、以下のようにします。 `uidAttributeID=member` 詳細については、183ページの「ユーザー グループの識別」を参照してください。
userRoleFilterList	オプション。NNMi コンソールで関連ユーザーにインシデントを割り当てることができる NNMi ユーザー グループを制限します。 このリストのユーザー グループは、LDAP で認証されるディレクトリ サービス ユーザー名のみに適用されます。このパラメータでは、NNMi ユーザー グループが NNMi コンソールで割り当てられて、NNMi データベースに保存されるときに使用できない機能が提供されます。 1 つ以上の定義済み NNMi ユーザー グループ名の一意の名前 (184 ページの表 10 で定義) をセミコロンで区切ったリストという形式です。 `userRoleFilterList=admin;level2;level1`
searchTimeLimit	オプション。タイムアウト値をミリ秒単位で指定します。デフォルト値は 10000 (10 秒) です。NNMi ユーザー サインイン中にタイムアウトになる場合は、この値を増やします。 たとえば、以下のようにします。 `searchTimeLimit=10000`

例

Active Directory の場合の ldap.propaties ファイルの例

Active Directory の場合の ldap.properties ファイルの例を以下に示します。

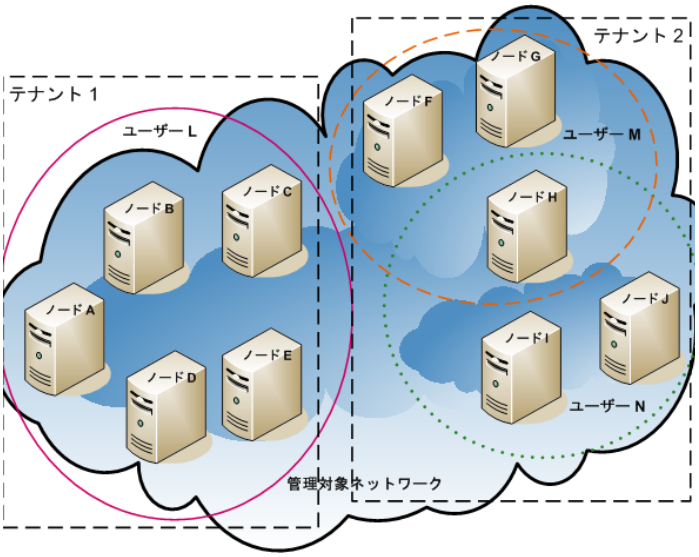
```
java.naming.provider.url=ldap://MYldapserver.example.com:389/
bindDN=MYdomain¥¥MYusername
bindCredential=MYpassword
baseCtxDN=CN=Users,DC=MYldapserver,DC=EXAMPLE,DC=com
baseFilter=CN={0}
defaultRole=guest
rolesCtxDN=CN=Users,DC=MYldapserver,DC=EXAMPLE,DC=com
roleFilter=member={1}
uidAttributeID=member
userRoleFilterList=admin;level2;level1
```

他のディレクトリ サービスの場合の ldap.propaties ファイルの例

他のディレクトリ サービスの場合の ldap.properties ファイルの例を以下に示します。

```
java.naming.provider.url=ldap://MYldapserver.example.com:389/
baseCtxDN=ou=People,o=EXAMPLE.com
baseFilter=uid={0}
defaultRole=guest
rolesCtxDN=ou=Groups,o=EXAMPLE.com
roleFilter=member={1}
uidAttributeID=member
userRoleFilterList=admin;level2;level1
```

NNMi セキュリティおよびマルチテナント



デフォルトでは、すべての NNMi コンソール ユーザーが NNMi データベースのすべてのオブジェクトを参照できます。使用環境でこのデフォルト設定を許容できる場合、この章を読む必要はありません。

NNMi セキュリティおよびマルチテナントでは、NNMi データベースのオブジェクトに関する情報へのユーザーアクセスを制限できます。この制限は、ネットワーク オペレータのビューをその責任範囲に合わせてカスタマイズする場合に役立ちます。また、サービス プロバイダが NNMi を組織ごとに設定する場合にも役立ちます。

この章では、NNMi セキュリティおよびテナント モデルについて説明し、設定の推奨事項について記載します。内容は以下のとおりです。

- 194 ページの「オブジェクトのアクセス制限による影響」
- 195 ページの「NNMi セキュリティ モデル」
- 200 ページの「NNMi テナント モデル」
- 203 ページの「NNMi のセキュリティおよびマルチテナント設定」
- 210 ページの「NNMi セキュリティ、マルチテナント、およびグローバル ネットワーク管理」
- 213 ページの「NPS レポートへの選択インタフェースの追加」

オブジェクトのアクセス制限による影響

NNMi セキュリティを設定すると以下のような影響があります。

- トポロジインベントリオブジェクト：
  - 各 NNMi コンソールユーザーには、それぞれのユーザーの NNMi ユーザーアカウント設定に対応するノードのみが表示されます。
  - インタフェースなどのサブノード オブジェクトは、そのノードからアクセス制御を継承します。
  - 接続などのノード間オブジェクトは、NNMi コンソールユーザーが、関連するノードの少なくとも 1 つを表示できる場合にのみ表示されます。
  - NNMi コンソールユーザーには、ノードグループの中の少なくとも 1 つのノードにそのユーザーがアクセスできるノードグループのみが表示されます。
  - Network Performance Server (NPS) レポートの場合、NNMi 管理者はインタフェースのアクセス制御の継承を選択的に上書きできます。詳細については、213 ページの「NPS レポートへの選択インタフェースの追加」を参照してください。
- マップおよびパス ビュー：
  - マップには、関与している両方のノードを表示する権限を NNMi コンソールユーザーが持っている接続が表示されます。
  - パスビューでは、NNMi コンソールユーザーがアクセスできないすべての中間ノードは省略されるか、クラウドとして表示されます。
  - NNM iSPI for MPLS および NNM iSPI for IP Multicast については、マップとパスビューに NNMi コンソールユーザーがアクセスできないノードが含まれている場合、NNM iSPI には接続中のインタフェースとノードの名前しか表示されません。アクセスできないノードのアイコンは白色で表示され、それらのノードのステータスと詳細情報を入手できないことが示されます。
  - NNM iSPI for IP Telephony については、マップとパスビューに NNMi コンソールユーザーがアクセスできないノードが含まれている場合、NNM iSPI には接続されているインタフェースとノードの名前しか表示されません。アクセスできないノードのアイコンには NNMi ステータスが表示されますが、アクションを行ってもすべて失敗します。
- インシデント：
  - ソースノードが NNMi トポロジ内にあるインシデントについては、NNMi コンソールユーザーには、そのユーザーがソースノードにアクセスできるインシデントのみが表示されます。
  - NNMi の稼働状態およびライセンス管理イベントのインシデントなど、ソースノードが含まれないインシデントは、1 つのグループとして処理されます。NNMi 管理者は、どの NNMi コンソールユーザーにそれらのインシデントが表示されるかを (ユーザーに [未解決のインシデント] セキュリティグループを関連付けることで) 決定します。
  - ソースノードが NNMi トポロジ内にないトラップから生じたインシデントは、ソースノードが含まれないインシデントと同様に処理されます。これらのインシデントを生成するように NNMi が設定されている場合、NNMi 管理者は、どの NNMi コンソールユーザーにそれらのインシデントが表示されるかを (ユーザーに [未解決のインシデント] セキュリティグループを関連付けることで) 決定します。

インシデントの割り当てアクションでは、ユーザーのアクセス権はチェックされません。NNMi 管理者によって、あるインシデントがそのインシデントを表示する権限を持たない NNMi コンソールユーザーに割り当てられる可能性があります。

- NNMi コンソールアクション :
  - 何も選択を行わずに実行されるアクションについては、NNMi コンソールユーザーには、そのユーザーが実行する権限を持っているアクションのみが表示されます。
  - 選択された1つ以上のオブジェクトに対して実行されるアクションの場合、NNMi コンソールユーザーは、選択されたオブジェクトに対する適切なアクセスレベルを持っている必要があります。セキュリティ設定によっては、NNMi コンソールビューに表示されている一部のオブジェクトに対して有効ではないアクションが NNMi コンソールに表示される場合もあります。これらの無効なアクションを実行すると、この制限に関するエラーメッセージが表示されます。
  - マップビューや、NNM iSPI テーブルビューおよびフォームについては、NNMi は、不明なノードと、NNMi トポロジ内に存在するが現在のユーザーがアクセスできないノードの区別を行うことができません。
- MIB ブラウザおよび Line Grapher:
  - NNMi コンソールユーザーは、ユーザーがアクセスできるノードの MIB データとグラフを表示できます。
  - NNMi コンソールユーザーは、ユーザーが SNMP コミュニティ文字列を認識しているノードの MIB データを表示できます。
- NNMi コンソール URL:

  ダイレクト URL から NNMi コンソールビューにアクセスするには、NNMi にログオンする必要があります。NNMi は、NNMi セキュリティ設定に応じてユーザーのアクセス権を適用し、それに従って、使用可能なトポロジを制限します。

NNMi セキュリティ モデル

NNMi セキュリティ モデルでは、NNMi データベースのオブジェクトへのユーザー アクセスを制御できます。このモデルは、NNMi ユーザーのアクセスを特定のオブジェクトやインシデントに制限するネットワーク管理組織で使用する場合に適しています。NNMi セキュリティ モデルには、以下の利点があります。

- NNMi コンソール オペレータのネットワークのビューを制限できます。オペレータは特定のデバイス タイプまたはネットワーク領域に集中できます。
- NNMi トポロジへのオペレータ アクセスをカスタマイズできます。オペレータ アクセスのレベルは、ノードごとに設定できます。
- [カスタム ノード] ビューおよび Network Performance Server レポートをセキュリティ グループでフィルタリングできます。
- セキュリティ設定で構成されるノード グループの設定およびメンテナンスが簡素化されます。
- NNMi テナント モデルとは独立して使用できます。

NNMi セキュリティは、以下のような場合に使用されます。

- NNMi オペレータがサイト (カスタム マップ) 内の機器タイプに集中できるようにする。
- 特定のサイト (カスタム マップ) のノードのみが表示される各サイト ビューを NNMi オペレータに提供する。
- 導入時にノードをステージングする。 NNMi 管理者にはすべてのノードが表示されますが、NNMi オペレータには導入したノードのみが表示されます。

- すべての NOC オペレータにフルアクセスを付与し、NOC ユーザーのアクセスを制限する。
- 中央の NOC オペレータに完全なネットワーク ビューを提供し、地域の NOC オペレータのビューを制限する。

セキュリティ グループ

NNMi セキュリティ モデルでは、ノードへのユーザー アクセスはユーザー グループおよびセキュリティ グループを介して間接的に制御されます。NNMi トポロジ内の各ノードは、1 つのセキュリティグループのみに関連付けられます。セキュリティ グループは複数のユーザー グループに関連付けることができます。

各ユーザー アカウントは、以下のユーザー グループにマッピングされます。

- 以下に示す事前設定された 1 つ以上の NNMi ユーザー グループ :
  - NNMi 管理者
  - NNMi レベル 1 オペレータ
  - NNMi レベル 2 オペレータ
  - NNMi ゲスト ユーザー

  このマッピングは NNMi コンソール アクセスに必要で、これによって NNMi コンソール内で使用できるアクションが決まります。ユーザー アカウントがこれらの複数の NNMi ユーザー グループにマッピングされている場合、許可されるアクションのスーパーセットがユーザーに付与されます。

  [NNMi Web サービス クライアント] ユーザー グループでは、NNMi コンソールへのアクセス権は付与されませんが、すべての NNMi オブジェクトへの管理者レベルのアクセス権が付与されます。

- セキュリティ グループにマッピングされる 0 個以上のカスタム ユーザー グループ

  これらのマッピングでは、NNMi データベースのオブジェクトへのアクセスが提供されます。各マッピングには、セキュリティ グループのノードに適用されるオブジェクト アクセス権限レベルが含まれています。オブジェクト アクセス権限レベルは、インタフェースやインシデントなどの関連するデータベース オブジェクトにも適用されます。たとえば、インタフェース X および Y を含むノードへのオブジェクト オペレータ レベル 1 のアクセス権限があるユーザーには、以下のすべてのデータベース オブジェクトへのオブジェクト オペレータ レベル 1 のアクセス権限があります。

  - ノード A
  - インタフェース X および Y
  - ソース オブジェクトがノード A、インタフェース X、またはインタフェース Y のインシデント

NNMi には、以下のセキュリティグループがあります。

- デフォルトセキュリティグループ

  新しい NNMi インストール済み環境では、[デフォルトセキュリティグループ] がすべてのノードに対する初期セキュリティグループとして割り当てられます。デフォルトでは、すべてのユーザーに、[デフォルトセキュリティグループ] 内のすべてのオブジェクトが表示されます。NNMi 管理者は、[デフォルトセキュリティグループ] に関連付けられるノードと、[デフォルトセキュリティグループ] 内のオブジェクトにアクセスできるユーザーを設定できます。

- 未解決のインシデント

  [未解決のインシデント] セキュリティグループは、ソースノードが NNMi トポロジ内にない受信トラップから NNMi が作成するインシデントへのアクセス権を提供します。デフォルトでは、すべてのユーザーに、[未解決のインシデント] セキュリティグループに関連付けられたすべてのインシデントが表示されます。NNMi 管理者は、[未解決のインシデント] セキュリティグループに関連付けられたインシデントにアクセスできるユーザーを設定できます。

すべてのノード コンポーネントは、ノードのセキュリティ グループの割り当てを継承します。

ベストプラクティス

以下のベスト プラクティスが NNMi セキュリティ設定に適用されます。

- 各ユーザー アカウントを事前設定された 1 つの NNMi ユーザー グループのみにマッピングします。
- 事前設定された NNMi ユーザー グループをセキュリティ グループにマッピングしないでください。
- [NNMi 管理者] ユーザーグループにマッピングされたすべてのユーザーアカウントには、NNMi データベースのすべてのオブジェクトに対する管理者レベルのアクセス権が付与されるため、このユーザーアカウントをほかのユーザーグループにマッピングしないでください。
- Web Service Client ロール専用のユーザー アカウントを別個に作成します。このユーザーアカウントは NNMi トポロジ全体にアクセスできるため、このユーザーアカウントは [NNMi Web Service Client] ユーザーグループにのみマッピングしてください。

セキュリティ グループ構造の例

図 13 内の 3 つの楕円形は、この NNMi トポロジの例で、ユーザーに表示する必要のあるノードのプライマリグループを示しています。ユーザーアクセスを完全に制御するには、4 つの各サブグループが一意のセキュリティグループに対応している必要があります。一意の各セキュリティグループを 1 つ以上のユーザーグループにマッピングして、そのセキュリティグループ内のオブジェクトに対する使用可能なユーザーアクセスのレベルを表すことができます。

198 ページの表 12 に、このトポロジにおけるセキュリティ グループと考えられるカスタム ユーザー グループ間のマッピングを示します (このセキュリティ モデルを実際に実装する場合、これらのカスタム ユーザー グループの一部は不要になる可能性があります)。199 ページの表 13 に、このトポロジにおけるいくつかのユーザー アカウントとユーザー グループのマッピングを示します。

図 13　ユーザー アクセス要件に対応するトポロジの例

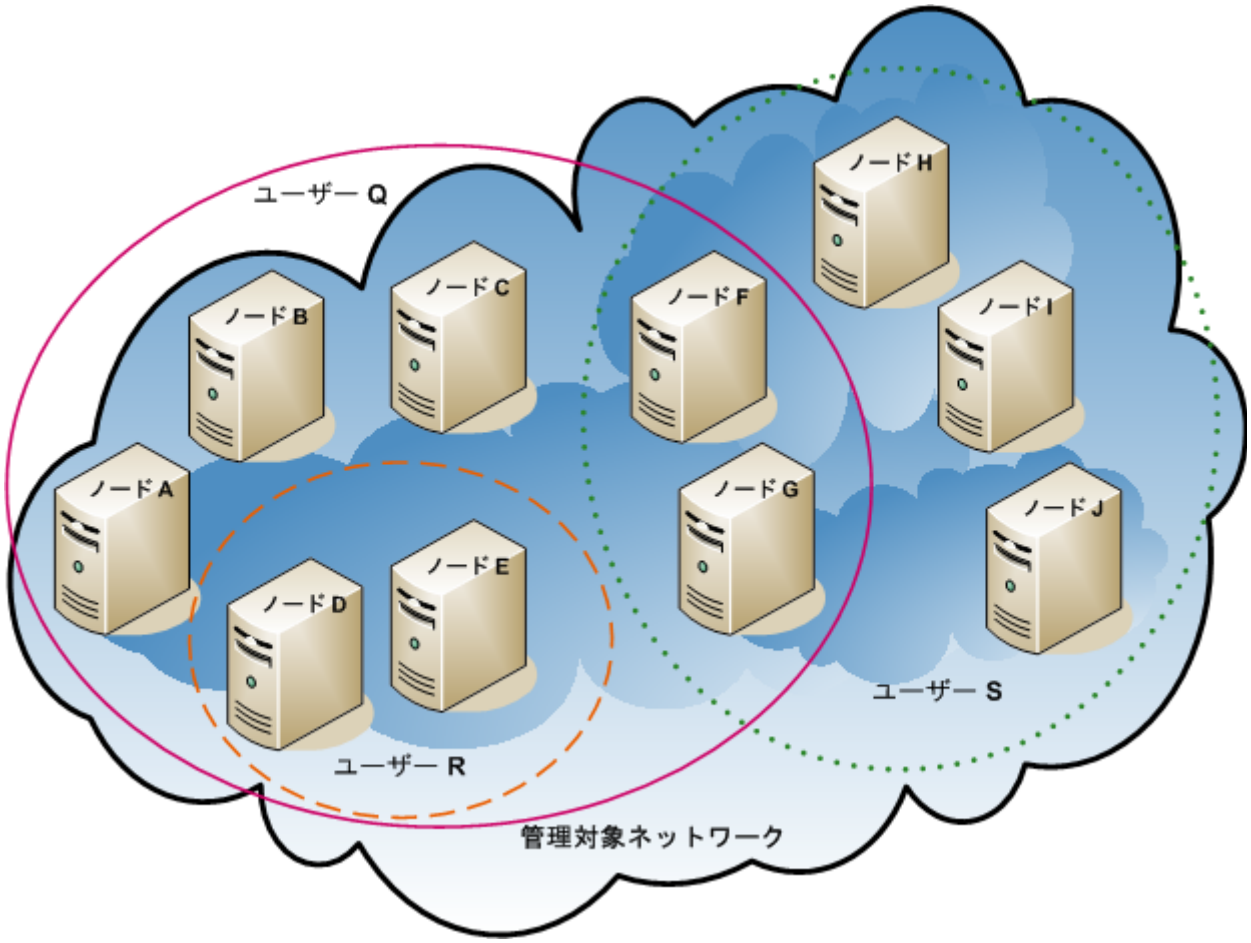


表 12　セキュリティ グループ マッピングの例

セキュリティ グループ	セキュリティ グループのノード	ユーザー グループ	オブジェクト アクセス権限
SG1	A、B、C	UG1 管理者	オブジェクト管理者
		UG1 レベル 2	オブジェクト オペレータ レベル 2
		UG1 レベル 1	オブジェクト オペレータ レベル 1
		UG1 ゲスト	オブジェクト ゲスト
SG2	D、E	UG2 管理者	オブジェクト管理者
		UG2 レベル 2	オブジェクト オペレータ レベル 2
		UG2 レベル 1	オブジェクト オペレータ レベル 1
		UG2 ゲスト	オブジェクト ゲスト

表 12　セキュリティ グループ マッピングの例（続く）

セキュリティ グループ	セキュリティ グループのノード	ユーザー グループ	オブジェクト アクセス権限
SG3	F、G	UG3 管理者	オブジェクト管理者
		UG3 レベル 2	オブジェクト オペレータ レベル 2
		UG3 レベル 1	オブジェクト オペレータ レベル 1
		UG3 ゲスト	オブジェクト ゲスト
SG4	H、I、J	UG4 管理者	オブジェクト管理者
		UG4 レベル 2	オブジェクト オペレータ レベル 2
		UG4 レベル 1	オブジェクト オペレータ レベル 1
		UG4 ゲスト	オブジェクト ゲスト

表 13　ユーザー アカウント マッピングの例

ユーザー アカウント	ユーザー グループ	ノード アクセス	注
ユーザー Q	NNMi レベル 2 オペレータ	なし	このユーザーには、ピンクの楕円形 (実線) に含まれるノードへのオペレータレベル2のアクセス権限があります。
	UG1 レベル 2	A、B、C	
	UG2 レベル 2	D、E	
	UG3 レベル 2	F、G	
ユーザー R	NNMi レベル 1 オペレータ	なし	このユーザーには、オレンジの楕円形 (破線) に含まれるノードへのオペレータレベル1のアクセス権限があります。
	UG2 レベル 1	D、E	
ユーザー S	NNMi レベル 2 オペレータ	なし	このユーザーには、緑の楕円形 (点線) に含まれるノードへのオペレータレベル2のアクセス権限があります。
	UG3 レベル 2	F、G	
	UG4 レベル 2	H、I、J	
ユーザー T	NNMi レベル 2 オペレータ	なし	このユーザーは、トポロジの例に含まれるすべてのノードに (各権限レベルで) アクセスできます。 このユーザーには、ノード D および E への管理アクセス権がありますが、管理アクセス権が必要なツールのメニュー項目は表示できません。 ユーザーに NNMi 管理サーバーへのアクセス権がある場合は、ノード D および E に対してのみ、管理アクセス権が必要なコマンドラインツールを実行できます。
	UG1 ゲスト	A、B、C	
	UG2 管理者	D、E	
	UG3 レベル 2	F、G	
	UG4 レベル 1	H、I、J	

NNMi テナント モデル

NNMi テナント モデルでは、トポロジ検出とトポロジ データが各テナント (組織または顧客とも呼ばれる) で完全に分離されます。このモデルは、サービス プロバイダ (特に管理対象サービス プロバイダ) や大規模エンタープライズに適しています。NNMi テナント モデルには、以下の利点があります。

- 各ノードが属する組織が明確になります。
- [カスタムノード] インベントリビューと Network Performance Server レポートを、テナントとセキュリティグループでフィルタリングできます。
- 顧客データへのオペレータ アクセスを分離する規制要件に適合します。
- テナント設定で構成されるノード　グループの設定およびメンテナンスが簡素化されます。
- NNMi セキュリティの設定が簡素化されます。

NNMi マルチテナントを使用すると、同じ NNMi 管理サーバーで複数の顧客 (テナント) を管理するサービスプロバイダに、異なる顧客ビューを提供することができます。

テナント

NNMi テナント モデルでは、組織という概念がセキュリティ設定に加わります。NNMi トポロジ内の各ノードが属するテナントは、1 つのみです。テナントによって、NNMi データベースが論理的に分離されます。オブジェクト アクセスはセキュリティ グループで管理されます。

ノードが最初に検出されて NNMi データベースに追加されるときに、各ノードで初期検出テナントの割り当てが発生します。シード済みのノードで、各ノードに割り当てるテナントを指定できます。NNMi によって、検出された他のすべてのノード (自動検出ルールに含まれているが直接シードされないノード) がデフォルト テナントに割り当てられます。NNMi 管理者は、検出後にいつでもノードのテナントを変更できます。

各テナント定義には、初期検出セキュリティ グループが含まれます。NNMi によって、この初期検出セキュリティグループが初期検出テナントとともにノードに割り当てられます。NNMi 管理者は、検出後にいつでもノードのセキュリティ グループを変更できます。

ノードのテナントの割り当てを変更しても、セキュリティ グループの割り当ては自動的に変更されません。

NNMi には、デフォルトテナントが備わっています。デフォルトでは、すべての NNMi ユーザーが、([デフォルトセキュリティグループ] を介して) このテナントに関連付けられたすべてのオブジェクトにアクセスできます。

すべてのノード コンポーネントは、ノードのテナントおよびセキュリティ グループの割り当てを継承します。

ベストプラクティス

以下のベスト プラクティスが NNMi テナント設定に適用されます。

- 小規模な組織の場合、テナントごとに 1 つのセキュリティ グループで十分です。
- 大規模な組織を複数のセキュリティ グループに分割できます。
- ユーザーが組織をまたいでノードにアクセスできないようにするには、各セキュリティグループに、1 つのテナントのみに対応するノードしか含まれないようにします。

テナント構造の例

図 14 に、NNMi トポロジ内に 2 つのテナントが含まれている様子を長方形の線で囲んで示します。これらの 3 つの楕円形は、ユーザーにノードを表示する必要があるプライマリグループを表しています。テナント 1 のトポロジは 1 つのグループとして管理されるため、1 つのセキュリティ グループのみが必要です。テナント 2 のトポロジは重複しているセットで管理されるため、3 つのセキュリティグループに分割されます。

202 ページの表 14 に、このトポロジにおけるセキュリティ グループと考えられるカスタム ユーザー グループ間のマッピングを示します (このセキュリティ モデルを実際に実装する場合、これらのカスタム ユーザー グループの一部は不要になる可能性があります)。202 ページの表 15 に、このトポロジにおけるいくつかのユーザー アカウントとユーザー グループのマッピングを示します。

図 14　　複数のテナントのトポロジの例

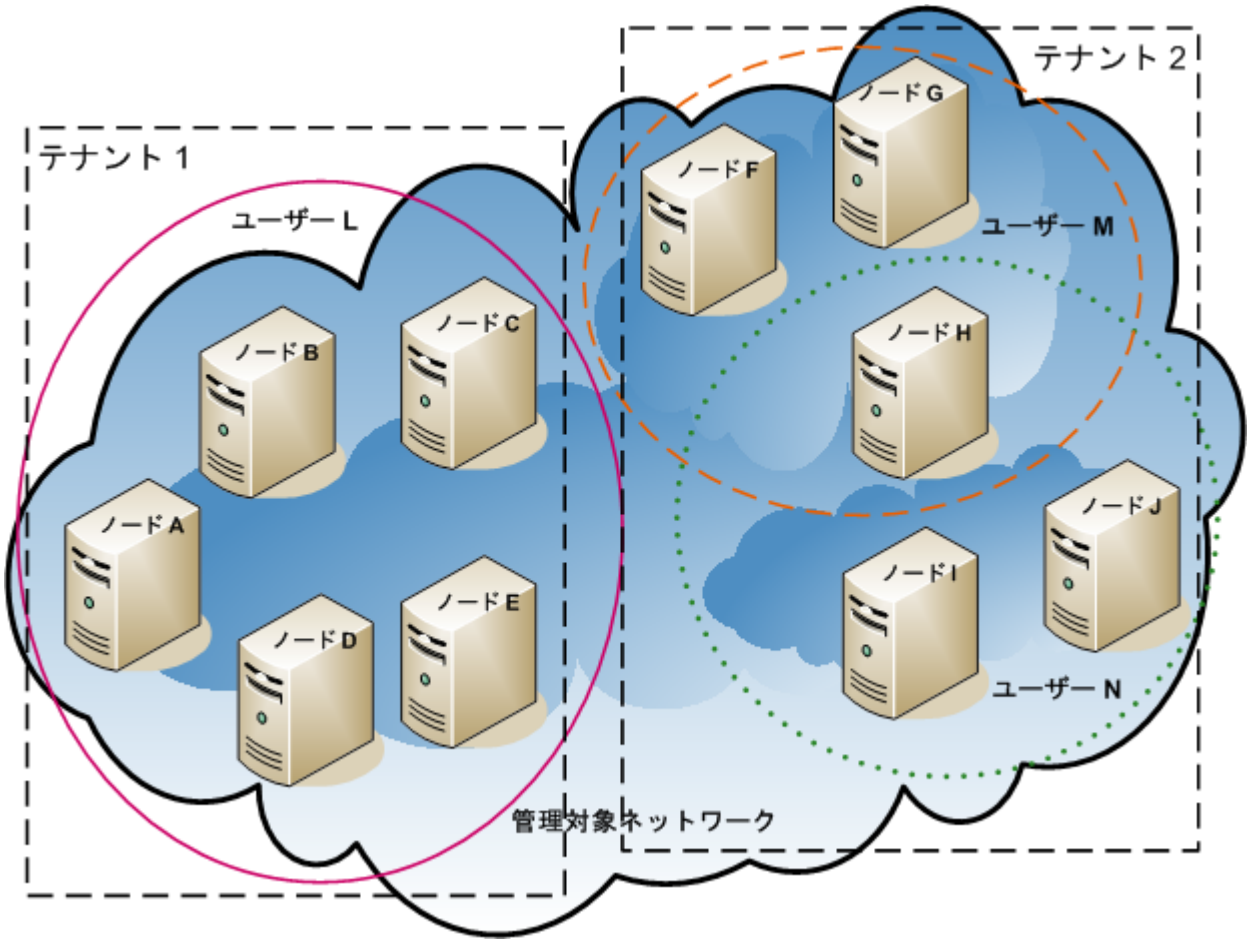


表 14　複数のテナントのセキュリティ グループ マッピングの例

セキュリティ グループ	セキュリティ グループのノード	ユーザー グループ	オブジェクト アクセス権限
T1 SG	A、B、C、D、E	T1 管理者	オブジェクト管理者
		T1 レベル 2	オブジェクト オペレータ レベル 2
		T1 レベル 1	オブジェクト オペレータ レベル 1
		T1 ゲスト	オブジェクト ゲスト
T2 SGa	F、G	T2_a 管理者	オブジェクト管理者
		T2_a レベル 2	オブジェクト オペレータ レベル 2
		T2_a レベル 1	オブジェクト オペレータ レベル 1
		T2_a ゲスト	オブジェクト ゲスト
T2 SGb	H	T2_b 管理者	オブジェクト管理者
		T2_b レベル 2	オブジェクト オペレータ レベル 2
		T2_b レベル 1	オブジェクト オペレータ レベル 1
		T2_b ゲスト	オブジェクト ゲスト
T2 SGc	I、J	T2_c 管理者	オブジェクト管理者
		T2_c レベル 2	オブジェクト オペレータ レベル 2
		T2_c レベル 1	オブジェクト オペレータ レベル 1
		T2_c ゲスト	オブジェクト ゲスト

表 15　複数のテナントのユーザー アカウント マッピングの例

ユーザー アカウント	ユーザー グループ	ノード アクセス	注
ユーザー L	NNMi レベル 2 オペレータ	なし	このユーザーには、テナント 1 のすべてのノードをグループ化する、ピンクの楕円形 (実線) に含まれるノードへのオペレータ レベル 2 のアクセス権限があります。
	T1 レベル 2	A、B、C、D、E	
ユーザー M	NNMi レベル 1 オペレータ	なし	このユーザーには、テナント 2 のノードのサブセットをグループ化する、オレンジの楕円形 (破線) に含まれるノードへのオペレータ レベル1のアクセス権限があります。
	T2_a レベル 1	F、G	
	T2_b レベル 1	H	
ユーザー N	NNMi レベル 2 オペレータ	なし	このユーザーには、テナント 2 のノードのサブセットをグループ化する、緑の楕円形 (点線) に含まれるノードへのオペレータ レベル2のアクセス権限があります。
	T2_b レベル 2	H	
	T2_c レベル 2	I、J	

NNMi のセキュリティおよびマルチテナント設定

NNMi のセキュリティおよびマルチテナント設定は、NNMi データベース全体に適用されます。NNMi 管理者であれば、すべてのテナントのすべてのオブジェクトへのオペレータアクセス権限を表示および設定できます。

NNMi 管理者が少なくとも 1 つのカスタムセキュリティグループを定義すると、**[セキュリティグループ]** がすべての **[ノード]** フォームに表示されます。また、**[ノード]** および **[カスタムノード]** インベントリビューの列としても表示されます。

NNMi 管理者が少なくとも 1 つのカスタムテナントを定義すると、**[テナント]** フィールドがすべての **[ノード]** フォームに表示されます。また、**[ノード]** および **[カスタムノード]** インベントリビューの列としても表示されます。

ノードグループ

セキュリティ設定またはマルチテナント設定の一部と適合するようにノードグループを作成するには、セキュリティグループ UUID、セキュリティグループ名、テナント UUID、またはテナント名に基づいて、ノードグループの追加フィルタを指定します。これらのノードグループを使用して、監視アクションおよびインシデントライフサイクル移行アクション用のポーリングサイクルを、セキュリティグループまたはテナントごとに設定します。

ベストプラクティス

セキュリティグループとテナントの名前は変更できるため、追加フィルタにはセキュリティグループまたはテナントの UUID を指定します。この情報は、設定フォームと、`nnmsecurity.ovpl` コマンド出力で使用できます。

ユーザーグループ : NNMi コンソールアクセス

事前に定義された NNMi ユーザーグループの 1 つにユーザーアカウントをマッピングすると、NNMi ロールと、NNMi コンソールで表示されるメニュー項目が設定されます。各ユーザーアカウントには、そのユーザーのトポロジオブジェクトに対する最も高いオブジェクトアクセス権限とに対応する NNMi ロールを付与することをお勧めします。

ただし、NNMi 管理者はすべてのトポロジオブジェクトへのアクセス権を持つため、管理者レベルの権限を付与することは避けてください。NNMi トポロジ内の一部のノードに対してのみ、NNMi コンソールユーザーを管理者として設定するには、そのユーザーを NNMi レベル 1 オペレータまたは NNMi レベル 2 オペレータのユーザーグループに割り当てます。また、オブジェクト管理者オブジェクトアクセス権限を使用して、トポロジ内のノードのサブセットを含むセキュリティグループにマッピングされたカスタムユーザーグループを作成し、ユーザーをそのグループに割り当てます。

ユーザーグループ : ディレクトリサービス

ユーザーグループメンバーシップを NNMi データベースに保存する場合、すべてのオブジェクトアクセス設定は、NNMi 設定エリア内で、ユーザーグループ、ユーザーアカウントマッピング、セキュリティグループ、およびセキュリティグループマッピングを使用して行われます。

ユーザーグループメンバーシップをディレクトリサービスに保存する場合、オブジェクトアクセス設定は、NNMi 設定 (セキュリティグループおよびセキュリティグループマッピング) と、ディレクトリサービスコンテンツ (ユーザーグループメンバーシップ) の間で共有されます。NNMi データベースに、ユーザーアカウントまたはユーザーアカウントマッピングを作成しないでください。ディレクトリサービス内の適用可能なグループごとに、NNMi データベースに 1 つ以上のユーザーグループを作成してください。NNMi で、各ユーザーグループ定義の **[ディレクトリサービス名]** フィールドに、ディレクトリサービス内のそのグループの識別名を設定します。

詳細については、163 ページの「NNMi と LDAP によるディレクトリ サービスの統合」を参照してください。

設定ツール

NNMi には、マルチテナントとセキュリティを設定するためのいくつかのツールが備わっています。

セキュリティウィザード

NNMi コンソールの **[セキュリティウィザード]** は、セキュリティ設定の可視化に役立ちます。NNMi コンソール内でノードをセキュリティグループに割り当てるには、このウィザードを使用する方法が最も簡単です。**[変更概要の表示]** ページには、現在のウィザードセッションで保存されていない変更点のリストが表示されます。また、セキュリティ設定に関する潜在的な問題も示されます。

[**セキュリティウィザード**] は、NNMi セキュリティ設定に関してのみ使用できます。テナント情報は含まれていません。

[セキュリティウィザード] の使用法の詳細については、ウィザード内の NNMi ヘルプリンクをクリックしてください。

NNMi コンソールフォーム

NNMi コンソール内の個々のセキュリティオブジェクトおよびマルチテナントオブジェクトのフォームは、設定の 1 つの側面を同時に集中的に捉える場合に便利です。これらのフォームの使用法の詳細については、各フォームの NNMi ヘルプを参照してください。

[テナント] ビューには NNMi マルチテナント設定情報が含まれています。このビューは、**[設定]** ワークスペースの **[検出]** の下に表示されます。各 **[テナント]** フォームには 1 つの NNMi テナントが記述され、現在そのテナントに割り当てられているノードが表示されます。ノードの割り当て情報は読み取り専用です。

ノードに割り当てられているテナントまたはセキュリティグループを変更するには、**[ノード]** フォームまたは `nnmsecurity.ovpl` コマンドを使用します。

以下の NNMi コンソールビューは、**[設定]** ワークスペースの **[セキュリティ]** の下に表示されます。これらのビューには、以下の NNMi セキュリティ設定情報が含まれています。

- **ユーザーアカウント**
  - 各 **[ユーザーアカウント]** フォームには 1 つの NNMi ユーザーが記述され、そのユーザーが属するユーザーグループが表示されます。メンバーシップ情報は読み取り専用です。
  - ユーザーグループメンバーシップをディレクトリサービスに保存すると、ユーザーアカウントは NNMi コンソールに表示されません。
- **ユーザー グループ**

  各 **[ユーザーグループ]** フォームには 1 つの NNMi ユーザーグループが記述され、そのユーザーグループにマッピングされたユーザーアカウントとセキュリティグループが表示されます。マッピング情報は読み取り専用です。
- **ユーザーアカウントのマッピング**
  - 各 **[ユーザーアカウントのマッピング]** フォームには、1 つのユーザーアカウントとユーザーグループの関連付けが表示されます。
  - ユーザーアカウントマッピングに変更を行っても、現在の NNMi コンソールユーザーにその変更は反映されません。現在のユーザーは、NNMi コンソールに次回ログオンしたときに、変更を受け取ります。
  - ユーザーグループメンバーシップをディレクトリサービスに保存すると、ユーザーアカウントマッピングは NNMi コンソールに表示されません。
- **セキュリティ グループ**

  各 **[セキュリティグループ]** フォームには 1 つの NNMi セキュリティグループが記述され、そのセキュリティグループに現在割り当てられているノードが表示されます。ノードの割り当て情報は読み取り専用です。

- **セキュリティグループのマッピング**
  - 各 **[セキュリティグループのマッピング]** フォームには、1 つのユーザーグループとセキュリティグループの関連付けが表示されます。
  - 初期設定の後、セキュリティグループマッピングに関連付けられたオブジェクトのアクセス権限は読み取り専用になっています。セキュリティグループマッピングのオブジェクトアクセス権限を変更するには、そのマッピングを削除して、再度作成します。

コマンドライン

nnmsecurity.ovpl コマンドラインインタフェースは、自動操作や一括操作を行う場合に便利です。このツールは、セキュリティ設定に関する潜在的な問題のレポートも提供します。

nnmsecurity.ovpl オプションの多くは、カンマ区切り値 (CSV) ファイルからの入力データのロードをサポートしています。設定データは、nnmsecurity.ovpl コマンドで使用するために、CSV 出力を生成できるファイルまたはシステムに保持できます。このコマンドは、NNMi の外部で生成された UUID も受け入れます。

ベストプラクティス

セキュリティグループとテナントの名前は一意である必要はないため、nnmsecurity.ovpl コマンドへの入力値としてセキュリティグループまたはテナントの UUID を指定します。

以下のスクリプト例では、nnmsecurity.ovpl コマンドを使用して、2 つのユーザーアカウントと 5 つのノードにセキュリティ設定を作成しています。

```
#!/bin/sh
# 2 つのユーザーを作成する
nnmsecurity.ovpl -createUserAccount user1 -password password -role level1
nnmsecurity.ovpl -createUserAccount user2 -password password -role level2

# 2 つのグループを作成する
nnmsecurity.ovpl -createUserGroup local1
nnmsecurity.ovpl -createUserGroup local2

# 新しいユーザー グループにユーザー アカウントを割り当てる
nnmsecurity.ovpl -assignUserToGroup -user user1 -userGroup local1
nnmsecurity.ovpl -assignUserToGroup -user user2 -userGroup local2

# 2 つのセキュリティ グループを作成する
nnmsecurity.ovpl -createSecurityGroup secgroup1
nnmsecurity.ovpl -createSecurityGroup secgroup2

# 新しいセキュリティ グループに新しいユーザー グループを割り当てる
nnmsecurity.ovpl -assignUserGroupToSecurityGroup -userGroup local1 ¥
  -securityGroup secgroup1 -role level1
nnmsecurity.ovpl -assignUserGroupToSecurityGroup -userGroup local2 ¥
  -securityGroup secgroup2 -role level2

# セキュリティ グループをノードに割り当てる
nnmsecurity.ovpl -assignNodeToSecurityGroup -node mplspe01 -securityGroup secgroup1
nnmsecurity.ovpl -assignNodeToSecurityGroup -node vwan_router-1 -securityGroup secgroup1
nnmsecurity.ovpl -assignNodeToSecurityGroup -node vwan_router-2 -securityGroup secgroup1
nnmsecurity.ovpl -assignNodeToSecurityGroup -node data_center_1 -securityGroup secgroup2
nnmsecurity.ovpl -assignNodeToSecurityGroup -node mplspe03 -securityGroup secgroup2
```

テナントの設定

NNMi では、以下の方法でマルチテナントを設定できます。

- NNMi コンソールの **[テナント]** フォームは、個々のテナントを処理する際に役立ちます。
- nnmsecurity.ovpl コマンドラインインタフェースは、自動操作や一括操作を行う場合に便利です。このツールは、テナント設定に関する潜在的な問題のレポートも提供します。

各 NNMi トポロジオブジェクトをテナント (組織) に割り当てるために NNMi マルチテナントを定義および設定するプロセスは、循環的なプロセスです。この概略的な手順では、NNMi マルチテナントを設定するための 1 つの方法を説明します。

NNMi マルチテナントの設定に関しては、以下に注意してください。

- 検出されたノードに NNMi によって割り当てられるセキュリティグループは、そのノードに関連付けられたテナントの [初期検出セキュリティグループ] の値によって設定されます。
- NNMi テナントを設定しないで、NNMi セキュリティモデルを使用すると、すべてのノードがデフォルトテナントに割り当てられます。
- NNMi 検出用にノードをシードするときに、そのノードが属するテナントを指定できます。自動検出ルールを使用して NNMi でノードが検出されると、NNMi によってそのノードはデフォルトテナントに割り当てられます。検出後、ノードに対するテナントの割り当てを変更できます。

NNMi マルチテナントを計画および設定するための概略的な方法を以下に示します。

1. ユーザー要件を分析して、NNMi 環境で必要なテナントの数を判別します。

   1 つの NNMi 管理サーバーで複数のネットワークを個々に管理する場合のみ、テナントを使用することをお勧めします。

2. 管理対象のネットワークトポロジを分析して、各テナントにどのノードが属するかを判別します。
3. 各テナントのトポロジを分析して、NNMi ユーザーがアクセスする必要のあるノードのグループを判別します。
4. 事前に定義された NNMi ユーザーグループと、[デフォルトセキュリティグループ] および [未解決のインシデント] セキュリティグループの間のデフォルトの関係を削除します。

   この手順により、ユーザーが管理してはならないノードへのアクセス権が、そのユーザーに間違って付与されることがないようにします。この時点では、NNMi トポロジ内のオブジェクトにアクセスできるのは NNMi 管理者のみです。

5. 特定されたテナントを設定します。
   a. 特定されたセキュリティグループを作成します。
   b. 特定されたテナントを作成します。

      テナントごとに、[デフォルトセキュリティグループ]、またはアクセスが制限されたテナント固有のセキュリティグループのいずれかに、[初期検出セキュリティグループ] を設定します。これを行うことで、NNMi 管理者がアクセス権を設定するまで、テナントの新しいノードが全体に表示されることはなくなります。

6. テナントをシードに割り当てて、検出の準備を行います。

   ノードのグループを検出した後、[初期検出セキュリティグループ] の値を変更できます。これを行うことで、ノードをセキュリティグループに手動で再割り当てする処理が制限されます。

7. 検出が完了したら、以下を実行します。
   - ノードごとにテナントを確認し、必要に応じて変更します。
   - ノードごとにセキュリティグループを確認し、必要に応じて変更します。
8. 208 ページの手順 4 を継続します。

セキュリティ グループの設定

NNMi をディレクトリサービスと統合して、ユーザー名、パスワード、およびオプションとして NNMi ユーザーグループの割り当ての保管場所を統合する場合は、NNMi セキュリティを設定する前に、その統合の設定を実行してください。

NNMi では、以下の方法でセキュリティを設定できます。

- NNMi コンソールの **[セキュリティウィザード]** は、セキュリティ設定の可視化に役立ちます。**[変更概要の表示]** ページには、現在のウィザードセッションで保存されていない変更点のリストが表示されます。また、セキュリティ設定に関する潜在的な問題も示されます。
- 個々のセキュリティオブジェクトに対応した NNMi コンソールのフォームは、セキュリティ設定の 1 つの側面を同時に集中的に捉える場合に便利です。
- `nnmsecurity.ovpl` コマンドラインインタフェースは、自動操作や一括操作を行う場合に便利です。このツールは、セキュリティ設定に関する潜在的な問題のレポートも提供します。

NNMi トポロジ内のオブジェクトに対するユーザーのアクセス権を制限するために NNMi セキュリティを定義および設定するプロセスは、循環的なプロセスです。この概略的な手順では、NNMi セキュリティを設定するための 1 つの方法を説明します。

この例では、セキュリティグループからユーザーアカウントに移動します。たとえば、ユーザーアカウントからセキュリティグループに NNMi セキュリティを設定する場合、NNMi ヘルプで「セキュリティの設定例」を検索してください。

NNMi セキュリティの設定に関しては、以下に注意してください。

- 検出されたノードに NNMi によって割り当てられるセキュリティグループは、そのノードに関連付けられたテナントの [初期検出セキュリティグループ] の値によって設定されます。
- NNMi テナントを設定しないで、NNMi セキュリティモデルを使用すると、すべてのノードがデフォルトテナントに割り当てられます。

NNMi セキュリティを計画および設定するための概略的な方法を以下に示します。

1. 管理対象のネットワークトポロジを分析して、NNMi ユーザーがアクセスする必要のあるノードのグループを判別します。
2. 事前に定義された NNMi ユーザーグループと、[デフォルトセキュリティグループ] および [未解決のインシデント] セキュリティグループの間のデフォルトの関係を削除します。

   この手順により、ユーザーが管理してはならないノードへのアクセス権が、そのユーザーに間違って付与されることがないようにします。この時点では、NNMi トポロジ内のオブジェクトにアクセスできるのは NNMi 管理者のみです。
3. ノードの各サブセットのセキュリティ グループを設定します。特定のノードは 1 つのセキュリティ グループにのみ属することができます。
   a. セキュリティ グループを作成します。
   b. 適切なノードを各セキュリティ グループに割り当てます。

4 カスタムユーザーグループを設定します。

a セキュリティ グループごとに、NNMi ユーザー アクセスの各レベルに対応するユーザー グループを設定します。

— ユーザーグループメンバーシップを NNMi データベースに保存しても、それらのユーザーグループにユーザーはマッピングされません。

— ユーザーグループメンバーシップをディレクトリサービスに保存する場合は、各ユーザーグループの [ディレクトリサービス名] フィールドに、ディレクトリサービス内のそのグループの識別名を設定します。

b 各カスタムユーザーグループを、適切なセキュリティグループにマッピングします。マッピングごとに適切なオブジェクト アクセス権限を設定します。

5 ユーザー アカウントを設定します。

- ユーザーグループメンバーシップを NNMi データベースに保存する場合は、以下の手順を実行します。

  — NNMi コンソールへのアクセス権を持つ必要のあるユーザーごとに、ユーザーアカウントオブジェクトを作成します (ユーザーアカウントを設定するプロセスは、NNMi コンソールログオンにディレクトリサービスを使用しているかどうかによって異なります)。

  — 各ユーザーアカウントを、(NNMi コンソールにアクセスするために) 事前に定義した NNMi ユーザーグループの 1 つにマッピングします。

  — 各ユーザーアカウントを (トポロジオブジェクトにアクセスするために) 1 つ以上のカスタム NNMi ユーザーグループにマッピングします。

- ユーザーグループメンバーシップをディレクトリサービスに保存する場合、各ユーザーが、事前に定義された NNMi ユーザーグループの 1 つ、および 1 つ以上のカスタムユーザーグループに属していることを確認します。

6 208 ページの「設定の確認」の説明に従って、設定を確認します。

7 セキュリティ設定を管理します。

- [デフォルトセキュリティグループ] に追加されたノードに注目し、これらのノードを適切なセキュリティグループに移動します。
- 新しい NNMi コンソールユーザーを適切なユーザーグループに追加します。

設定の確認

セキュリティ設定が適切であるかを確認するために、設定の各側面を別個に確認します。このセクションでは、設定を確認するためのいくつかの方法を説明します。ここに記載されていない方法も使用できます。

NNMi には、潜在的なセキュリティ設定エラーのレポートが備わっています。これらのレポートには、NNMi コンソールの **[ツール] > [セキュリティレポート]** で、`-displayConfigReport` オプションを `nnmsecurity.ovpl` コマンドに設定してアクセスします。

セキュリティグループとノード間の割り当てを確認する

各ノードが適切なセキュリティグループに割り当てられていることを確認する方法の1つとして、セキュリティグループごとに **[ノード]** または **[カスタムノード]** インベントリビューをソートし、グループ分けを調べる方法があります。

また、`-listNodesInSecurityGroup` オプションを `nnmsecurity.ovpl` コマンドに指定して使用することもできます。

ユーザーグループとセキュリティグループ間の割り当てを確認する

どのユーザーグループが各セキュリティグループにマッピングされているかを確認する方法の 1 つとして、ユーザーグループまたはセキュリティグループごとに **[セキュリティグループのマッピング]** ビューをソートして、グループ分けを調べる方法があります。また、各マッピングのオブジェクトアクセス権限も確認します。

あるいは、**[セキュリティウィザード]** の **[ユーザーグループをセキュリティグループにマッピングする]** ページで、同時に 1 つのユーザーグループまたはセキュリティグループを選択して、そのオブジェクトに対する現在のマッピングを確認します。

また、`-listUserGroupsForSecurityGroup` オプションを `nnmsecurity.ovpl` コマンドに指定して使用することもできます。

各ユーザーが NNMi コンソールアクセス権を持っているかを確認する

NNMi コンソールアクセス権について、事前に設定された NNMi ユーザーグループの 1 つに各ユーザーが割り当てられていることを確認します。

- NNMi 管理者
- NNMi レベル 1 オペレータ
- NNMi レベル 2 オペレータ
- NNMi ゲスト ユーザー

その他のすべてのユーザーグループ割り当てで、NNMi データベースのオブジェクトへのアクセス権が付与されます。

NNMi コンソールアクセス権を持たないユーザーは、**[セキュリティウィザード]** の **[変更概要の表示]** ページにリストされます。**[ツール] > [セキュリティレポート]** メニュー項目で、`-displayConfigReport usersWithoutRoles` オプションを `nnmsecurity.ovpl` コマンドに設定して、この情報を得ることもできます。

ユーザーとユーザーグループ間の割り当てを確認する

ユーザーグループメンバーシップを確認する方法の 1 つとして、ユーザーアカウントまたはユーザーグループごとに **[ユーザーアカウントのマッピング]** ビューをソートして、グループ分けを調べる方法があります。

あるいは、**[セキュリティウィザード]** の **[ユーザーアカウントとユーザーグループのマップ]** ページで、同時に 1 つのユーザーアカウントまたはユーザーグループを選択して、そのオブジェクトに対する現在のマッピングを確認します。

また、`-listUserGroups` オプションと `-listUserGroupMembers` オプションを `nnmsecurity.ovpl` コマンドに指定して使用することもできます。

テナントとノード間の割り当てを確認する

各ノードが適切なテナントに割り当てられていることを確認する方法の 1 つとして、テナントごとに **[ノード]** または **[カスタムノード]** インベントリビューをソートし、グループ分けを調べる方法があります。

現在のユーザー設定を確認する

現在ログオンしているユーザーの NNMi コンソールアクセス権を確認するには、**[ヘルプ] > [システム情報]** をクリックします。**[製品]** タブの **[ユーザー情報]** セクションに、現在の NNMi セッションに関する以下の情報がリストされます。

- NNMi データベースのユーザーアカウント、またはアクセス対象のディレクトリサービスに定義されているユーザー名。
- NNMi ロール。これは、ユーザーがマッピングされる、事前に定義された NNMi ユーザーグループ (NNMi 管理者、NNMi レベル 1 オペレータ、NNMi レベル 2 オペレータ、および NNMi ゲストユーザー) の中で最も高い権限を持つものに対応します。このマッピングによって、NNMi コンソールで使用できるアクションが決まります。
- このユーザー名にマッピングされたユーザーグループ。このリストには、NNMi ロールを設定する事前に設定された NNMi ユーザーグループと、NNMi データベース内のオブジェクトへのアクセス権を付与するその他のすべてのユーザーグループが含まれています。

NNMiのセキュリティおよびマルチテナント設定のエクスポート

表 16 は、NNMi のセキュリティおよびマルチテナント設定をエクスポートするための設定エリア (nnmconfigexport.ovpl -c で使用可能) を示しています。これらのエクスポートエリアは、特にグローバルネットワーク管理環境で、複数の NNMi 管理サーバーにわたって設定を管理するのに役立ちます。

表 16　NNMi のセキュリティおよびマルチテナント設定のエクスポートエリア

設定エリア	説明
アカウント	ユーザーアカウント、ユーザーグループ、およびユーザーアカウントとユーザーグループ間のマッピングをエクスポートします。 複数の NNMi データベースにわたってユーザー定義を共有するのに便利です。
security	テナントおよびセキュリティグループをエクスポートします。 複数の NNMi データベースにわたってセキュリティ定義を共有するのに便利です。 この情報をインポートすると、新しいオブジェクトが作成され、既存のオブジェクトが更新されますが、現在のエクスポートに含まれていないオブジェクトは削除されません。このため、ローカルで定義されたオブジェクトが NNMi データベースに含まれている場合でも、このオプションは安全に使用できます。
securitymappings	ユーザーグループとセキュリティグループ間のマッピングをエクスポートします。 セキュリティとマルチテナント設定を完全にエクスポートするには、account、security、および securitymappings 設定エリアの同時エクスポートを実行してください。

NNMi セキュリティ、マルチテナント、およびグローバル ネットワーク管理

グローバルネットワーク管理 (GNM) 環境では、ノードのテナントは、そのノードを管理する NNMi 管理サーバーに設定されます。GNM 環境では、指定されたノードのテナント UUID は各グローバルマネージャとリージョナルマネージャで同じです。

ノードのセキュリティグループは、トポロジにそのノードが含まれる各 NNMi 管理サーバーに設定されます。したがって、トポロジ内のオブジェクトへのユーザーアクセスは、GNM 環境の各 NNMi 管理サーバーに別個に設定されます。グローバルマネージャとリージョナルマネージャが使用するセキュリティグループ定義は、同じである場合も、異なる場合もあります。

グローバルマネージャとリージョナルマネージャに同様のユーザーアクセスを設定する場合、いくつかの裏技を使用して設定することもできますが、大部分の場合、各 NNMi 管理サーバーにカスタム設定を行う必要があります。

ベストプラクティス　グローバルマネージャにすべてのテナントとセキュリティグループを定義します。`nnmconfigexport.ovpl -c security` を使用して、テナントとセキュリティグループ定義をエクスポートします。各リージョナルマネージャで、`nnmconfigimport.ovpl` を使用してテナントとセキュリティグループ定義をインポートします。　あるいは、`nnmsecurity.ovpl` コマンドを使用して、別の NNMi 管理サーバーの UUID と同じ UUID を使用して、テナントおよびセキュリティグループを作成することができます。この推奨手順に従うことで、GNM 環境内で、各テナントとセキュリティグループの UUID を同じにすることができます。

- ユーザーがグローバルマネージャから NPS レポートを開始する場合、このベストプラクティスは設定の*必須*部分になります。
- テナント UUID は一意である必要がありますが、テナント名は再利用できます。NNMi は、名前が同じで UUID が異なる 2 つのテナントを、共有設定を持たない 2 つの別個のテナントであると見なします。

ベストプラクティス　組織ごとに 1 つのリージョナルマネージャをセットアップする場合は、リージョナルマネージャのすべてのノードを 1 つのテナントに入れることができます。ただし、各リージョナルマネージャに一意のテナントを設定し、グローバルマネージャでトポロジデータが確実に分離されるようにしてください。

リージョナルマネージャからグローバルマネージャに転送されたインシデントに、セキュリティ情報とテナント情報を伝達するいくつかの追加カスタムインシデント属性 (CIA) が含まれる場合があります。

このようなインシデントのソースオブジェクトがデフォルトテナント以外のテナントに属している場合、転送されるインシデントには以下の CIA が含まれます。

- cia.tenant.name
- cia.tenant.uuid

このようなインシデントのソースオブジェクトが [デフォルトセキュリティグループ] 以外のセキュリティグループに属している場合、転送されるインシデントには以下の CIA が含まれます。

- cia.securityGroup.name
- cia.securityGroup.uuid

この項では以下の内容について説明します。

- 211 ページの「初期 GNM 設定」
- 213 ページの「GNM のメンテナンス」

初期 GNM 設定

GNM の初期設定後、リージョナルマネージャは、(GNM 設定に従って) リージョナルトポロジ内のノードに関する情報を使用して、グローバルマネージャを更新します。

デフォルトテナントのみとのトポロジの同期

カスタムセキュリティグループとデフォルトテナントを持つ GNM 環境の場合、グローバルマネージャでは、リモートで管理されているすべてのノードが、以下の設定でグローバルマネージャトポロジに追加されます。

- デフォルトテナント
- デフォルトテナントの [初期検出セキュリティグループ] として設定されるセキュリティグループ。

カスタムテナントとのトポロジの同期

カスタムセキュリティグループとカスタムテナントを持つ GNM 環境の場合、グローバルマネージャでは、リモートで管理されているすべてのノードが、そのノードに割り当てられているテナントの UUID を使用して、グローバルマネージャトポロジに追加されます。そのテナント UUID がグローバルマネージャにない場合、以下のように、GNM プロセスによってグローバルマネージャの NNMi 設定にテナントが作成されます。

- このテナント UUID は、リージョナルマネージャの場合と同じ値です。
- テナント名は、リージョナルマネージャの場合と同じ値です。
- [初期検出セキュリティグループ] の値は、テナントと同じ名前のセキュリティグループに設定されます (このセキュリティグループがグローバルマネージャにない場合、NNMi によってそのセキュリティグループが作成されます)。

グローバルマネージャのトポロジにノードが追加されると、そのノードは、グローバルマネージャに設定されたテナント UUID に対応する [初期検出セキュリティグループ] に割り当てられます。このため、グローバルマネージャ上でのセキュリティグループの関連付けは、リージョナルマネージャ上でのセキュリティグループの関れ付けから独立しています。

ベストプラクティス

グローバルマネージャでのセキュリティ設定を簡素化するために、以下をお勧めします。

- 各リージョナルマネージャによって管理されるノードのスプレッドシートまたはその他のレコードを保持します。ノードごとに、リージョナルマネージャとグローバルマネージャのそれぞれに必要なセキュリティグループをメモしておきます。GNM 設定が完了したら、`nnmsecurity.ovpl` コマンドを使用して、セキュリティグループの割り当ての確認および更新を行います。
- GNM 環境で、複数のリージョナルマネージャによって 1 つのグローバルマネージャが更新されている場合、そのグローバルマネージャーに対して GNM 設定を有効にするには、各リージョナルマネージャから 1 つずつ設定を行ってください。

  該当する場合は、各リージョナルマネージャを GNM 設定に追加する前に、デフォルトテナント (またはカスタムテナント) の [初期検出セキュリティグループ] の値を変更できます。これを実行した場合、以前に設定されたリージョナルマネージャのトポロジに新しいノードが追加されると、さまざまな結果が生じる可能性があることに注意してください。
- GNM を有効にする前に、グローバルマネージャ上で、リージョナルマネージャで使用される各テナントの [初期検出セキュリティグループ] を、オペレータがアクセスできない専用セキュリティグループに設定してください。これにより、グローバルマネージャ上の管理者は、ほかの NNMi コンソールオペレータのために、ノードを適切なセキュリティグループに明示的に移動しなくてはならなくなります。

GNM のメンテナンス

表 17は、リージョナルマネージャでのノードのテナントまたはセキュリティグループの割り当てへの変更が、グローバルマネージャにどのように影響を及ぼすかを示しています。

表 17　リージョナルマネージャでの設定変更がグローバルマネージャに及ぼす影響

アクション	影響
リージョナルマネージャで、ノードを別のテナントに割り当てる。	グローバルマネージャのノードは、その別のテナントに割り当てられるように変更されます。このテナント UUID がグローバルマネージャにない場合は作成されます。
リージョナルマネージャで、ノードを別のセキュリティグループに割り当てる。	グローバルマネージャでは変更は行われません。NNMi 管理者は、その変更を手動で複製するように選択できます。
リージョナルマネージャで、テナントの設定 (名前、説明、または初期検出セキュリティグループ) を変更する。	グローバルマネージャでは変更は行われません。NNMi 管理者は、その変更を手動で複製するように選択できます。
リージョナルマネージャで、セキュリティグループの設定 (名前または説明) を変更する。	グローバルマネージャでは変更は行われません。NNMi 管理者は、その変更を手動で複製するように選択できます。

NPS レポートへの選択インタフェースの追加

デフォルトで、ノードのすべてのコンポーネントは、そのノードと同じセキュリティグループに属します。個々のインタフェースに対して、このデフォルトの動作をオーバーライドし、インタフェースを別のセキュリティグループに割り当てることができます。このオーバーライドは、共有デバイスのテナント (顧客) 向けの適切なインタフェースを含むテナント固有のレポートを生成するために行います。このようにすると、各顧客には、自分のインタフェースに関するインタフェース情報が表示され、デバイス上のほかのインタフェースは表示されないようになります。

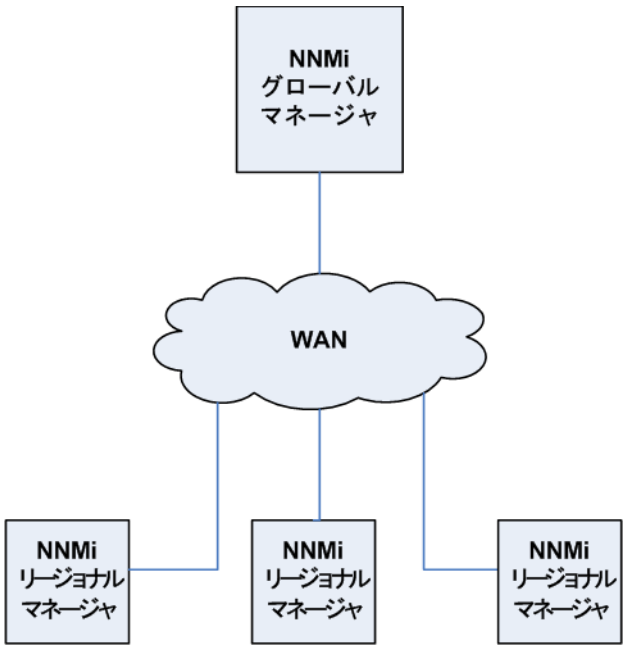
セキュリティグループのオーバーライドは、NPS レポートにのみ反映されます。NNMi コンソールでユーザーに表示される内容や、ユーザーが実行できる事柄には影響は及ぼされません。

インタフェースのセキュリティグループ割り当てを変更するには、**[インタフェース]** フォームの **[カスタム属性]** タブ、または `nnmloadattributes.ovpl` コマンドを使用して、`InterfaceSecurityGroupOverride` カスタム属性をインタフェースに追加します。このカスタム属性の値をセキュリティグループの UUID に設定します。たとえば、以下のようにします。

```
InterfaceSecurityGroupOverride=0826c95c-5ec8-4b8c-8998-301e0cf3c1c2
```

インタフェースは、同時に 1 つのセキュリティグループにしか属すことができません。インタフェースに `InterfaceSecurityGroupOverride` カスタム属性を設定すると、そのインタフェースと、ノードが属するセキュリティグループの間の関連付けが壊れます。

グローバル ネットワーク管理



この章には、以下のトピックがあります。

- グローバル ネットワーク管理の利点
- グローバル ネットワーク管理が自分のネットワークの管理に適しているかどうかを判断するには？
- 実践的なグローバル ネットワーク管理の例
- 要件のレビュー
- 初期準備
- グローバル ネットワーク管理用にシングル サインオンを設定する
- リージョナル マネージャでの転送フィルタの設定
- グローバル マネージャとリージョナル マネージャの接続
- `global1` から `regional1` と `regional2` への 接続ステータスの判定
- global1 インベントリの確認
- `global1` と `regional1` との通信の切断
- 追加情報
- グローバル ネットワーク管理でアプリケーション フェイルオーバーの設定を行う
- グローバル ネットワーク管理のトラブルシューティングのヒント
- グローバル ネットワーク管理と NNM iSPI または第三者の統合

グローバル ネットワーク管理の利点

HP Network Node Manager i Software (NNMi) を地理的位置が異なる複数の NNMi 管理サーバーに導入しているとします。各 NNMi 管理サーバーでは、検出と監視のニーズに合うように、ネットワークの検出および監視を行っています。こうした既存の NNMi 管理サーバーと設定を使用して、特定の NNMi 管理サーバーをグローバル マネージャとして指定することで、新たな検出を追加したり監視の設定を変更したりせずに、集約したノード オブジェクト データを表示することができます。

NNMi グローバル ネットワーク管理機能により、地理的位置が異なるネットワークを管理しながら、複数の NNMi 管理サーバーを連携させることができます。特定の NNMi 管理サーバーをグローバル マネージャとして指定し、複数のリージョナル マネージャを集約したノード オブジェクト データを表示します。

NNMi グローバル ネットワーク管理機能には、以下の利点があります。

- グローバル マネージャから見た、企業のネットワークの全体像を表示できます。
- 以下のように容易に設定できます。
  - リージョナル　マネージャの管理者はそれぞれ、すべてのノード　オブジェクト データを指定するか、またはグローバル マネージャ レベルで参加する特定のノード グループを指定します。
  - 各グローバル　マネージャの管理者は、情報の提供を許可するリージョナル　マネージャを指定します。
- 各サーバーごとに、インシデントの生成と管理を行うことができます (各サーバーで使用可能なトポロジのコンテキスト内で生成されます)。

詳細については、NNMi ヘルプの「*NNMi のグローバル ネットワーク管理機能*」を参照してください。

グローバル ネットワーク管理が自分のネットワークの管理に適しているかどうかを判断するには？

以下の質問に答えることで、NNMi のグローバル ネットワーク管理機能が自分のネットワーク管理に役立つかどうかを判断できます。

マルチサイト ネットワークを継続的に監視する必要がありますか？

IT グループは、複数のサイトに配備されているネットワーク機器を 週 7 日、24 時間体制で管理していますか ? NNMi のグローバル ネットワーク管理機能を使用すれば、トポロジとインシデントを集約して表示し、監視することができるようになります。

重要デバイスを表示できるか？

複数の場所に配備された重要デバイスのステータスとインシデントを、1 つの NNMi 管理サーバーで表示できますか ? はい。リージョナル マネージャに転送フィルタを設定します。このフィルタにより、リージョナル マネージャからグローバル マネージャに送信するノード オブジェクト データを選択できます。たとえば、リージョナル マネージャに対し転送フィルタを設定して、重要デバイスに関する情報のみをグローバル マネージャに転送するようにできます。

ライセンスの考慮事項

NNMi ライセンス キーの取得とインストールの詳細については、115 ページの「NNMi ライセンスの取得」を参照してください。

グローバル マネージャ、リージョナル マネージャ両方について NNMi Advanced ライセンスが必要ですか？ グローバル マネージャとして使用する NNMi 管理サーバーには、NNMi Advanced ライセンスを購入してインストールする必要があります。NNMi 管理サーバーをリージョナル マネージャとして使用する場合は、NNMi ライセンスは必要ありません。

1 つの地域をカバーするのに十分な NNMi ライセンスを持っています。グローバル ネットワーク管理機能を使用しながら、グローバル マネージャに必要な新しいライセンスの数を抑えることはできますか？ はい。IT グループが複数のサイトに配備された重要な装置をモニタする必要がある場合は、リージョナル マネージャに転送フィルタを設定して、グローバル マネージャに重要な装置に関する情報のみが転送されるようにすることができます。このようなフィルタ設定を使用することで、既存のグローバルマネージャのライセンスを最大限に活用し、NNMi への投資を無駄なく使用できます。

ライセンスを取得したノードの総数がグローバル マネージャの NNMi Advanced ライセンスより多くなるように、リージョナル マネージャ用に NNMi ライセンスを増やしました。グローバル マネージャには、すべての領域のすべてのノードの完全なインベントリがありません。十分なライセンスをグローバル マネージャ用に購入した後で、グローバル マネージャをすべてのリージョナル マネージャと同期させて、ライセンスが不十分だったために前回省略したノードを検索して作成するにはどうしたら良いでしょうか？ グローバル マネージャで十分な NNMi Advanced ライセンスを購入してインストールし、リージョナル マネージャでインストールしたライセンス総数を上回るようにする必要があります。十分なライセンスをインストールしたら、以下のいずれかを実行します。

- すべてのリージョナル マネージャで設定されている、すべての再検出間隔の時間が経過して、すべての領域ですべてのノードが再検出されるのを待機します。リージョナル マネージャは、すべての領域ですべてのノードを再検出したら、再検出されたノードの情報をグローバル マネージャに送信します。グローバル マネージャはこのノード情報を受信し、各領域でノードごとにグローバル ノードを作成します。
- 各リージョナル マネージャで **nnmnoderediscover.ovpl -all** スクリプトを実行します。

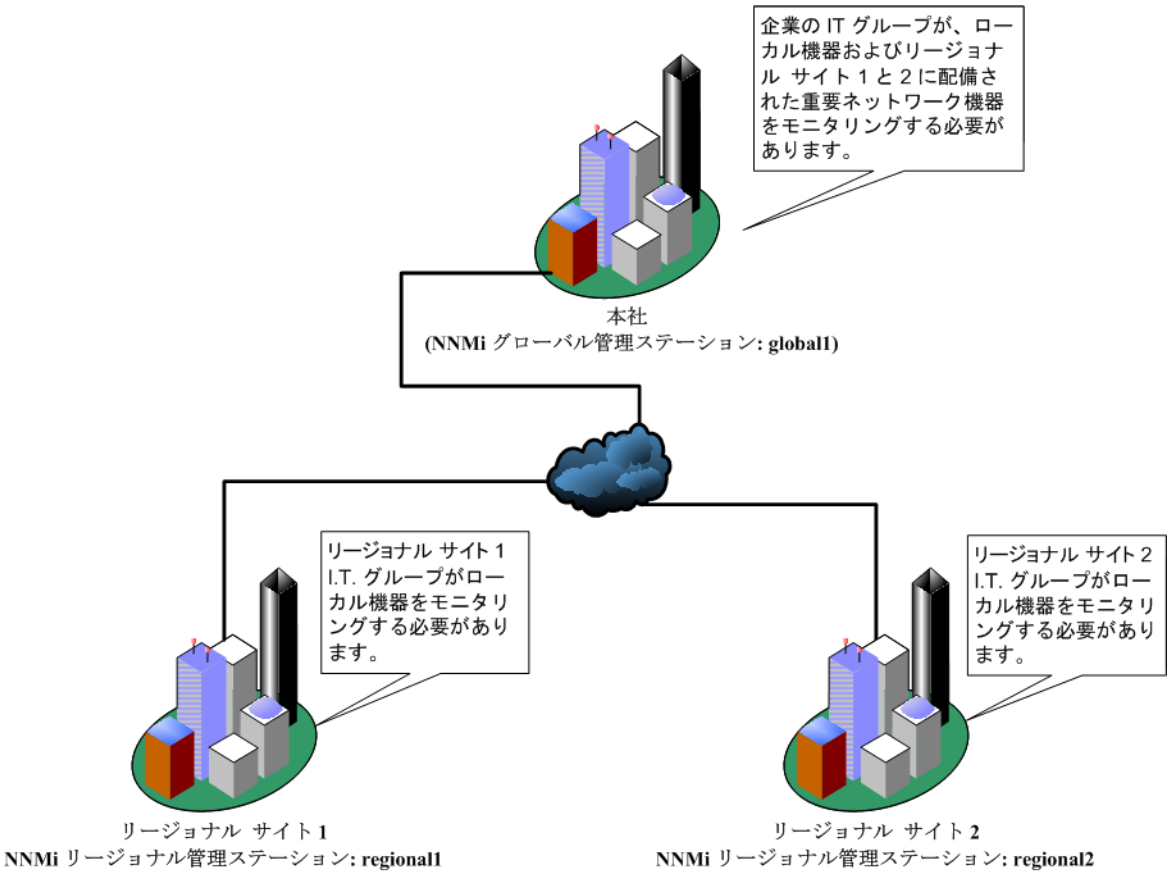
2 番目のオプションでは、ネットワーク上のトラフィックが増加し、NNMi マネージャのセット全体から多くの NNMi リソースが消費されることにもなります。このオプションは、最初の NNMi 検出ほどリソースの多くを消費しませんが、最初の検出を実行することに似ています。最適な方法では、ある程度の時間をおくか、現在のリージョナル マネージャの負荷が減って正常になるのを待ち、領域ごとに間隔をおいてスクリプトを実行してから、次のリージョナル マネージャの再検出を始めます。

実践的なグローバル ネットワーク管理の例

218 ページ の図 15を参照してください。地理的位置が異なる 2 つの運用サイトがあるとします。本社は、運用サイトとは別の地理的位置にあります。つまり、全部で 3 か所で NNMi 管理サーバーが機能しています。

本社の IT 担当者が、ローカル ネットワーク機器およびリージョナル サイト 1 と 2 の両方に配備された重要ネットワーク機器を、ネットワークの観点から監視する必要があります。リージョナル サイト 1 と 2 両方の IT 担当者は、そぞれのサイトに配備されている重要なネットワーク機器を監視する必要があります。

図 15　　ネットワークの例



要件のレビュー

本社、リージョナル サイト 1、リージョナル サイト 2 の NNMi 管理サーバーが、それぞれのサイトに配備された複数のルーターとスイッチを管理すると想定します。この例では、NNMi 管理サーバーをそれぞれ `global1`、`regional1` および `regional2` と呼びます。それぞれの場所に配備された重要なスイッチとルーターの検出と監視を行うように NNMi 管理サーバーを設定したとします。グローバル ネットワーク管理機能を使用するために、これらのサイトにある NNMi 管理サーバーでの検出を再設定する必要はありません。

グローバル ネットワーク管理機能の設定中、**`nnmbackup.ovpl`** スクリプトを使って 1 つの NNMi 管理サーバーをバックアップし、**`nnmrestore.ovpl`** スクリプトを使ってこのバックアップを第 2 の NNMi 管理サーバーに復元し、この両方の NNMi 管理サーバーをリージョナル NNMi 管理サーバーに接続してみる場合があります。このようなことはしないでください。ある NNMi 管理サーバーから 2 番目の NNMi 管理サーバーにバックアップデータを配置すると、これらの両方のサーバーに同じデータベース UUID が存在することになります。NNMi を第 2 の NNMi 管理サーバーに復元した後、元の NNMi 管理サーバーから NNMi をアンインストールする必要があります。

本社 IT グループでは、リージョナル サイト 1 と 2 に配備された重要な機器のみの監視を行い、ほかのデバイスの管理はしない予定です。以下の表に、監視のニーズをまとめます。

表 18　グローバル ネットワーク管理のネットワーク要件

サイト	NNMi 管理サーバー	重要なスイッチ	管理するリージョナル機器
本社	global1	15 台の Model 3500yl HP Procurve Switch	各リージョナル サイトの Model 3500yl HP ProCurve Switch すべて
リージョナル サイト 1	regional1	15 台の Model 3500yl HP Procurve Switch	該当なし
リージョナル サイト 2	regional2	15 台の Model 3500yl HP Procurve Switch	該当なし

要約すると、NNMi 管理サーバー regional1 が本社を監視し、NNMi 管理サーバー regional1 と regional2 が、各リージョナル サイトを監視しています。リージョナル サイト 1 と 2 に配備された Model 3500yl ProCurve Switch のインシデントとデバイス情報を、本社で表示する必要があります。この例では、regional1 と regional2 の両方で、リージョナル サイト 1 に配備された複数の共通スイッチを管理していています。

リージョナル マネージャとグローバル マネージャの接続

グローバル ネットワーク管理接続を設定するときに、以下の情報を考慮します。

- NNMi では、リージョナル マネージャと通信する 1 つ以上のグローバル マネージャを設定できます。たとえば、regional1 と通信するために第 2 のグローバル マネージャ、global2 が必要な場合、NNMi では、regional1 と通信する global1 と global2 の両方を設定できます。詳細については、『HP Network Node Manager i Software システムとデバイス対応マトリックス』を参照してください。
- グローバル ネットワーク管理は、1 つの接続レイヤーで動作します。たとえば、この章の例では、1 つの接続レイヤ、regional1 と通信する global1 と regional2 と通信する global1 について検討します。NNMi は、複数の接続レベルを設定しないでください。 たとえば、global1 は regional1 と通信する設定にはせず、regional1 は regional2 と通信する設定にします。グローバル ネットワーク管理機能は、この 3 つのレイヤー設定用に設計されています。
- 2 つの NNMi 管理サーバーは、相互に両方向に通信する設定にはしないでください。たとえば、global1 は regional1 と通信する設定にはせず、regional1 は global1 と通信する設定にします。

初期準備

ポート可用性 : ファイアウォールの設定

グローバル ネットワーク管理機能が正しく機能するためには、global1 から regional1 と regional2 への TCP アクセス用に、特定のウェルノウン ポートが開いているかどうかを確認する必要があります。NNMi インストール スクリプトでは、デフォルトとしてポート 80 と 443 を設定します。ただし、インストール中にこれらの値は変更できます。

このセクションで説明した例では、global1 が regional1 と regional2 への TCP アクセスを確立します。ファイアウォールは、一般的に接続を開始するサーバーに基づいて設定されます。global1 が regional1 と regional2 への接続を確立すると、トラフィックは両方向に流れます。

現在の値を確認したりポート設定を変更したりするには、以下のファイルを編集します。

- *Windows*: `%NNM_CONF%¥nnm¥props¥nms-local.properties`
- *UNIX*: `$NNM_CONF/nnm/props/nms-local.properties`

以下の表に、アクセス可能にしておく必要があるウェルノウン ポートを示します。

表 19　アクセス可能にしておく必要があるソケット

セキュリティ	パラメータ	TCP ポート
非 SSL	jboss.http.port	80
	jboss.bisocket.port	4457
	jboss.jmsControl.port	4458
SSL	jboss.https.port	443
	jboss.sslbisocket.port	4459
	jboss.ssljmsControl.port	4460

詳細については、NNMi 9.10 およびウェルノウン ポート を参照してください。

自己署名証明書の設定

global1 と 2 つのリージョナル NNMi 管理サーバー (regional1 と regional2) 間で SSL (Secure Sockets Layer) を使用してグローバル ネットワーク管理機能を使用する場合は、追加の作業が必要です。NNMi のインストール中、NNMi インストール スクリプトでは、他のエンティティに対して自身を識別できるよう、NNMi 管理サーバーに自己署名証明書を作成します。使用する NNMi 管理サーバーには、正しい証明書を持つグローバル ネットワーク管理機能を設定する必要があります。129 ページの「自己署名証明書を使用するようにグローバル ネットワーク管理機能を設定する」に示した手順を実行してください。

グローバル ネットワーク管理でアプリケーション フェイルオーバーの設定を行う

NNMi のインストール中、NNMi インストール スクリプトでは、他のエンティティに対して自身を識別できるよう、NNMi 管理サーバーに自己署名証明書を作成します。グローバル ネットワーク管理機能とともにアプリケーション フェイルオーバーを使用する場合は、追加の設定を行う必要があります。131 ページの「自己署名証明書を使用するようにアプリケーション フェイルオーバーが有効なグローバル ネットワーク管理を設定する」に示した手順を実行してください。

NNMi 管理サーバー規模の考慮事項

この例では、グローバル ネットワーク管理設定で既存の NNMi 管理サーバーを使用することを想定しています。グローバル ネットワーク管理機能は、以前の NNM 製品で使用されていた分散ソリューションとは異なります。グローバル ネットワーク管理機能を使用すると、リージョナル システムによるポーリング ノードの管理が回避されるため、ネットワーク帯域幅やコンピュータ リソースを考慮する必要がなくなります。

NNMi のインストールが必要となるサーバーのサイズに関する具体的な情報については、NNMi インストール ガイド、*NNMi リリース ノート*、*NNMi システムおよびデバイスのサポート マトリックス*を参照してください。

システム クロックの同期化

`global1`、`regional1`、および `regional1` サーバーをグローバル ネットワーク管理設定に接続する前に、これらの NNMi 管理サーバー クロックを同期化することが重要です。グローバル ネットワーク管理 (グローバル マネージャとリージョナル マネージャ) やシングル サインオン (SSO) に属するネットワーク環境内のすべての NNMi 管理サーバーは、それぞれの内部タイム クロックを世界標準時で同期化する必要があります。たとえば、UNIX (HP-UX / Linux / Solaris) ツールの Network Time Protocol Daemon (NTPD) や使用可能な Windows オペレーティング システム ツールなどの時刻の同期プログラムを使用します。詳細については、NNMi ヘルプの「*クロック同期の問題*」または「*グローバル ネットワーク管理のトラブルシューティング*」と 248 ページの「クロック同期」を参照してください。

➤ サーバー クロック同期の問題など、リージョナル マネージャとの接続に問題がある場合、NNMi では NNMi コンソールの下部に警告メッセージが表示されます。

グローバル ネットワーク管理で自己署名証明書を使用する場合のアプリケーション フェイルオーバー機能の使用法

アプリケーション フェイルオーバー設定で、自己署名証明書を使用したグローバル ネットワーク管理機能を使用する場合は、追加の手順を実行する必要があります。131 ページの「自己署名証明書を使用するようにアプリケーション フェイルオーバーが有効なグローバル ネットワーク管理を設定する」を参照してください。

グローバル ネットワーク管理における自己署名証明書の使用法

グローバル ネットワーク管理機能で自己署名証明書を使用する場合は、追加の手順を実行する必要があります。129 ページの「自己署名証明書を使用するようにグローバル ネットワーク管理機能を設定する」を参照してください。

グローバル ネットワーク管理における認証機関の使用法

グローバル ネットワーク管理機能で認証機関を使用する場合は、追加の手順を実行する必要があります。130 ページの「認証機関を使用するようにグローバル ネットワーク管理機能を設定する」を参照してください。

監視する重要な機器の一覧作成

global1 から監視する、regional1 と regional2 の管理機器一覧を作成します。この情報を転送フィルタ (これについては後で説明します) で使用します。regional1 と regional2 から global1 に転送する情報を制限した場合に得られる結果については、慎重に考慮する必要があります。計画を立てるときに、以下の点を考慮してください。

- global1 で完全な分析を行って正確なインシデントを生成するには、regional1 と regional2 から得られる完全なトポロジが必要になるため、除外するデバイスが多くなりすぎないように注意します。
- 重要ではないデバイスを除外すると、global1 のライセンス コストのを節約できます。
- 重要ではないデバイスを除外すると、ソリューションの全体的な拡張性が改善され、NNMi で必要となるネットワーク トラフィックを削減できます。

グローバル マネージャとリージョナル マネージャの管理ドメインの検討

NNMi 管理サーバー global1、regional1、および regional2 は、独自のノード セットを管理しています。この例では、後で regional1 と regional2 から global1 に、それぞれが管理する機器に関する情報を転送するよう設定します。

以下の手順に従って、global1、regional1、および regional2 が現在監視している機器を確認します。機器を確認しておくと、regional1 と regional2 から global1 に転送する重要な機器を選択するときに役立ちます。

この例では、以下の手順を実行してこの情報を確認します。

1. ブラウザで global1 の NNMi コンソールを指します。
2. サインインします。
3. **[インベントリ]** ワークスペースをクリックします。
4. このワークスペースで global1 が現在監視していて検出されたインベントリを確認できます。
5. ブラウザで regional1 の NNMi コンソールを指します。
6. サインインします。
7. **[インベントリ]** ワークスペースをクリックします。
8. regional1 が監視しているノードを確認し、global1 で監視するデバイスの一覧を作成します。
9. ブラウザで regional2 の NNMi コンソールを指します。
10. サインインします。
11. **[インベントリ]** ワークスペースをクリックします。
12. regional2 が監視しているノードを確認し、global1 で監視するデバイスの一覧を作成します。

NNMi ヘルプ トピックの確認

グローバル ネットワーク管理に関するすべてのヘルプ トピックを確認するには、以下の手順を実行します。

1 NNMi ヘルプで、**[検索]** をクリックします。

2 ［Search］フィールドに「**Global Network Management**」と入力します。

3 **[検索]** をクリックします。

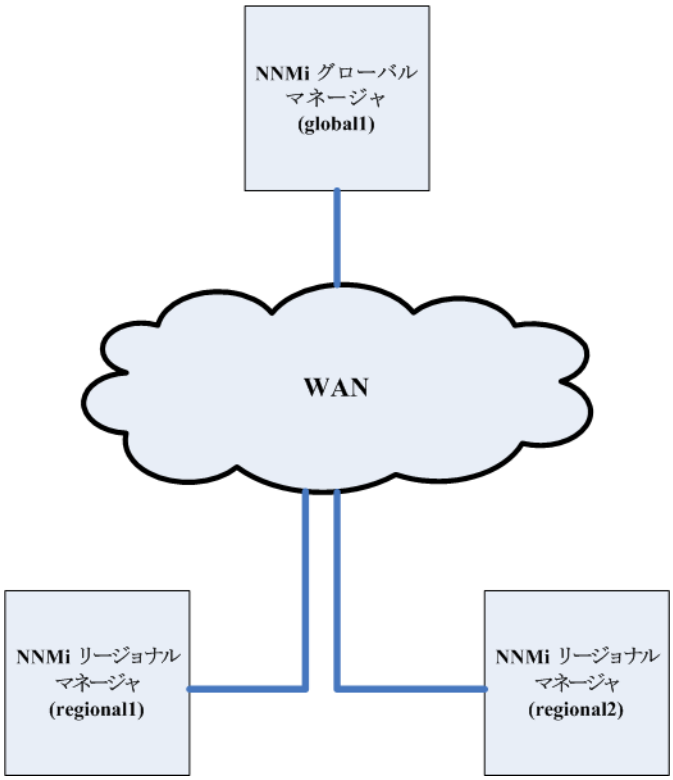
この検索により、グローバル ネットワーク管理に関連する 50 以上のトピックが見つかります。

SSO およびアクション メニュー

グローバル マネージャの NNMi コンソールから、リージョナル マネージャが管理するノードを選択した後に、**[アクション]** メニューを使用して、選択したノードに対するアクションを開始するとします。NNMi 管理サーバーの間で `initString` と `domain` のパラメータを同一にしないと、グローバル マネージャのセッション情報は新しいセッションに渡されず、アクションは開始されません。この問題を回避するには、223 ページの「グローバル ネットワーク管理用にシングル サインオンを設定する」の設定手順に従ってください。

グローバル ネットワーク管理用にシングル サインオンを設定する

NNMi シングル サインオン (SSO) を設定すると、NNMi グローバル マネージャから簡単に NNMi リージョナル マネージャにアクセスできるようになります。グローバル マネージャからリージョナル マネージャに接続する前に、この手順を完了しておく必要があります。詳細については、139 ページの「NNMi とシングル サインオンの使用」を参照してください。



SSO 機能は、NNMi 管理サーバー内のユーザー名を交換しますが、パスワードやロールは交換しません。たとえば、NNMi は 1 つの NNMi 管理サーバー (global1) の特定のユーザー名を、別の NNMi 管理サーバー (regional1 または regional2) の異なるロールに関連付けます。3 つの NNMi 管理サーバーで、同じユーザー名に異なるパスワードが関連付けられることもあります。

グローバル マネージャとリージョナル マネージャが同じ管理ドメインにあり、224 ページの手順 3 に示したように *Initialization String* 値をグローバル NNMi 管理サーバーからリージョナル NNMi 管理サーバーにコピーしないと、NNMi コンソールのアクセスに問題が起こる場合があります。これを回避するには、以下の手順に従って SSO を正しく設定するか、148 ページの「SSO の無効化」で説明したように SSO を無効にします。

SSO をグローバル ネットワーク管理機能と連携させるには、以下の手順を実行します。

1 global1 で以下のファイルを編集します。

- *Windows*: %NNM_PROPS%¥nms-ui.properties
- *UNIX*: $NNM_PROPS/nms-ui.properties

2 global1 の SSO NNMi 初期化文字列を探します。nms-ui.properties 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.initString = *Initialization String*

3 global1 の nms-ui.properties ファイルにある *Initialization String* の値を、regional1 と regional2 の nms-ui.properties ファイルにコピーします。*Initialization String* は、すべてのサーバーで同じ値を使用する必要があります。変更を保存します。

グローバル NNMi 管理サーバーから リージョナル NNMi 管理サーバーへの *Initialization String* 値のコピーは NNMi でサポートされます。この操作により、グローバル マネージャから 2 つのリージョナル マネージャに *Initialization String* 値がコピーされます。グローバル ネットワーク管理機能で SSO を使用する場合は、*Initialization String* 値のコピーは、常にグローバル マネージャからリージョナル マネージャに対して行ってください。

グローバル マネージャとリージョナル マネージャが同じ管理ドメインにあり、*Initialization String* 値をグローバル NNMi 管理サーバーからリージョナル NNMi 管理サーバーにコピーしない場合は、SSO を無効にして、NNMi コンソールのアクセスに問題が起こらないようにします。詳細については、148 ページの「SSO の無効化」を参照してください。

4 global1、regional1、および regional2 が異なるドメインにある場合は、protectedDomains の内容を変更します。変更するには、nms-ui.properties ファイルの中から以下のようなセクションを探します。

com.hp.nms.ui.sso.protectedDomains=*group1.mycompany.com*

global1 は global1.company1.com に、regional1 は regional1.company2.com に、そして、regional2 は regional2.company3.com にあるとします。global1、regional1、regional2 にある nms-ui.properties ファイルの protectedDomains セクションを以下のように変更します。

com.hp.nms.ui.sso.protectedDomains=regional1.company1.com,
regional2.company2.com,regional3.company3.com

変更を保存します。

5 global1、regional1、regional2 で、以下の一連のコマンドを実行します。

a **ovstop ovjboss**

b **ovstart ovjboss**

アプリケーション フェイルオーバー設定でシングル サインオンを有効にするときに、手動で行う設定手順はありません。たとえば、アプリケーション フェイルオーバー設定でシングル サインオンを設定する場合、NNMi によりアクティブ NNMi 管理サーバーからスタンバイ NNMi 管理サーバーに上記の変更を複製されます。

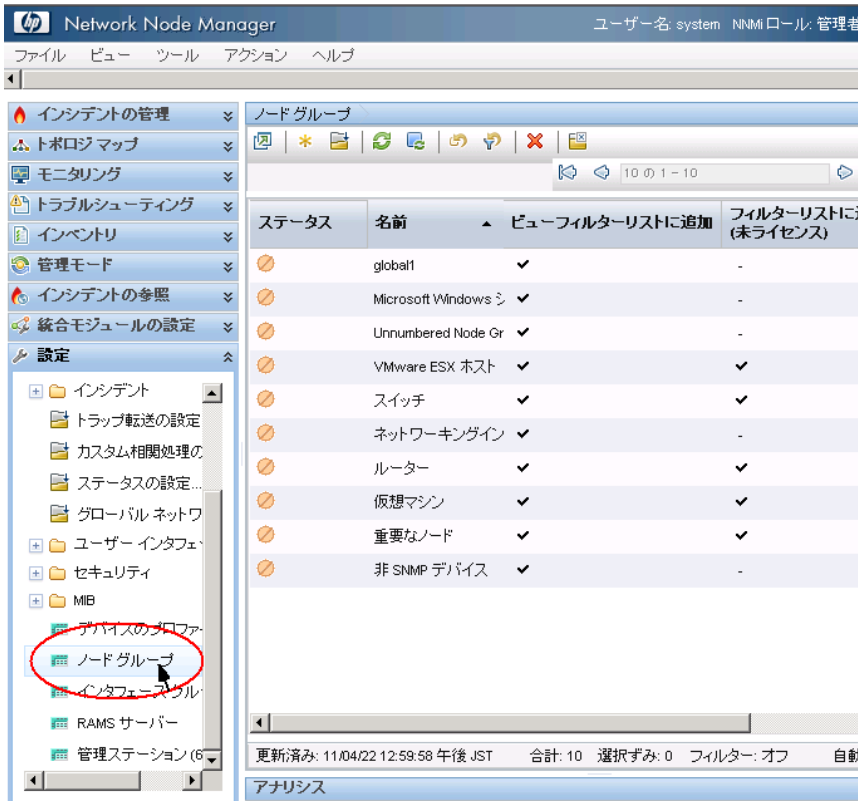
リージョナル マネージャでの転送フィルタの設定

この例では、global1 は regional1 と regional2 の両方と通信します。グローバル マネージャ global1 がリージョナル マネージャ regional1 と regional2 から受け取るノード オブジェクト データを制御するには、regional1 と regional2 の両方で転送フィルタを設定する必要があります。

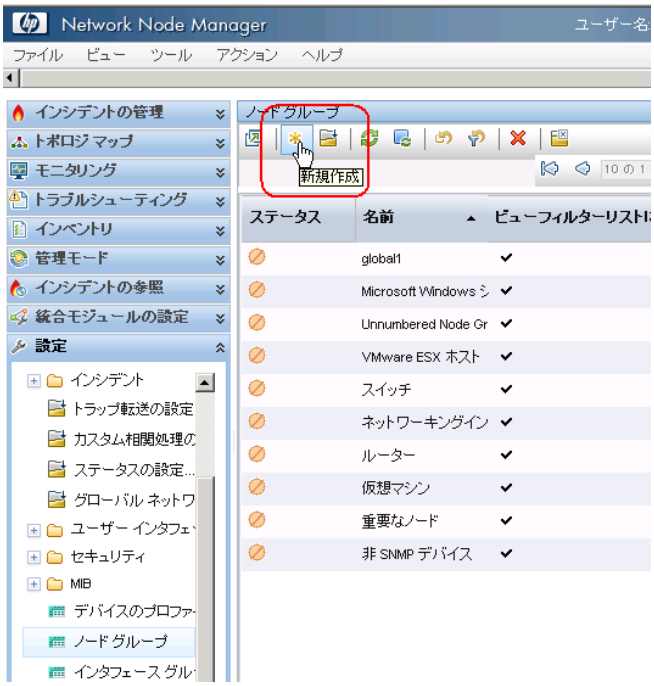
転送されるノードを制限する転送フィルタの設定

ノード グループを設定し、regional1 から Model 3500yl ProCurve Switch のノード情報のみを global1 に転送するようにします。新しいノード グループを作成し、グループに制限を設定するには、以下の手順を実行します。

1 NNMi コンソールの regional1 の **[設定]** ワークスペースから **[ノード グループ]** をクリックします。



2 **[新規作成]** をクリックします。

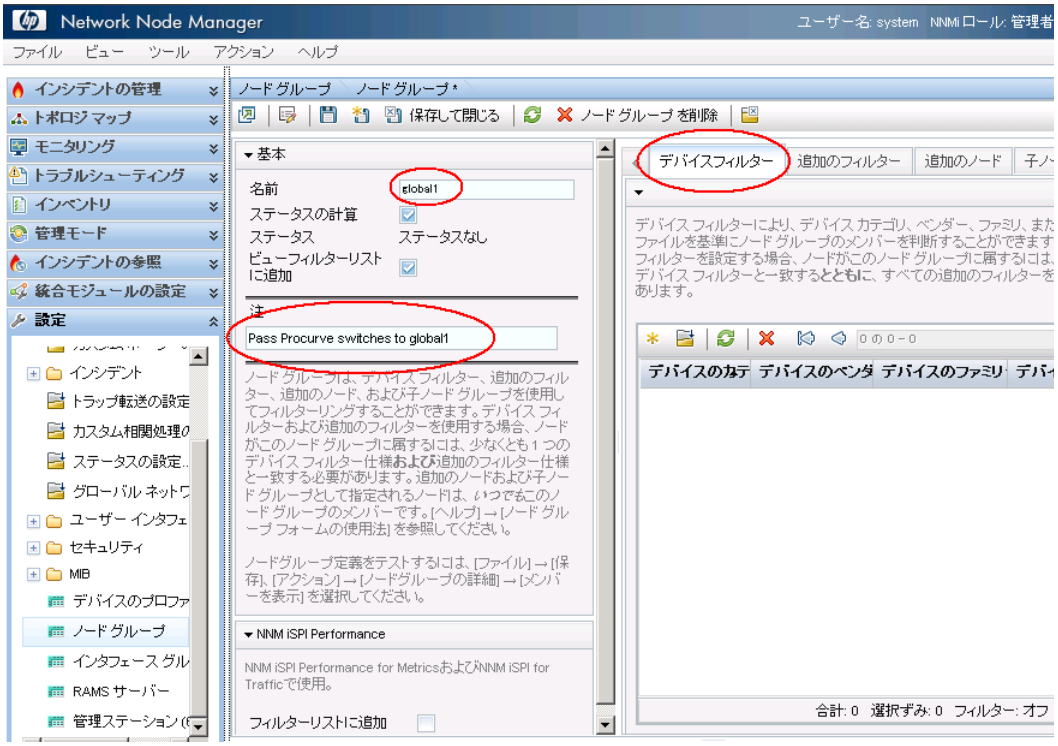


この例では、ノード フィルタの新規作成し、そのフィルタを使用して regional1 と regional2 の転送フィルタを作成する方法を説明していますが、既存のフィルタを使用して、リージョナル NNMi 管理サーバーからグローバル NNMi 管理サーバーへの転送フィルタを設定することもできます。

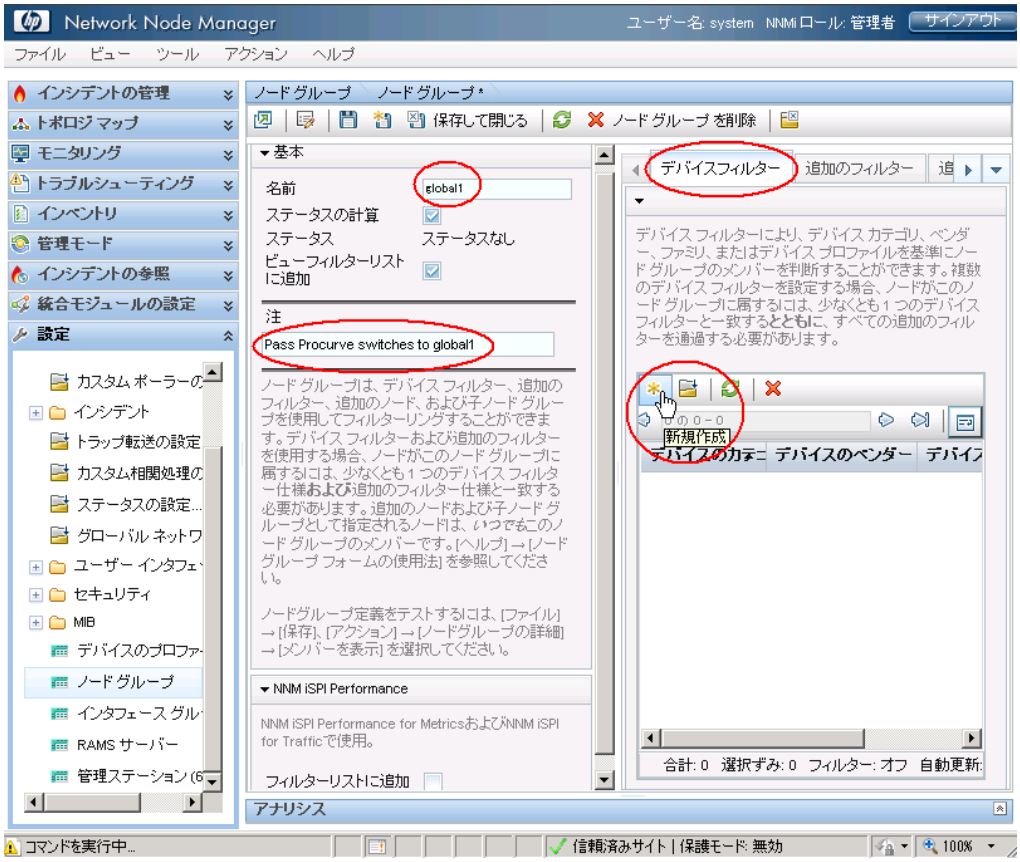
独自のデバイスもフィルタも含まれていないコンテナ ノード グループを作成して、このノード グループを使用して子ノード グループを指定できます。この方法を使用すると、1 つのコンテナ ノード グループを使用して、ノード オブジェクト データをグローバル NNMi 管理サーバーに転送できます。

3 **[デバイスフィルタ]** タブをクリックします。フィルタ名に `global1` と入力し、[注] フィールドに作成するフィルタの説明を入力します。

.

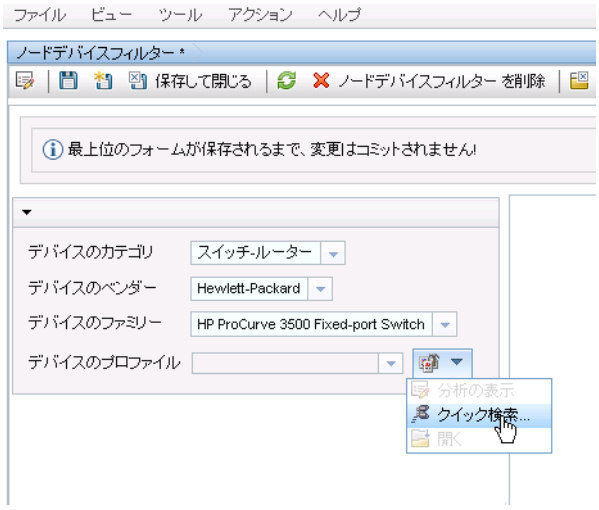


4 **[新規作成]** アイコンをクリックして、[ノード デバイス フィルタ] フォームを開きます。

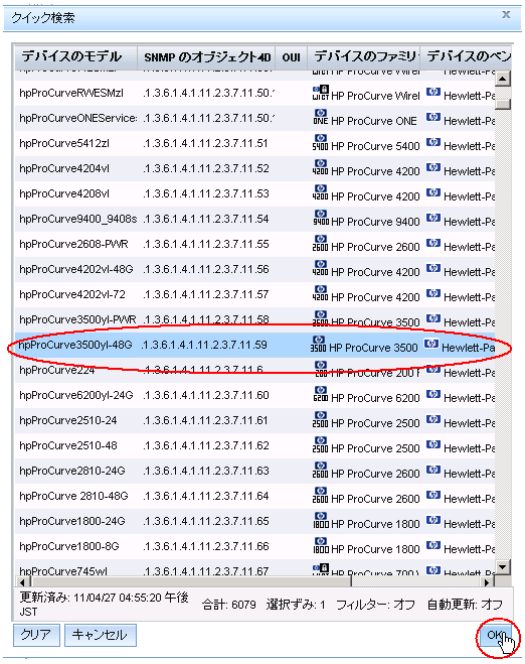


5 プルダウン メニューを使用して、[デバイスのカテゴリ] では [スイッチルーター]、[デバイスのベンダー] では [Hewlett-Packard]、および [デバイスのファミリー] では [HP Procurve 3500 Fixed-port Switch] を選択します。

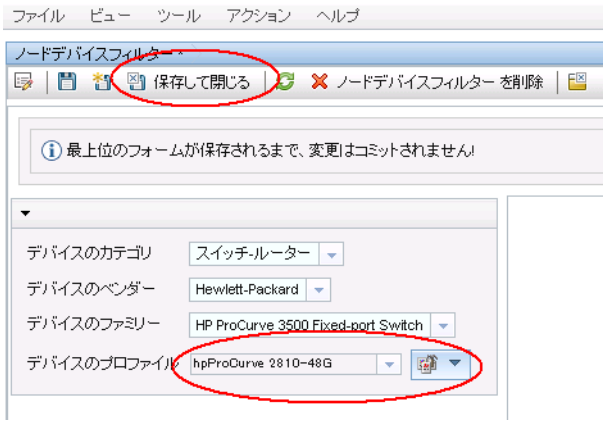
6 プルダウン メニューから、**[クイック検索]** をクリックして、[デバイスのプロファイル] フォームを開きます。



7 3500yl HP ProCurve Switch のプロファイルを検索して選択し、**[OK]** をクリックします。

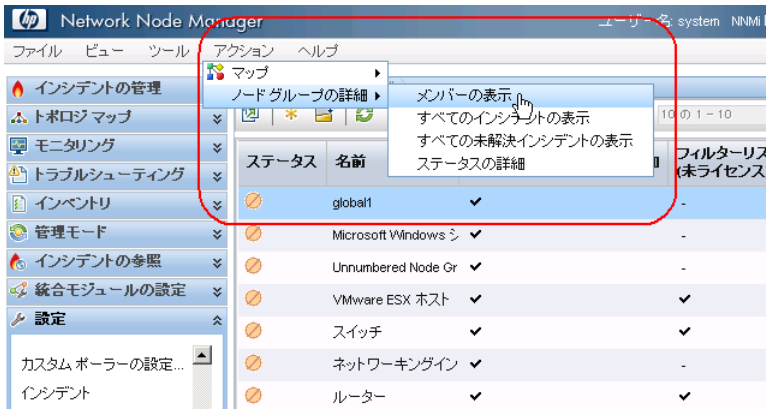


8 **[保存して閉じる]** を 2 回クリックします。

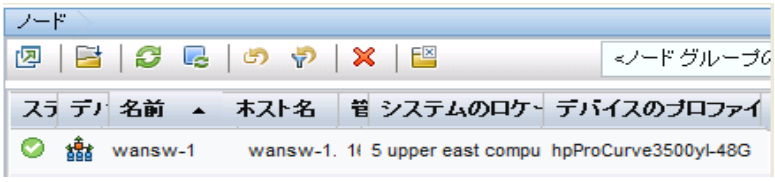


9 このフィルタをテストするため、**[global1]** を選択します。

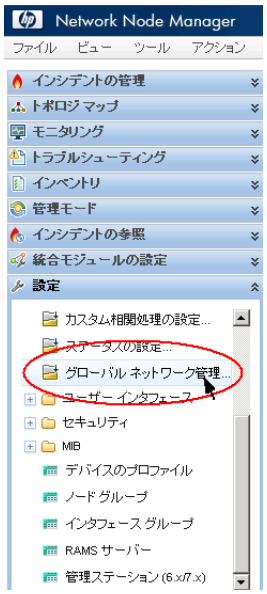
10 プルダウン メニューから、**[メンバーの表示]** をクリックします。



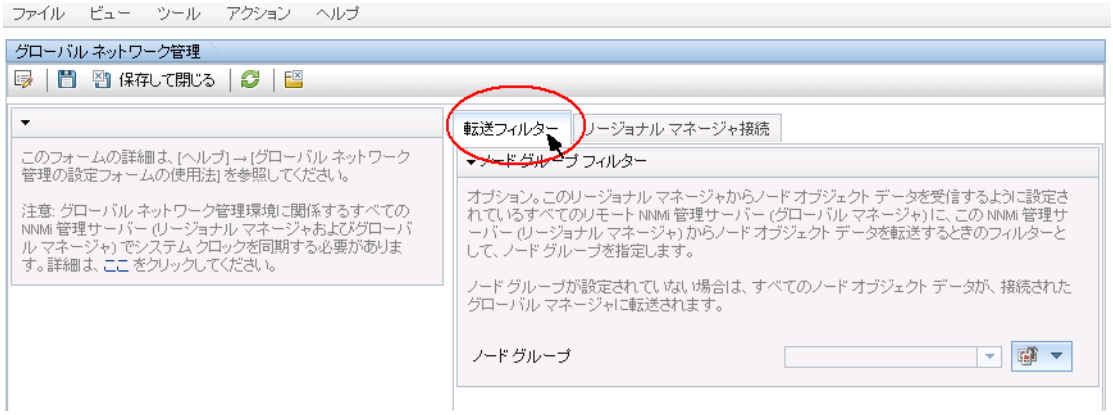
11 NNMi ではすでに HP 3500yl スイッチが 1 つ検出されています。これは、作成したフィルタが、設定した特定のスイッチ モデルを検索していることを示しています。次のステップでは、今作成したこのノード フィルタを使用して転送フィルタを設定します。



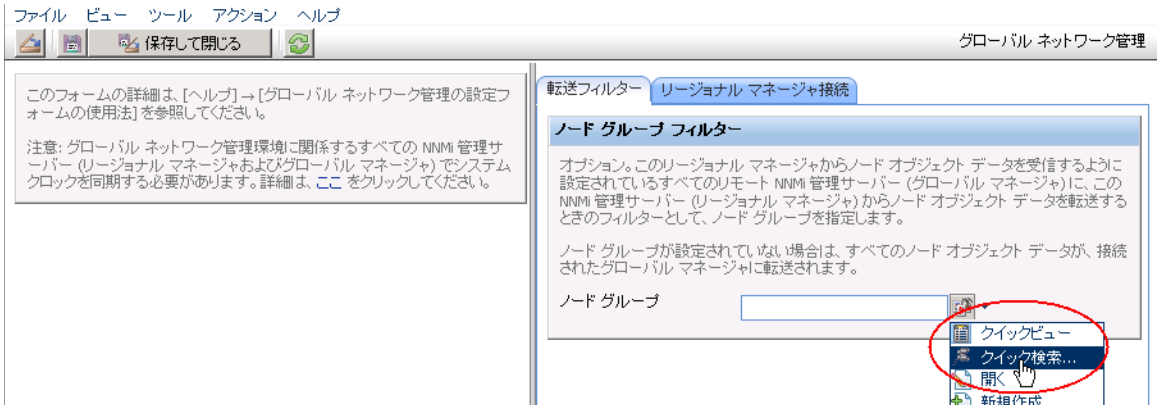
12 NNMi コンソールの `regional1` の **[設定]** ワークスペースから **[グローバル ネットワーク管理]** をクリックします。



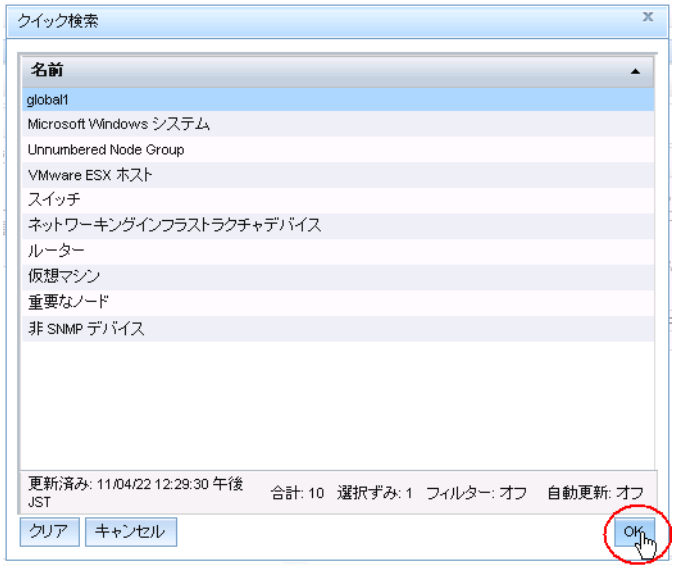
13 **[転送フィルター]** タブをクリックします。



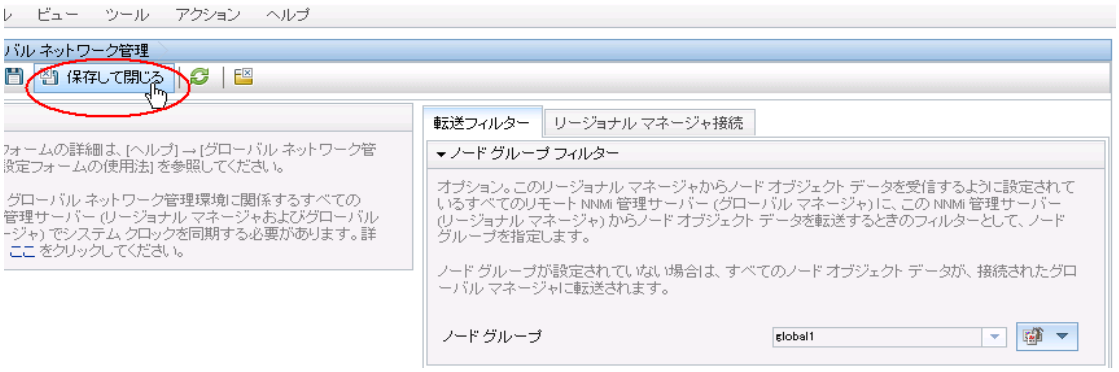
14 **[クイック検索]** をクリックします。



15 **global1** フィルタを選択し、**[OK]** をクリックします。



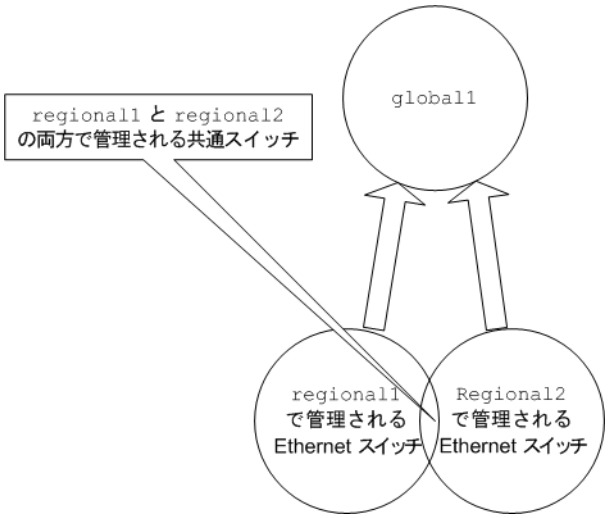
16 **[保存して閉じる]** をクリックします。



これで、regional1 の転送フィルタの設定作業は完了です。regional2 についても手順 1 から手順 16 を実行したら、次のセクションに進み、global1 を regional1 と regional2 に接続します。

グローバル マネージャとリージョナル マネージャの接続

すでに述べたように、regional1 と regional2 の両方で、共通のスイッチを複数管理しているとします。この共通のスイッチ情報を regional1 から global1 に転送します。



そのためには、global1 を先に regional1 に接続してから regional2 に接続する必要があります。この接続順により、global1 は regional1 をこれらの共通スイッチの監視を行う NNMi 管理サーバーであるとみなします。Global1 は、また、regional2 から受け取るこれらの共通スイッチに関する情報を無視します。

この機能の動作を理解するには、まずは小さな規模で使用してから、それぞれのネットワーク管理ニーズに合わせて拡張することを推奨します。

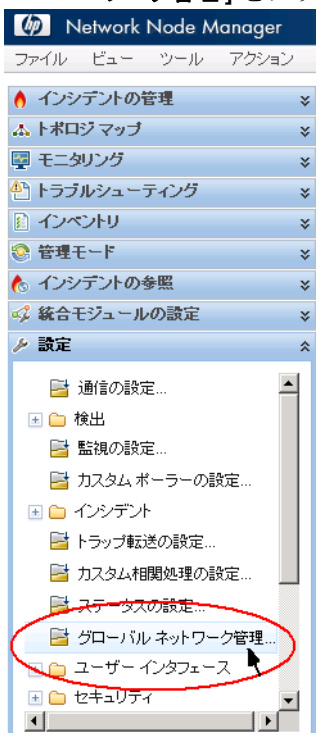
global1 を先に regional1 に接続し、次に regional2 に接続するには、以下の手順を実行します。

1 すでに述べたように、NNMi 管理サーバーのクロックを global1、regional1、および regional2 と同期化してから、グローバル ネットワーク管理設定内のこれらのサーバーを接続します。詳細については、NNMi ヘルプの「*クロック同期の問題*」を参照してください。

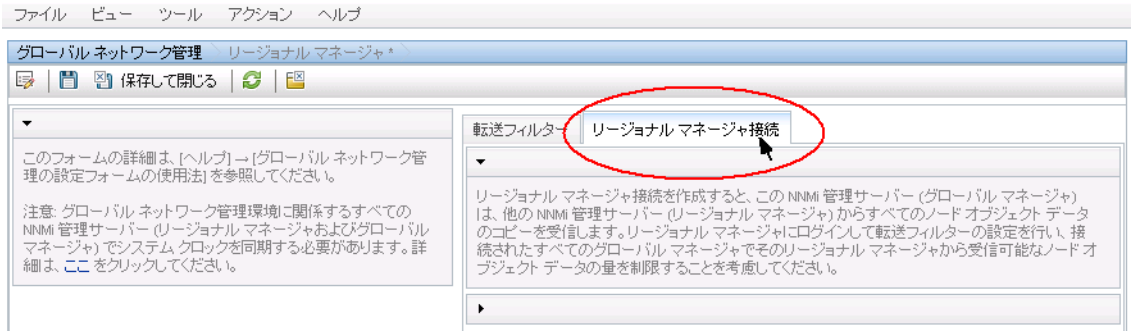
サーバー クロック同期の問題など、リージョナル マネージャとの接続に問題がある場合は、NNMi では警告メッセージが表示されます。

2 global1 から regional1 への接続を設定します。

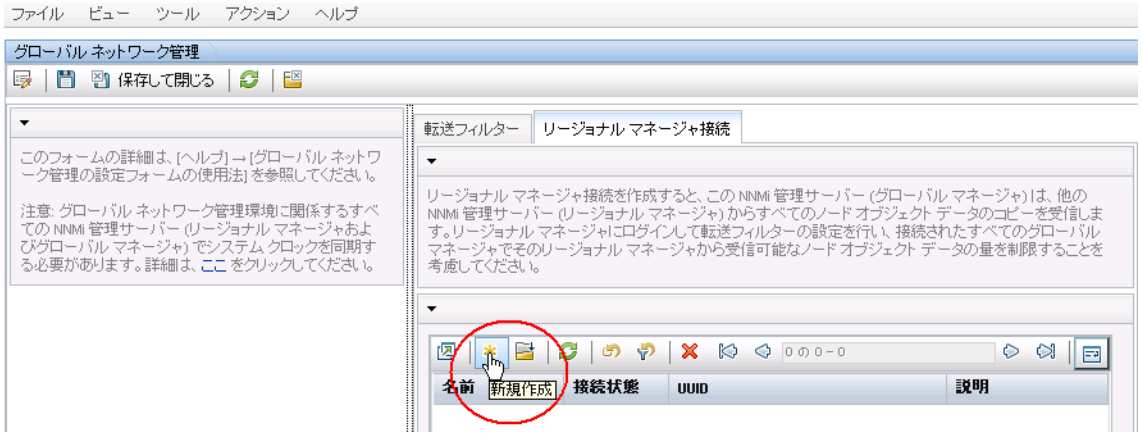
a global1 の NNMi コンソールで、**[設定]** ワークスペースの **[グローバル ネットワーク管理]** をクリックします。



b **[リージョナル マネージャ接続]** をクリックします。



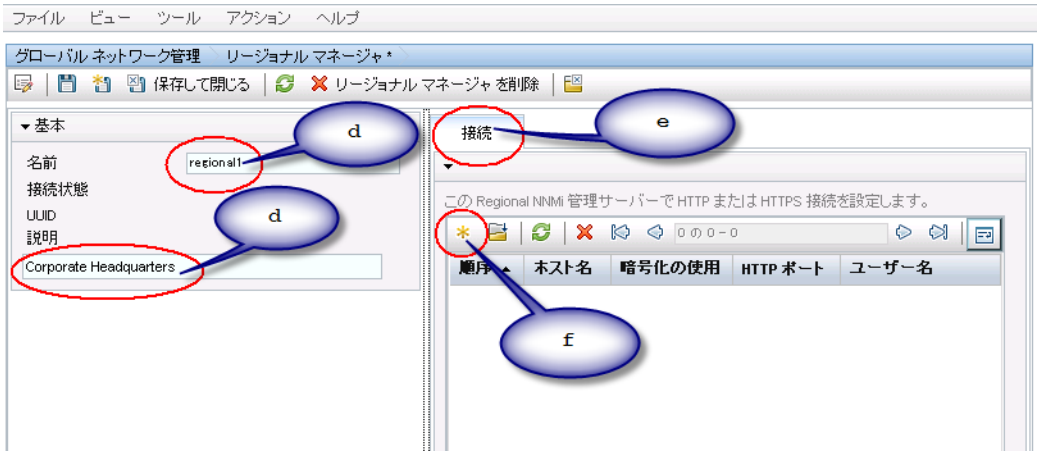
c アイコンをクリックして、リージョナル マネージャを新規作成します。



d regional1 の名前と説明情報を追加します。

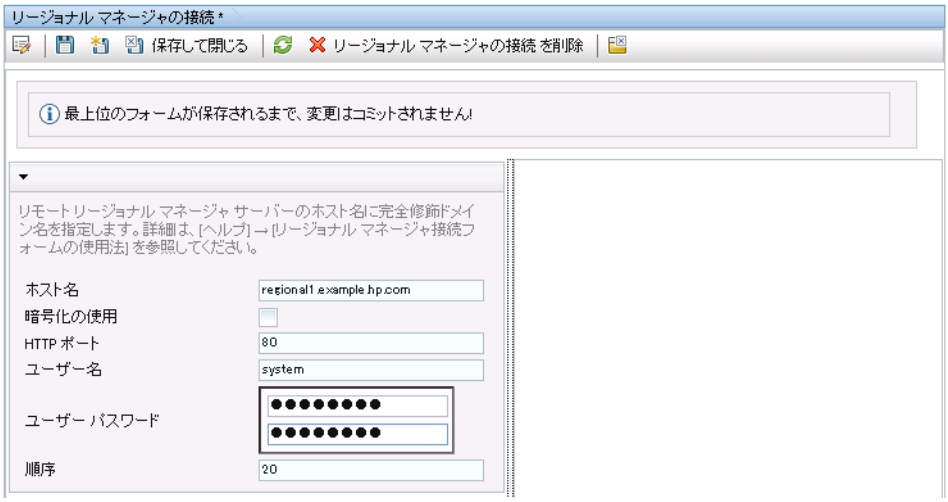
e **[接続]** タブをクリックします。

f アイコンをクリックします。



g　regional1 の接続情報を追加します。

このフォームで作成するエントリに関する個別の情報については、NNMi ヘルプの **「[リージョナル マネージャ接続] フォームの使用法」** を参照してください。



h　**[保存して閉じる]** を 2 回クリックして作業を保存します。

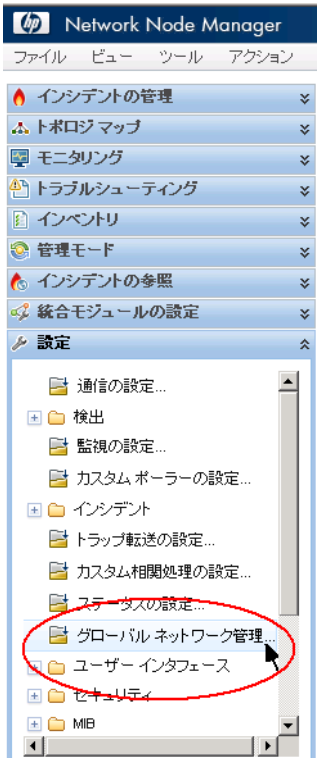
3　global1 から regional2 への接続を確立するため、233 ページの手順 a から 235 ページの手順 g までを実行します。

global1 から regional1 と regional2 への 接続ステータスの判定

global1 から regional1 および regional2 への接続の状態を確認するには、以下の手順を実行します。

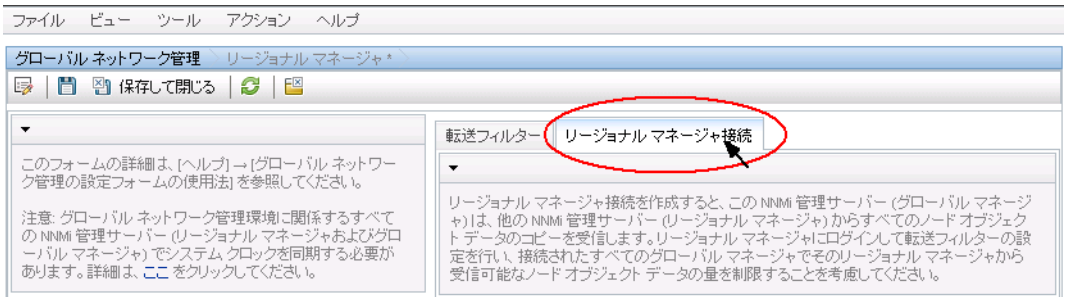
1 global1 の NNMi コンソールで、**[設定]** ワークスペースの **[グローバル ネットワーク管理]** をクリックします。

.



2 **[リージョナル マネージャ接続]** タブをクリックします。

.



3 regional1 と regional2 の接続ステータスを確認します。[接続済み] と表示され、正しく機能していることを意味します。

詳細については、NNMi ヘルプの「*リージョナル マネージャの接続ステータスの判定*」を参照してください。

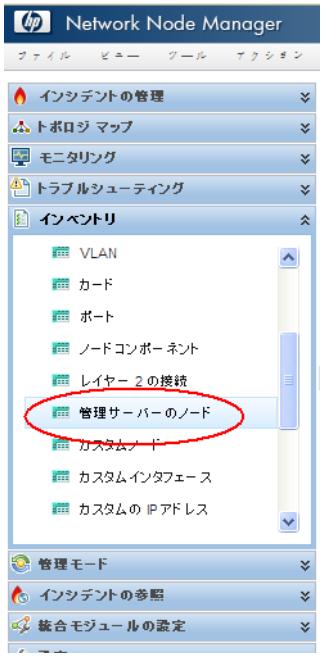
NNMi が検出を完了するまで、次のセクションには進まないでください。詳細については、『NNMi インストール ガイド』の「*検出の進行状況の確認*」を参照してください。

global1 インベントリの確認

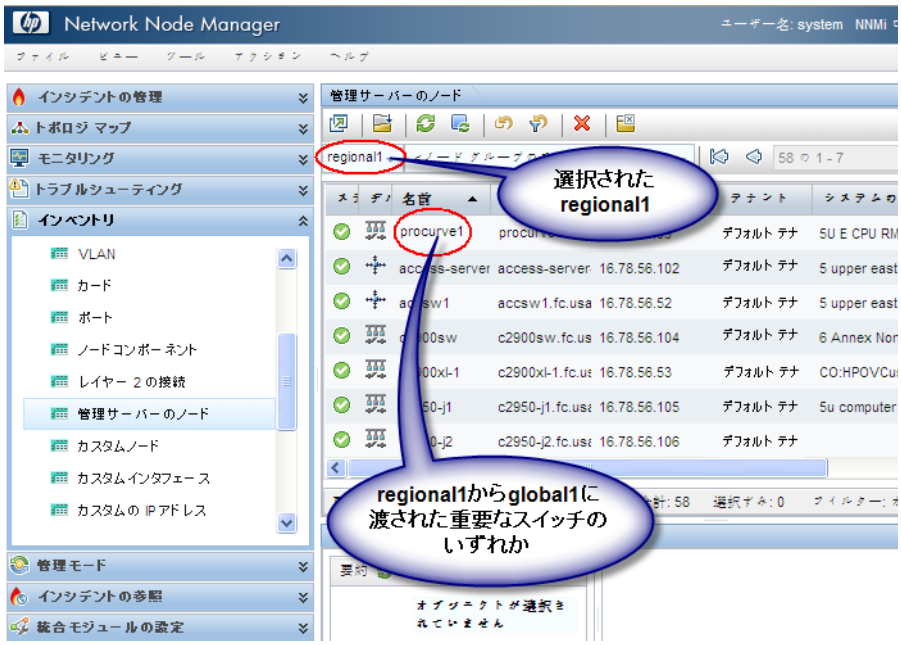
NNMi が検出を完了するまで、このセクションは実行しないでください。詳細については、『NNMi インストール ガイド』の「*検出の進行状況の確認*」を参照してください。

global1 に転送されるノード情報 regional1 を表示するには、以下の手順を実行します。

1 **[インベントリ]** ワークスペースに配置されている **[管理サーバーごとのノード]** フォームに、global1 の NNMi コンソールから移動します。



2 スイッチ procurve1.x.y.z に関する情報が regional1 から global1 に転送されたと仮定します。**regional1** を選択すると、インベントリは以下のように表示されます。

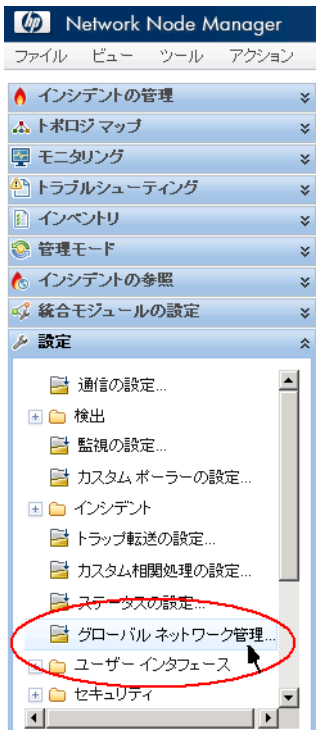


手順 1 から手順 2 を実行して、接続されている他のリージョナル マネージャから global1 に転送されたデバイス インベントリも表示します。

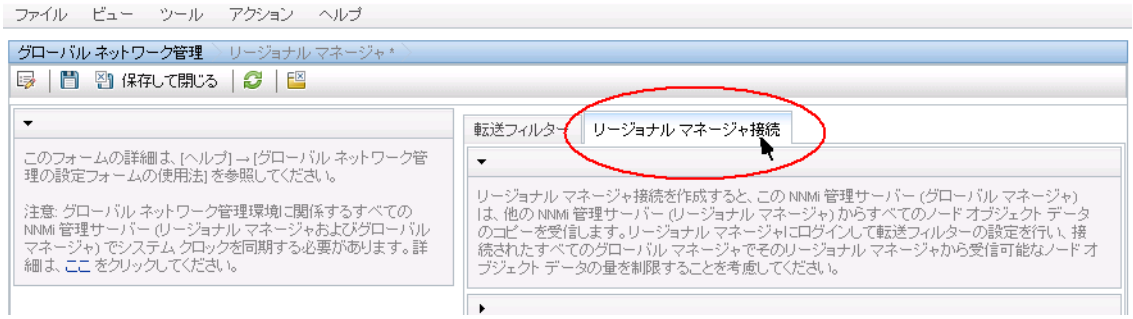
global1 と regional1 との通信の切断

global1 を完全にシャットダウンするか、何日間かシャットダウンする計画であることを想定します。この例では、global1 では対 regional1 のサブスクリプションがまだアクティブであると仮定します。シャットダウンを完了するには、追加の手順を実行する必要があります。

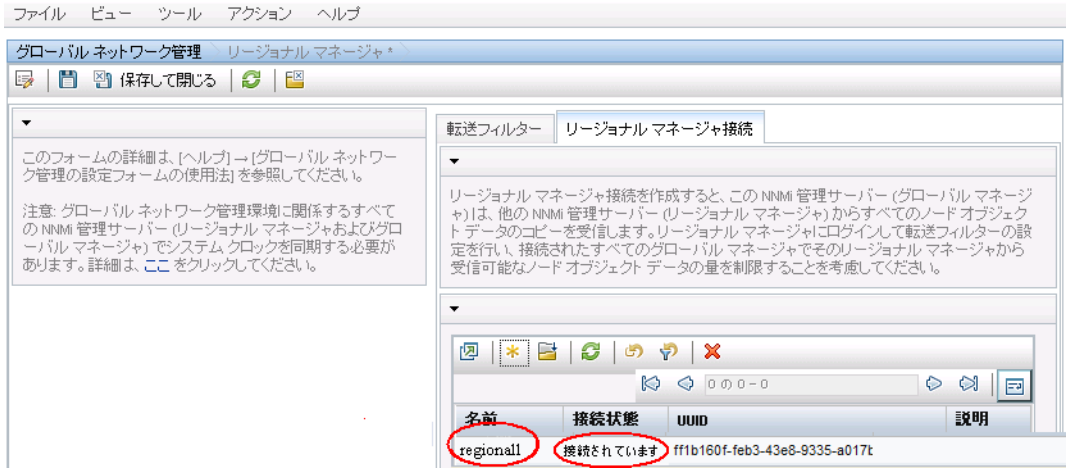
1 global1 の NNMi コンソールで、**[設定]** ワークスペースの **[グローバル ネットワーク管理]** をクリックします。



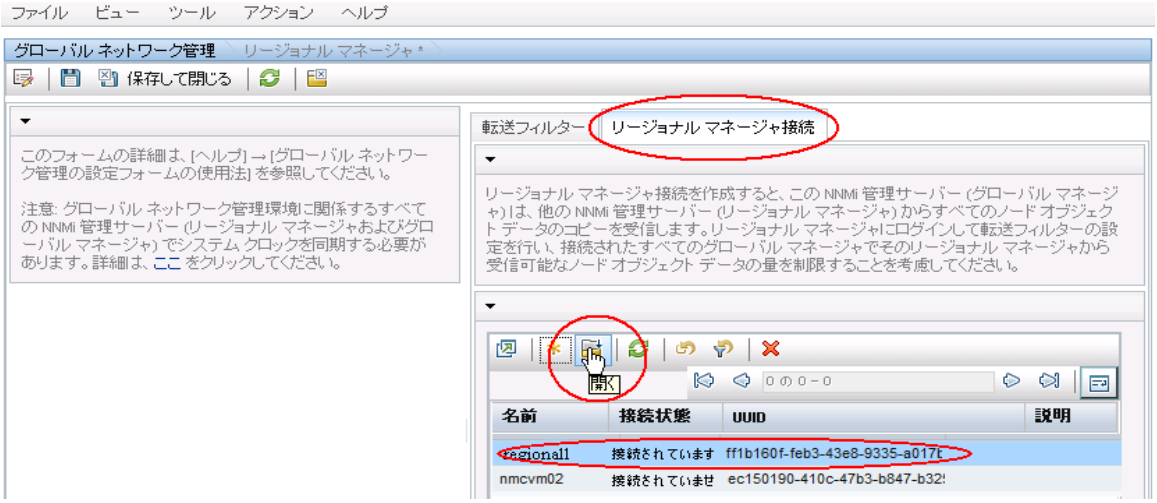
2 [リージョナル マネージャ接続] をクリックします。



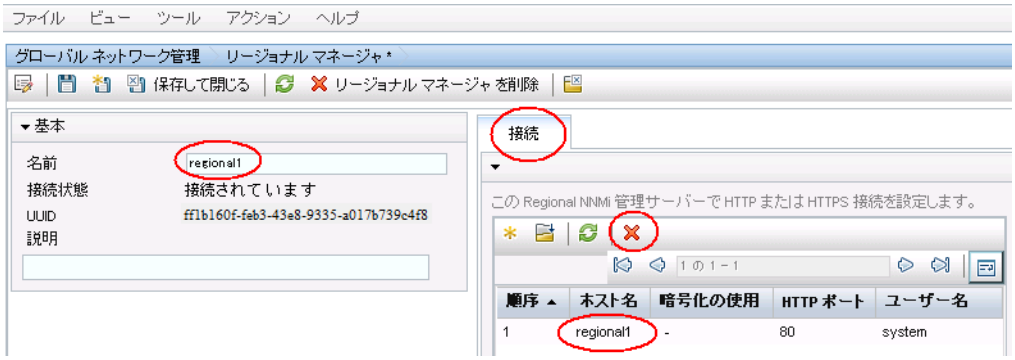
3 ステータスが [接続済み] であることを確認します。ステータスが [接続済み] ではない場合、処理を続行する前に、NNMi ヘルプの「*グローバル ネットワーク管理のトラブルシューティング*」を参照して問題を診断します。



4 `regional1` を選択して [開く] アイコンをクリックします。



5 **[接続]** をクリックして **[regional1.x.y.z]** を選択してから **[削除]** をクリックします。



6 **[保存して閉じる]** をクリックします。

7 [リージョナル マネージャ接続] タブでは、`regional1` の [名前] 属性に注意してください (大文字小文字は区別されます)。後のステップで、`RemoteNNMiServerName` 変数にこのテキスト文字列が必要になります。

8 **[保存して閉じる]** をもう一度クリックします。

9 global1 で、コマンド ラインで以下のコマンドを入力します。

nnmnodedelete.ovpl -rm regional1 -u *NNMiadminUserName* **-p** *NNMiadminPassword*

10 これらのコマンドにより、regional1 から転送されたノード レコードを global1 から削除します。コマンドでは、regional1 から global1 に転送されたノードに関連するインシデントも閉じます。詳細については、NNMi ヘルプの「*リージョナル マネージャとの通信の切断*」を参照してください。

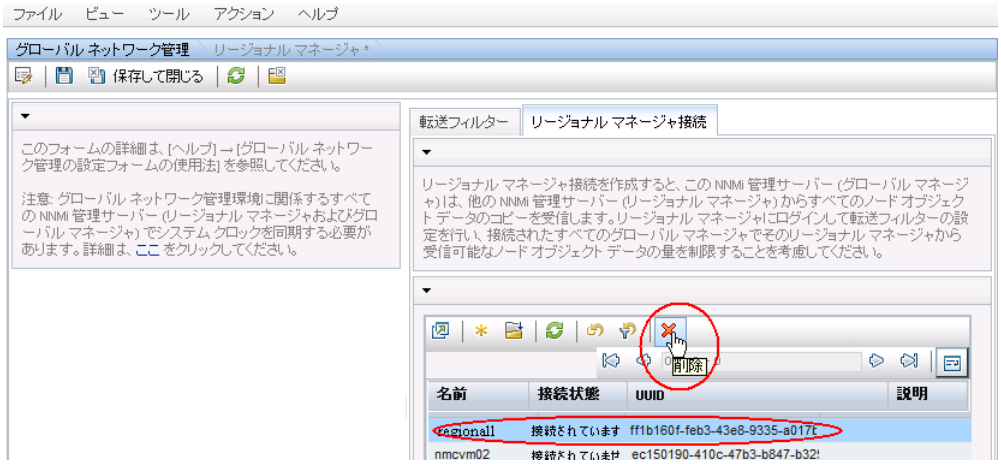
11 regional1 の設定レコードを削除するには、以下を実行します。

a **[設定]** ワークスペースをクリックします。

b **[グローバル ネットワーク管理]** フォームを選択します。

c **[リージョナル マネージャ接続]** タブを選択します。

d regional1 を選択して [削除] アイコンをクリックします。



e **[保存して閉じる]** をクリックして削除を保存します。

12 regional2 など、global1 に接続している他のリージョナル NNMi 管理サーバーについても手順 1 から手順 11 を実行します。

追加情報

検出とデータの同期化

ネットワーク管理者がネットワーク上のデバイスの追加、削除、または変更を行うと、regional1 や regional2 などのリージョナル サーバーはそうした変更を検出して、この章の例での global1 などのグローバル サーバーを更新します。regional1 と regional2 では、global1 が管理するノードの管理モードに対して管理者が行う変更についても global1 に通知します。

整合性を保つため、regional1 と regional2 はデバイスの状態の変化を検出すると、global1 を継続的に更新するので、グローバル サーバーとリージョナル サーバーの両方でノードの状態が同じに保たれます。

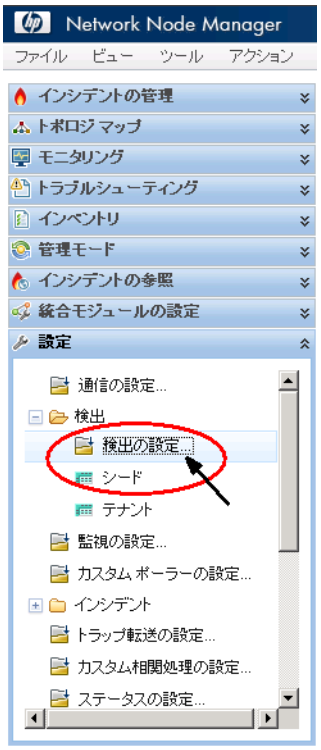
regional1 または regional2 が管理するノードに関する情報を global1 が要求するたびに、regional1 または regional2 は要求された情報を global1 に返します。global1 からノードに直接要求することはありません。global1 が検出を実行するとき、デバイスに対する SNMP クエリは重複しません。

global1 は、regional1 または regional2 が検出を完了するたびに、regional1 と regional2 を同期します。NNMi は FDB (転送データベース) データを使用して、レイヤ 2 接続を計算します。FDB データは非常にダイナミックなもので、特に、1 つのグローバル サーバーに複数のリージョナル サーバーが接続しているような場合には、検出するごとに大きく異なります。

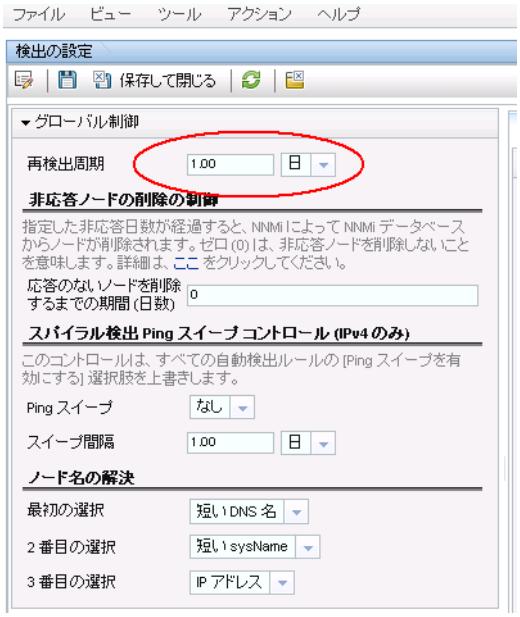
ユーザーが修正した属性やアプリケーションが修正した属性に対する変更は、グローバル サーバーでは同期中に更新されません。

[再検出間隔] は、各リージョナル サーバーで調整でき、global1 とリージョナル マネージャとの間の検出の精度を変更できます。[再検出間隔] が短くなるほど、検出の精度が上がり、NNMi が行うネットワーク トラフィックも増えます。[再検出間隔] が長くなるほど、検出の精度は下がり、NNMi が行うネットワーク トラフィックも減ります。これは、ネットワークが大きくなるほど、ユーザーが行う再検出の頻度が少なくなることを意味します。[再検出間隔] を設定するには、以下の手順を実行します。

regional1 または regional2 の NNMi コンソールから、**[設定]** ワークスペースの **[検出の設定]** をクリックします。



13 リージョナル サーバーで検出を開始する頻度に従い、[再検出周期] を調整します。グローバル サーバーは、リージョナル サーバーが検出を完了するとすぐに検出を開始します。

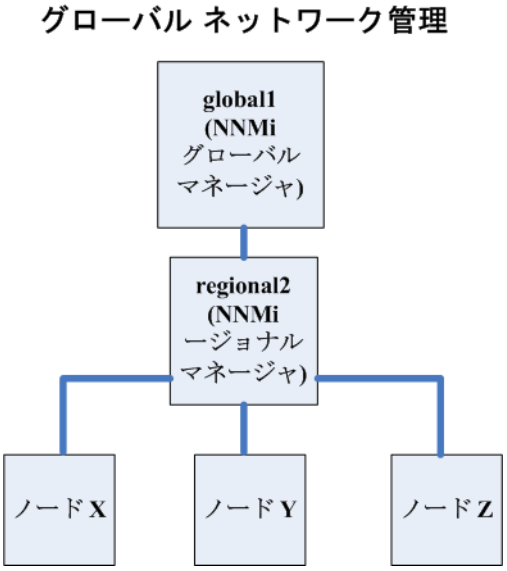


14 **[保存して閉じる]** をクリックします。

デバイスのステータス ポーリングまたは設定ポーリング

リージョナル NNMi 管理サーバー regional2 が Node X を検出して管理し、グローバル NNMi 管理サーバー global1 が リージョナル NNMi 管理サーバー regional2 に接続すると想定します。

図 16 ノードのステータス ポーリングまたは設定ポーリング



global1 から Node X のステータスをポーリングするには、以下を実行します。

1 global1 から、**[インベントリ]** ワークスペースの **[ノード]** をクリックします。

2 ノード インベントリから Node X を選択します。

3 **[アクション] > [ステータスのポーリング]** メニュー項目を使用して、Node X のステータス ポーリングを要求します。

4 NNMi 管理サーバー global1 は、リージョナル NNMi 管理サーバー regional2 からのステータス ポーリングを要求し、結果を画面に表示します。ステータス ポーリング要求は、global1 と regional2 のどちらから発行しても問題はありません。ステータス ポーリングの結果は同じものが表示されます。

global1 で Node X の最新の検出情報を取得するようにするには、以下を実行して global1 から Node X の設定ポーリングを行います。

1 global1 から、**[インベントリ]** ワークスペースの **[ノード]** をクリックします。

2 ノード インベントリから Node X を選択します。

3 **[アクション] > [設定のポーリング]** メニュー項目を使用して、Node X の設定ポーリングを要求します。

4 NNMi 管理サーバー global1 は、リージョナル NNMi 管理サーバー regional2 からの設定ポーリングを要求し、結果を画面に表示します。設定ポーリング要求は、global1 と regional2 のどちらから発行しても問題はありません。設定ポーリングの結果は同じものが表示されます。

グローバル マネージャを使ったデバイス ステータスの判定と NNMi インシデント生成

NNMi 管理サーバー global1 は、リージョナル マネージャ regional1 と regional2 からくるステータス変更をリッスンし、ローカル データベースにあるステータスを更新します。

NNMi 管理サーバー regional1 と regional2 の NNMi StatePoller サービスは、監視するデバイスの状態の値を計算します。global1 は、regional1 と regional2 から状態の値の更新を受け取ります。global1 は、自分が検出するノードにポーリングしますが、regional1 と regional2 によって管理されているノードにはポーリングしません。

regional1 によって管理されているノードの管理モードを変更した後、global1 上の管理モードも変更されます。ネットワーク管理者が regional1 または regional2 によって管理されるネットワーク機器の追加、削除、変更を行うと、regional1 または regional2 はそれらのネットワーク デバイスの変更について global1 を更新します。

global1 は、regional1 と regional2 によって転送されてきたノード オブジェクト データなど、独自の Causal Engine とトポロジを使用してインシデントを生成します。これは、生成するインシデントが、トポロジに違いがある場合に、regional1 と regional2 のインシデントとは少し異なる場合があることを意味します。

フィルタリングが global1. の接続性に影響する可能性があるため、転送フィルタを regional1 や regional2 に使用することは避けたほうがよいでしょう。ここで生じる差異が、global1 と 2 つのリージョナル (regional1 と regional2) との間の根本原因分析での差異になる可能性があります。ほとんどの場合、転送フィルタの使用しないことを選択すると、グローバル NNMi 管理サーバーのトポロジは大きくなります。これは、より正確な根本原因分析の結果を得るのに役立ちます。

追加の設定をしないと、regional1 はトラップを global1 に転送しません。これを行うには、特定のトラップを global1 に転送するように regional1 を設定する必要があります。HP では、グローバル マネージャに過剰な負荷がかからないように、リージョナル マネージャは量の少ない、重要なトラップを転送するよう設定することをお勧めします。NNMi は、転送されたトラップが TrapStorm インシデントを引き起こすような場合、転送されたトラップを削除します。NNMi コンソールで TrapStorm Management Event の詳細を参照してください。

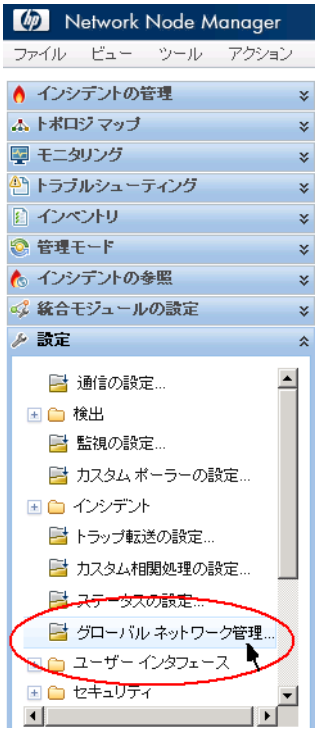
グローバル ネットワーク管理でアプリケーション フェイルオーバーの設定を行う

グローバル マネージャとリージョナル マネージャの両方を、アプリケーション フェイルオーバーを使用するよう設定できます。グローバル マネージャとリージョナル マネージャは、アクティブなシステムを自動的に検出して接続します。

グローバル マネージャでのアプリケーション フェイルオーバーの設定

アプリケーション フェイルオーバーを認識するよう global1 を設定するには、以下を実行します。

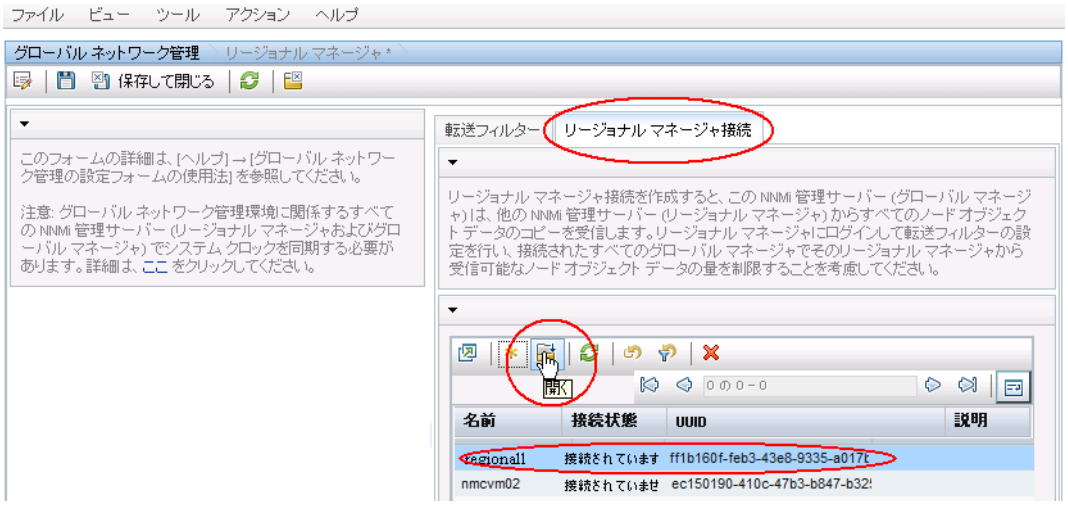
1 global1 の NNMi コンソールで、**[設定]** ワークスペースの **[グローバル ネットワーク管理]** をクリックします。



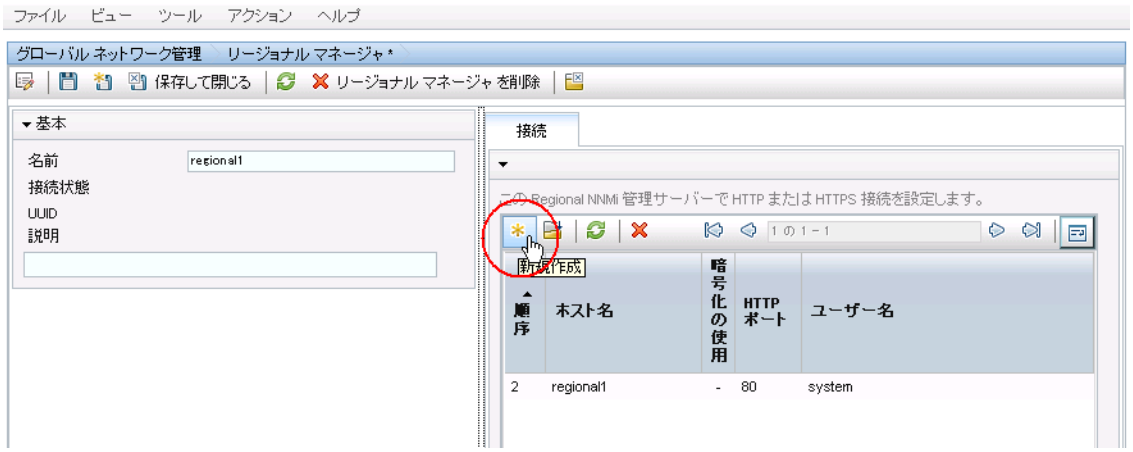
regional1 をアプリケーション フェイルオーバー用に設定し、セカンダリ サーバーとして regional1_backup を設定したと想定します。

2 **[リージョナル マネージャ接続]** をクリックします。

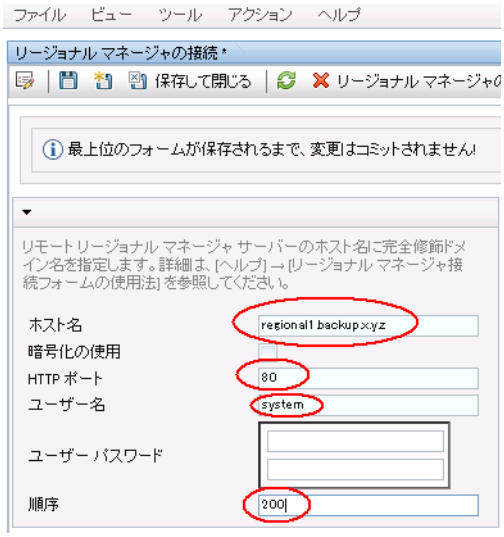
3 regional1 を選択して **[開く]** アイコンをクリックします。



4 **[新規作成]** アイコンをクリックします。



5 **[ホスト名]**、**[HTTP ポート]**、**[ユーザー名]**、および **[順序]** に値を入力します。順番の値には、regional1 より大きな値を設定します。



6 **[保存して閉じる]** を 3 回クリックして作業を保存します。

リージョナル マネージャが失敗すると、グローバル マネージャは以下を実行します。

a プライマリに問い合わせます。

b プライマリからの応答がない場合、セカンダリに問い合わせます。

グローバル システムでアクティブ システムが応答しないことを検出すると、順序の番号が最も小さいものから再接続を試みます。

グローバル ネットワーク管理のトラブルシューティングのヒント

NNMi ヘルプのトラブルシューティング情報

グローバル ネットワーク管理のトラブルシューティング情報については、NNMi ヘルプの「*グローバル ネットワーク管理のトラブルシューティング*」を参照してください。

クロック同期

グローバル ネットワーク管理 (グローバル マネージャとリージョナル マネージャ) やシングル サインオン (SSO) に属するネットワーク環境内のすべての NNMi 管理サーバーは、それぞれの内部タイム クロックを世界標準時で同期化する必要があります。たとえば、UNIX (HP-UX/Linux/Solaris) ツールの Network Time Protocol Daemon (NTPD) や使用可能な Windows オペレーティング システム ツールなどの時刻の同期プログラムを使用します。

NNMi コンソールの下部に次のメッセージが表示される場合の対応は、次のとおりです。

`NNMi がリージョナル マネージャに接続されていません。[ ヘルプ ] > [ システム情報 ] をクリックし、[ グローバル ネットワーク管理 ] タブを選択します。`

グローバル マネージャの `nnm.0.0.log` ファイルに次のメッセージがないか確認します。

`警告 : <number of seconds> のクロックの違いにより、システム <serverName> には接続されません リモート時間は、<date/time> です。`

クロックが合わなくなり、再同期化が必要です。グローバル マネージャの `nnm.0.0.log` ファイルに次のメッセージがないか確認します。

`警告 : <number of seconds> のクロックの違いにより、システム <serverName> には接続されません リモート時間は、<date/time> です。`

この警告が表示されて数分以内に、NNMi はリージョナル マネージャ接続を切断します。また、NNMi コンソールの下部に次のメッセージが表示されます。

`NNMi がリージョナル マネージャに接続されていません。[ ヘルプ ] > [ システム情報 ] をクリックし、[ グローバル ネットワーク管理 ] タブを選択します。`

グローバル ネットワーク管理システム情報

グローバル ネットワーク管理接続に関する情報を表示するには、**[ヘルプ] > [システム情報]** を選択して **[グローバル ネットワーク管理]** タブをクリックします。

グローバル マネージャからのリージョナル マネージャ検出の同期化

global1 と regional2 の間で情報に矛盾があることに気がついたと想定します。それを解決するため、global1 から **nnmnoderediscover.ovpl** スクリプトを実行し、global1 と regional2 を同期化します。実行の結果、regional2 は新しい検出結果を使用して global1 を更新します。

244 ページ の図 16 に示したネットワークについて考えます。regional2 をノード X、Y、および Z とそのノード セット全体を global1 を使用して同期化すると想定します。以下のコマンドを実行してノード X、Y、および Z と global1 を同期化します：**nnmnoderediscover.ovpl -u *username* -p *password* -rm regional2** 詳細については、*nnmnoderediscover.ovp* リファレンス ページまたは UNIX のマンページを参照してください。

破損した global1 上のデータベースの修復

global1 のサービスを停止し、データベースを復元する必要がある場合、いくつかの方法があります。

1. global1 のデータベースを正しく復元すると、regional1 と regional2 は global1 を使用してキャッシュされた情報を同期化します。global1 をオンラインに戻した後、手動で行う手順はありません。
2. global1 のサービスが長時間停止すると、手順 1 は正常に機能しないことがあります。これを解消するには、global1 で **nnmnoderediscover.ovpl** スクリプトを実行して global1、regional1 および regional2 で新たな検出を開始します。この場合、さらに迅速に更新されたステータス情報を入手するため、キー デバイスに対してステータス ポーリングを実行できます。
3. global1 のデータベースを復元できない場合、**nnmsubscription.ovpl** スクリプトを使用して古い global1 データを regional1 と regional2 のデータベースから消去するには、サポートに問い合わせる必要があります。

NNMi 9.0x から NNMi 9.10 へのアップグレード

グローバルネットワーク管理によってサポートされている NNMi のバージョン

グローバルマネージャが、NNMi 9.0x パッチ 2 またはそれより前のレベルのパッチを実行しているリージョナルマネージャに接続されている場合、グローバルマネージャとリージョナルマネージャ間の SNMP クエリは機能しません。これを解決するには、リージョナルマネージャを NNMi 9.0x パッチ 3 またはそれより後のレベルのパッチにアップグレードします。最良の結果を得るには、グローバルマネージャのバージョンと NNMi パッチレベルが、リージョナルマネージャと同じである必要があります。HP は、NNMi 9.0x リージョナルマネージャに接続されている NNMi 9.10 グローバルマネージャをサポートしています。

グローバルネットワーク管理のアップグレード手順

グローバルネットワーク管理環境に設定されている NNMi 管理サーバーをアップグレードするには、以下の順序で NNMi 管理サーバーをアップグレードします。

1. グローバルマネージャを NNMi 9.0x から NNMi 9.10 にアップグレードします。
2. リージョナルマネージャを NNMi 9.0x から NNMi 9.10 にアップグレードします。

グローバルネットワーク管理機能は、アップグレードを完了する間、機能し続けますが、新規 NNMi 9.10 機能の中には、リージョナル NNMi 管理サーバーのアップグレードが完了するまでグローバル NNMi 管理サーバーで機能しないものもあります。

グローバル ネットワーク管理と NNM iSPI または第三者の統合

NNM iSPI または第三者の統合は、導入にあたりそれぞれ独自のガイドラインがあります。この章の例では、複数の NNM iSPI を `regional1` のみ、`global1` のみ、または `regiona1` と `global1` の両方に配備できます。その他の NNM iSPI または第三者の統合については、`regional1` と `global1` の両方にインストールされている必要があります。詳細については、NNM iSPI または第三者の統合に関するドキュメントを参照してください。

IPv6 用 NNMi Advanced の設定

IPv6 管理機能を使用するには、NNMi Advanced ライセンスを購入してインストールする必要があります。この章での NNMi は、NNMi Advanced ライセンスがインストールされている NNMi を指します。

NNMi の IPv6 管理により、インタフェース、ノード、サブネットも含めた IPv6 アドレスの検出と監視が可能になります。シームレスな統合を提供するため、NNMi は IPv4 と IPv6 両方のアドレスを含めるよう IP アドレスモデルを拡張します。NNMi では、可能なかぎりすべての IP アドレスが等しく扱われます。IPv4 アドレスに関連するほとんどの機能は IPv6 アドレスについても使用可能です。ただし、いくつか例外があります。NNMi コンソールに表示される IPv6 情報の詳細については、NNMi ヘルプを参照してください。

この章には、以下のトピックがあります。

- 機能説明
- 必要条件
- ライセンス
- サポートされる設定
- NNMi のインストール
- IPv6 機能のアクティブ化
- IPv6 機能の非アクティブ化

機能説明

NNMi IPv6 管理機能には、以下の機能があります。

- IPv6 専用デバイスおよびデュアルスタック デバイスの IPv6 インベントリ検出
  - IPv6 アドレス
  - IPv6 サブネット
  - IPv6 アドレス、サブネット、インタフェース、およびノード間の関連付け

- 以下のためのネイティブ IPv6 SNMP 通信
  - ノードの検出
  - インタフェースの監視
  - トラップと通知の受信と転送
- デュアルスタック デバイスでの IPv4 または IPv6 通信 (管理アドレス) の自動選択。NNMi コンソールを使用し、**[設定]** ワークスペースにある **[通信の設定]** で、SNMP 管理アドレス設定を IPv4 または IPv6 に設定します。
- IPv6 アドレス フォルト 監視のためのネイティブ ICMPv6 通信
- IPv6 アドレスまたはホスト名を使用したシード済みデバイスの検出
- IPv6 レイヤ 3 隣接検出ヒントを使用した IPv6 デバイスの自動検出
- LLDP (Link Layer Discovery Protocol) IPv6 隣接情報を使用するレイヤ 2 隣接検出ヒントを使用した IPv6 デバイスの自動検出
- IPv4、IPv6 情報の統合表示
  - ノード、インタフェース、アドレス、サブネット、および関連付けのインベントリ ビュー
  - IPv4 デバイスと IPv6 デバイス用のレイヤ 2 隣接ビューおよびトポロジ マップ
  - IPv4 デバイスと IPv6 デバイス用のレイヤ 3 隣接ビューおよびトポロジ マップ
  - インシデント、結果、根本原因分析
- NNMi コンソール アクション : IPv6 アドレスとノードに対する ping と traceroute
- IPv6 アドレスとアドレス範囲を使用した NNMi 設定
  - 通信の設定
  - 検出の設定
  - 監視の設定
  - ノードとインタフェース グループ
  - インシデントの設定
- IPv6 インベントリとインシデント用の SDK Web サービス サポート
- IPv6 インタフェースに対する NNM iSPI Performance for Metrics のサポート

NNMi IPv6 管理機能には、以下は含まれません。

- IPv6 サブネット接続の検出
- 検出のための IPv6 ping スィープの使用
- IPv6 ネットワーク パス ビュー (Smart Path)
- IPv6 リンク ローカル アドレス障害監視
- 検出シードとしての IPv6 リンク ローカル アドレスの使用

必要条件

管理サーバーの仕様および NNMi のインストールの詳細については、『NNMi デプロイメント リファレンス』、『NNMi リリース ノート』、および『NNMi システムおよびデバイスのサポート マトリックス』を参照してください。

ネイティブ IPv6 通信を使用するには、NNMi 管理サーバーはデュアルスタック システムであることが必要です。つまり、IPv4 と IPv6 両方を使用して通信するということです。

IPv6 は、Windows オペレーティング システムではサポートされていません。IPv6 をサポートするオペレーティング システムの詳細については、『NNMi システムおよびデバイスのサポート マトリックス』を参照してください。その他に、以下の要件があります。

- 少なくとも 1 つのネットワーク インタフェースで IPv4 を有効化し設定する必要があります。
- IPv6 を有効化し、管理する必要のある IPv6 ネットワークに接続する少なくとも 1 つのネットワーク インタフェースで、グローバル ユニキャスト アドレスを持つ必要があります。
- NNMi 管理サーバーに IPv6 ルートを設定し、IPv6 を使用して NNMi で検出と監視を行うデバイスと NNMi が通信できるようにする必要があります。

IPv4 専用の NNMi 管理サーバーを使用することもできますが、IPv4/IPv6 デュアルスタック デバイスを NNMi で完全に管理することはできなくなります。たとえば、IPv4 専用管理サーバーを使用すると、NNMi は IPv6 専用デバイスの検出、IPv6 シードとヒントを使用した検出、および IPv6 アドレスを持つデバイス上での障害の監視はできません。

NNMi 管理サーバーで使用される DNS サーバーは、DSN から IPv6 アドレスへのホスト名と IPv6 アドレス から DSN へのホスト名を解決する必要があります。たとえば、AAAA DNS レコードからのホスト名と AAAA DNS へのホスト名を解決する必要があります。つまり、DNS サーバーはホスト名を 128 ビット IPv6 アドレスにマッピングする必要があります。IPv6 対応 DNS サーバーが使用できない場合でも、NNMi は正しく機能しますが、NNMi では IPv6 アドレスを使用するノードの DNS ホスト名の判定や表示は行いません。

ライセンス

すでに説明したように、IPv6 管理機能を使用するには NNMi Advanced ライセンスを購入してインストールする必要があります。NNMi Advanced ライセンスの取得とインストールの詳細については、115 ページの「NNMi ライセンスの取得」を参照してください。

NNMi 製品には、インスタントオンライセンス用パスワードが含まれています。これは一時的なものですが、有効な NNMi Advanced ライセンスです。できるだけ早く、永久ライセンス キーを入手してインストールしてください。

サポートされる設定

NNMi をサポートするオペレーティング システム構成の詳細については、『NNMi システムおよびデバイスのサポート マトリックス』を参照してください。

管理サーバー

以下の表に、IPv4 専用およびデュアルスタック両方の NNMi 管理サーバーの機能を示します。

表 20　管理サーバーの機能

機能	IPv4 専用	デュアルスタック
IPv4 通信 (SNMP、ICMP)	対応	対応
IPv6 通信 (SNMP、ICMPv6)	非対応	対応
デュアルスタック管理ノード	対応	対応
IPv4 シードを使用した検出	対応	対応
IPv6 シードを使用した検出	非対応	対応
IPv4 アドレスおよびサブネット インベントリ	対応	対応
IPv6 アドレスおよびサブネット インベントリ	対応	対応
SNMP を使用したインタフェース ステータスとパフォーマンス	対応	対応
ICMP を使用した IPv4 アドレス ステータス	対応	対応
ICMPv6 を使用した IPv6 アドレス ステータス	非対応	対応
IPv6 専用管理ノード	非対応	対応
IPv6 シードを使用した検出	非対応	対応
IPv6 アドレスおよびサブネット インベントリ	非対応	対応
SNMP を使用したインタフェース ステータスとパフォーマンス	非対応	対応
ICMPv6 を使用した IPv6 アドレス ステータス	非対応	対応
IPv4 専用管理ノード	対応	対応
IPv4 シードを使用したノード検出	対応	対応
IPv4 シードを使用したノード検出	対応	対応

表 20　管理サーバーの機能 (続く)

SNMP を使用したインタフェース ステータスとパフォーマンス	対応	対応
SNMP を使用したインタフェース ステータスとパフォーマンス	対応	対応
IPv4 アドレスおよびサブネット インベントリ	対応	対応

IPv6 をサポートする SNMP MIB

NNMi では、IPv6 用の以下の SNMP MIB がサポートされています。

- RFC 4293 (現在の IETF 標準)
- RFC 2465 (元の IETF 提案)
- Cisco IP-MIB

NNMi のインストール

NNMi のインストールでは、インストール スクリプトに IPv6 機能が含まれますが、これらの IPv6 機能は手動で有効化する必要があります。IPv6 機能を有効化するには、まず NNMi Advanced ライセンスを購入して適用する必要があります。次に、`nms-jboss.properties` ファイルを編集して、IPv6 が機能するよう手動で設定する必要があります。

IPv6 機能のアクティブ化

IPv6 専用デバイスの検出や IPv6 アドレス ステータスの監視など、IPv6 通信を必要とする機能では、NNMi 管理サーバーに IPv6 グローバル ユニキャスト アドレスが設定され機能することが必要です。

以下に示す手順は、IPv6 機能を有効にする方法を説明しています。

- NNMi Advanced ライセンスのインストール
- `nms-jboss.properties` ファイルにある IPv6 マスター スイッチの有効化

先に進む前に、前のセクションで説明した必要条件すべてについてレビューと確認を行います。

1. NNMi に同梱されたインスタントオンライセンスを使用、または NNMi Advanced ライセンスをインストールします。NNMi ライセンスの取得とインストールの詳細については、115 ページの「NNMi ライセンスの取得」を参照してください。IPv6 機能は、基本 NNMi ライセンスでは使用できません。
2. `nms-jboss.properties` ファイルを編集します。以下の場所を探してください。
   - *UNIX*: `$NNM_PROPS/nms-jboss.properties`

3 # Enable NNMi IPv6 Management で始まるテキストを探します。

NNMi では、各プロパティの完全な記述を用意しており、nms-jboss.properties ファイルのコメントとして示しています。

a NNMi で IPv6 通信を有効化するには、以下のプロパティをコメント解除します。

java.net.preferIPv4Stack=false

プロパティをコメント解除するには、行の先頭から #! 文字を削除します。

b NNMi で IPv6 通信全体を有効化するには、以下のプロパティをコメント解除します。

com.hp.nnm.enableIPv6Mgmt=true

c nms-jboss.properties ファイルを保存して閉じます。

4 オプションで、デュアルスタック管理ノードの SNMP 管理アドレス設定を指定します。デュアルスタック管理ノードは、IPv4 または IPv6 いずれかを使用して通信できるノードです。これには、以下の手順を実行します。

a NNMi コンソールで、**[設定]** ワークスペースにある **[通信の設定]** をクリックします。

b [IP バージョン設定] フィールドで、[IPv4]、[IPv6]、または [いずれか] を選択します。

c 変更を保存します。

5 NNMi 管理サーバーを再起動します。

a NNMi 管理サーバーで **ovstop** コマンドを実行します。

b NNMi 管理サーバーで **ovstart** コマンドを実行します。

6 以下のコマンドを使用して、NNMi プロセスを確認します。

ovstatus -v ovjboss

起動に成功すると、以下のように表示されます。

```
object manager name: ovjboss
 state:                RUNNING
 PID:                  <Process ID #>
 last message:         Initialization complete.
 exit status:          -
 additional info:
            SERVICE                                  STATUS
           CommunicationModelService                 サービスが起動されました
           CommunicationParametersStatsService       サービスが起動されました
           EventsCustomExportService                 サービスが起動されました
           ExtensionDeployer                         サービスが起動されました
           IslandSpotterService                      サービスが起動されました
           KeyManager                                サービスが起動されました
           ManagedNodeLicenseManager                 サービスが起動されました
           ModelChangeNotificationAdapter            サービスが起動されました
```

MonitoringSettingsService	サービスが起動されました
NMSLogManager	サービスが起動されました
NamedPoll	サービスが起動されました
NetworkApplication	サービスが起動されました
NmsApa	サービスが起動されました
NmsDisco	サービスが起動されました
NmsEvents	サービスが起動されました
NmsEventsConfiguration	サービスが起動されました
NmsExtensionNotificationService	サービスが起動されました
NmsModel	サービスが起動されました
NmsWorkManager	サービスが起動されました
NnmTrapService	サービスが起動されました
RbaConfig	サービスが起動されました
RbaManager	サービスが起動されました
SpmdjbossStart	サービスが起動されました
StagedIcmp	サービスが起動されました
StagedSnmp	サービスが起動されました
StatePoller	サービスが起動されました
TrustManager	サービスが起動されました

7 IPv6 を有効化すると、NNMi ビューには、新たに検出されたノードの IPv6 インベントリが表示されます。次の検出サイクルの間に、NNMi ビューにはその前の検出ノードに関連する IPv6 インベントリが表示されます。

スピードアップを図るには、デュアルスタック ノードとわかっているノードを選択し、NNMi コンソールで **[アクション] > [設定のポーリング]** コマンドを使用します。`nnmnoderediscover.ovpl` スクリプトを使用して、NNMi 検出キューにノードを追加することもできます。詳細については、*nnmnoderediscover.ovpl* のリファレンス ページまたは UNIX のマンページを参照してください。

NNMi 管理サーバーで IPv6 通信を有効化すると、NNMi は ICMPv6 を使用して IPv6 アドレス フォルトがないかノードの監視を開始します。

IPv6 機能の非アクティブ化

以下のいずれかの方法を使用して、管理上 IPv6 機能を無効化することができます。

1 `nms-jboss.properties` ファイルの IPv6 マスター スイッチをオフにし、NNMi を再起動します。

2 NNMi Advanced ライセンスを期限切れにするか、または基本 NNMi ライセンスに置き換えます。

   NNMi ライセンスの変更の詳細については、115 ページの「NNMi ライセンスの取得」を参照してください。

以下のセクションでは、IPv6 を無効化した後の NNMi の動作とインベントリのクリーンアップについて説明します。

非アクティブ化後の IPv6 監視

IPv6 管理または IPv6 通信が完全に無効になると、StatePoller サービスは ICMPv6 による IPv6 アドレスの監視をすぐに停止します。NNMi は、これらのアドレスの IP アドレス状態を [未ポーリング] に設定します。アドレスを選択し、このアドレスに対して **[アクション] > [モニタリングの設定]** を使用すると、関連する [監視設定] ルールで [IP アドレスの障害のポーリング] が有効になっている場合でも、NNMi は「障害 ICMP ポーリングの有効化 : false」と表示します。

非アクティブ化後の IPv6 インベントリ

一度 NNMi が完全に IPv6 インベントリを検出すると、以下の場合には、NNMi にそのインベントリを自動的に消去させることができます。

- マスター IPv6 スイッチをオンにした後で、オフにして NNMi を再起動した。

  NNMi は IPv6 インベントリをすぐに削除しません。NNMi は SNMP ノード の IPv6 インベントリを次の検出サイクルで削除します。NNMi は 非 SNMP IPv6 ノードを削除しません。IPv6 ノードは、NNMi インベントリから手動で削除する必要があります。

- NNMi Advanced ライセンスが期限切れ、または誰かがライセンスを削除した。NNMi は、NNMi の基本ライセンスを使用します。基本ライセンスは、検出されたノードすべての管理を続行するのに十分な機能があります。

  NNMi は 非 SNMP IPv6 ノードすべてをインベントリからすぐに削除します。NNMi は SNMP ノードをすべて再検出し、IPv6 データはすべて削除します。

- NNMi Advanced ライセンスが期限切れ、または誰かがライセンスを削除した。NNMi は、NNMi 基本ライセンスを使用します。基本ライセンスは、検出したノードすべての管理を続行するのに十分な機能はありません。NNMi はすぐに、非 SNMP IPv6 ノードを削除します。Licensing サービスは、ライセンスを受けたインベントリ能力を超える SNMP ノードに [管理対象外] 状態のマークを付けます。NNMi はすぐに、管理対象 SNMP ノードから得た IPv6 データを削除します。

  管理対象外の SNMP ノードの場合は、以下の手順を実行します。

  a 追加ライセンス機能をインストールします。

  b NNMi コンソールの **[アクション] > [管理モード] > [管理]** コマンドを使用して、Licensing サービスによって unmanaged とマークされているノードの管理モードを変更します。nnmmanagementmode.ovpl スクリプトを使用して、これらのノードも管理できます。詳細については、*nnmmanagementmode.ovpl* のリファレンス ページ、または UNIX のマンページを参照してください。

  c NNMi コンソールにある **[アクション] > [設定のポーリング]** コマンドを使用して、NNMi で検出できるようにします。nnmnoderediscover.ovpl スクリプトを使用して、これらのノードも検出できます。詳細については、*nnmnoderediscover.ovpl* のリファレンス ページまたは UNIX のマンページを参照してください。

- NNMi Advanced ライセンスの期限が切れた、または誰かがライセンスを削除した。NNMi 基本ライセンスをインストールしなかった。

  NNMi によって直ちに SNMP IPv6 以外のノードがすべて削除され、残りのノードが自動的に管理対象外となります。この状況を解決するには、以下の手順を実行します。

  a 有効なライセンスをインストールします。

  b NNMi コンソールの **[アクション] > [管理モード] > [管理]** コマンドを使用して、`Licensing` サービスによって `unmanaged` とマークされているノードの管理モードを変更します。`nnmmanagementmode.ovpl` スクリプトを使用して、これらのノードも管理できます。詳細については、*nnmmanagementmode.ovpl* のリファレンス ページ、または UNIX のマンページを参照してください。

  c NNMi コンソール にある **[アクション] > [設定のポーリング]** コマンドを使用して、NNMi が `unmanaged` から `managed` に変更したノードを検出できるようにします。`nnmnoderediscover.ovpl` スクリプトを使用して、これらのノードも検出できます。詳細については、*nnmnoderediscover.ovpl* のリファレンス ページ、または UNIX のマンページを参照してください。

  d IPv6 リストを作成してから IPv6 インベントリを削除するには、**[アクション] > [設定のポーリング]** コマンドを使用して、各管理対象ノードから設定情報を取得します。

IPv6 インベントリ クリーンアップ時の既知の問題点

IPv6 インベントリが残る場合があります。たとえば、NNMi が SNMP を使用して、ある IPv6 ノードを正常に管理し、次の検出の前にそのノードにアクセスできなくなったような場合です。既存の検出システムの設計上、検出プロセスは SNMP を使用した通信ができなくなったノードを更新できません。このようにして残ったノードを削除するには、通信の問題を解決してから、NNMi コンソールの **[アクション] > [設定のポーリング]** コマンドを使用してそれらのノードの設定情報を取得する必要があります。ネイティブ IPv6 ノードの場合、NNMi コンソールから直接ノードを削除します。

Solaris ゾーン環境での NNMi の実行

Solaris オペレーティングシステムのサポート対象バージョンでは、Solaris ゾーン環境で特別な設定を行わなくても、HP Network Node Manager i Software (NNMi) が動作します。

この章には、以下のトピックがあります。

- Solaris ゾーンでの NNMi のインストール
- Solaris ゾーンでのトラップ転送
- Solaris ゾーン環境での NNMi アプリケーションフェイルオーバーの実行
- Solaris ゾーン環境の HA での NNMi の実行

Solaris ゾーンでの NNMi のインストール

Solaris ゾーン環境で NNMi アプリケーションフェイルオーバーを実装する場合は、262 ページの「Solaris ゾーン環境での NNMi アプリケーションフェイルオーバーの実行」を参照してください。

高可用性 (HA) で Solaris ゾーンを実行する場合は、262 ページの「Solaris ゾーン環境の HA での NNMi の実行」を参照してください。

他のすべての導入モデルの場合は、『NNMi インストール ガイド』の説明に従って NNMi をインストールします。

Solaris ゾーンでのトラップ転送

NNMi が管理対象デバイスから受信した SNMP トラップを別のアプリケーションに転送する場合を考えます。これを行うには、**[設定]** ワークスペースの **[トラップ転送の設定]** に移動します。詳細については、NNMi ヘルプを参照してください。

Solaris ゾーン環境では未処理トラップの転送がサポートされていないため、**[元のトラップ]** 転送オプションは選択しないでください。Solaris ゾーン環境で NNMi を実行する場合、他のいずれかの転送オプションを選択してください。

Solaris ゾーン環境での NNMi アプリケーションフェイルオーバーの実行

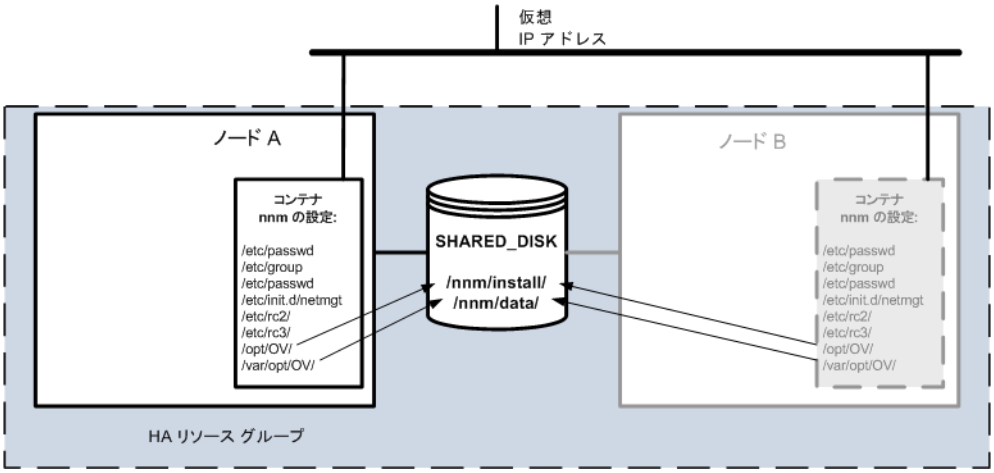
Solaris ゾーン環境で NNMi アプリケーションフェイルオーバー機能を使用する場合、2 つの各物理システムのゾーンに NNMi をインストールします。

267 ページの「アプリケーション フェイルオーバー構成の NNMi の設定」の説明に従ってアプリケーション フェイルオーバーを設定します。この手順全体で、「サーバー X」は一方のゾーンを表し、「サーバー Y」はもう一方のゾーンを表します。

Solaris ゾーン環境の HA での NNMi の実行

Solaris ゾーン環境では、HA クラスタで NNMi を実行するために NNMi が提供するソリューションを実装する必要はありません。Veritas Cluster Server (VCS) はゾーンを認識するため、図 17 に示すようにゾーンの HA リソースグループを設定します。

図 17　　HA で実行される Solaris ゾーンでの NNMi



これは、この環境で NNMi を実行するための最低限の設定です。NNMi のインストール プロセスでは、nmsdb グループに nmsdbmgr ユーザーが作成され、起動設定がホスト システムに追加されます。このセットアップは HA クラスタの 2 番目のノードに複製されます。

NNMi をインストールして、HA リソースグループ内のゾーンで実行するには、以下の手順を実行します。

1. 共有ディスクで、NNMi インストール フォルダを作成します。
   - `/nnm/install`
   - `/nnm/data`
2. ノード A で、**nnm** という新しいゾーンを作成して準備します。
   a. Solaris ゾーンのマニュアルの説明に従って、ゾーン **nnm** を作成します。

      すべての設定パラメータはゾーン作成時に設定されます。

   b. ゾーン **nnm** を起動します。

c ゾーン **nnm** にログオンし、以下のシンボリックリンクを作成します。

— 共有ディスクの /nnm/install/ を指し示す /opt/OV/

— 共有ディスクの /nnm/data/ を指し示す /var/opt/OV/

d ゾーン **nnm** からログオフして、そのゾーンをシャットダウンします。

3 ノード B で、**nnm** という同一の新しいゾーンを作成して、NNMi をインストールします。

a ノード A のゾーン **nnm** と同じプロパティ (IP アドレスなど) を使用して、ゾーン **nnm** を作成します。

b ゾーン **nnm** を起動します。

c ゾーン **nnm** にログオンし、以下のシンボリックリンクを作成します。

— 共有ディスクの /nnm/install/ を指し示す /opt/OV/

— 共有ディスクの /nnm/data/ を指し示す /var/opt/OV/

d 以下のコマンドを入力して NNMi インストーラがシンボリック リンクに従うように指定します。

```
PKG_NONABI_SYMLINKS=true
```

e **nnm** ゾーン内に NNMi をインストールします。

NNMi は、共有ディスクの /nnm/install/ および /nnm/data/ ディレクトリにインストールされます。

f **nnm** ゾーン外からアクセスできる一時保存場所 (共有ディスクなど) に以下のファイルをコピーします。

— /etc/passwd

— /etc/group

— /etc/shadow

— /etc/init.d/netmgt

g ゾーン **nnm** からログオフして、そのゾーンをシャットダウンします。

4 ノード A で、NNMi で変更されたシステム ファイルをコピーして NNMi を起動します。

a ゾーン **nnm** を起動します。

b ゾーン **nnm** にログオンし、手順 3 で特定した一時保存場所からゾーンの適切な場所にファイルをコピーします。

— /etc/passwd

— /etc/group

— /etc/shadow

— /etc/init.d/netmgt

c (ノード B で NNMi をインストールするときに作成された設定を複製するために) 以下のシンボリック リンクを作成します。

— `/etc/init.d/netmgt` を指し示す `/etc/rc0.d/K01netmgt`

— `/etc/init.d/netmgt` を指し示す `/etc/rc1.d/K01netmgt`

— `/etc/init.d/netmgt` を指し示す `/etc/rc2.d/K01netmgt`

— `/etc/init.d/netmgt` を指し示す `/etc/rc3.d/S98netmgt`

— `/etc/init.d/netmgt` を指し示す `/etc/rcS.d/K01netmgt`

d 以下のコマンドを実行して NNMi を起動します。

```
ovstart
```

5 ノード A とノード B の両方のゾーン **nnm** を含むリソースグループが作成されるように、Veritas Cluster Server を設定します。

詳細については、VCS のマニュアルを参照してください。

復元

HP Network Node Manager i Software (NNMi) では、ハードウェア障害の場合に NNMi データを保護するため、次の 2 つの方法がサポートされます。

- NNMi のアプリケーション フェイルオーバーでは、組み込み NNMi データベースのトランザクション ログのコピーが同一設定システムで維持され、ディザスタ リカバリが提供されます (NNMi で Oracle データベースが使用されている場合は、2 つのシステムが同一のデータベースに別々の時間に接続されます)。
- 高可用性 (HA) クラスタで NNMi を実行すると、組み込み NNMi データベースと設定ファイルが共有ディスクに保持され、NNMi 管理サーバーがほぼ 100 パーセント利用されます (NNMi で Oracle データベースが使用されている場合は、共有ディスクに NNMi 設定ファイルが含まれ、2 つのシステムが同一のデータベースに別々の時間に接続されます)。

両方の手法では、現在の NNMi 管理サーバーで障害が発生すると、第 2 システムが自動的に NNMi 管理サーバーになります。

表 21 では、NNMi データ復元の 2 つの方法のさまざまな側面を比較しています。

表 21　NNMi データ復元の比較

比較項目	NNMi のアプリケーション フェイルオーバー	HA クラスタで動作する NNMi
必要なソフトウェア製品	NNMi または NNMi Advanced	• NNMi または NNMi Advanced • 個別に購入する HA 製品
フェイルオーバーにかかる時間	組み込み NNMi データベース : トランザクションログを処理する時間 (通常の状態では、NNM iSPI を使用しない NNMi の場合、10-60 分間)。 Oracle NNMi データベース : ほぼ瞬時。	通常の状態ではNNM iSPIを使用しない NNMi の場合、5-30 分間。
フェイルオーバーの透過性	部分的。NNMi 管理サーバーの IP アドレスは、スタンバイ サーバーだったものの物理アドレスに変わります。ユーザーは新しい IP アドレスで NNMi コンソールに接続する必要があります。一部のアプリケーションは NNMi 管理サーバーの動作に従いますが、大部分のアプリケーション (NNM iSPI など) は従いません。	完全。すべての接続では HA クラスタの仮想 IP アドレスが使用され、これはフェイルオーバー時にも変わりません。
アクティブ サーバーとスタンバイ サーバーの相対的な近接性	LAN または WAN	LAN または WAN (一部の HA 製品のみ)

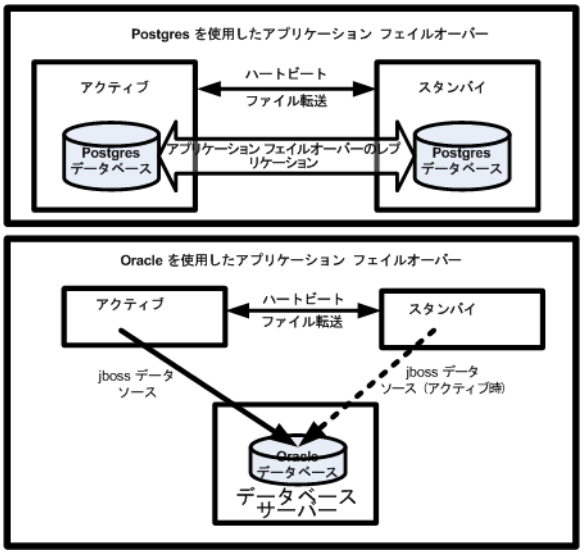
表 21　NNMi データ復元の比較

比較項目	NNMi のアプリケーション フェイルオーバー	HA クラスタで動作する NNMi
購入ライセンス	機能ごと • 商用ライセンスは、最初のアクティブ サーバーの IP アドレスが対象になります。 • 非商用ライセンスは、最初のスタンバイ サーバーの IP アドレスが対象になります。	機能ごと • 商用ライセンスは、HA クラスタのいずれかの物理システムの IP アドレスが対象になります。 • 非商用ライセンスは、HA クラスタの仮想 IP アドレスが対象になります。
インストールするライセンス	• 最初のアクティブ サーバーには商用ライセンス キー。 • 最初のスタンバイ サーバーには非商用ライセンス キー。	• 最初のアクティブサーバーには、共有ディスクで管理される非商用ライセンスキー。
NNM iSPI のサポート	さまざまなサポートがあります。各 NNM iSPI のマニュアルを参照してください。	
グローバルネットワーク管理とのインタラクション	• アプリケーションフェイルオーバーまたは HA 用に各グローバルマネージャを設定可能。 • アプリケーション フェイルオーバーまたは HA 用に各リージョナル マネージャを設定可能。 • それぞれの設定には、2 つの物理システムが必要です。 • グローバルマネージャまたはリージョナルマネージャがフェイルオーバーすると、NNMi は、グローバルマネージャとリージョナルマネージャ間の接続を再確立します。	
NNMi のメンテナンス	パッチまたはアップグレードを適用する前に、NNMi のアプリケーションフェイルオーバークラスタを停止する必要があります。	HA を設定解除しないで、NNMi にパッチおよびアップグレードを適用できます。

この項では以下の章について説明します。

- アプリケーション フェイルオーバー構成の NNMi の設定
- 高可用性クラスタに NNMi を設定する

アプリケーション フェイルオーバー構成の NNMi の設定



重要なネットワーク機器の障害発生を知らせ、その障害の根本原因を示す HP Network Node Manager i Software (NNMi) は、多くの IT プロフェッショナルから信頼を寄せられています。NNMi 管理サーバーに障害が発生した場合でも、引き続き NNMi がネットワーク機器の障害発生を知らせてくれる必要があります。このニーズを満たすのが **NNMi のアプリケーション フェイルオーバー**で、NNMi プロセスのアプリケーション コントロールをアクティブな NNMi 管理サーバーからスタンバイ NNMi 管理サーバーに引き渡すことで、NNMi の機能は中断なく提供されます。

この章には、以下のトピックがあります。

- アプリケーション フェイルオーバーの概要
- アプリケーション フェイルオーバーの基本セットアップ
- アプリケーション フェイルオーバー構成の NNMi の設定
- アプリケーション フェイルオーバー機能の使用
- フェイルオーバー後、元の設定に戻る
- NNM iSPI およびアプリケーション フェイルオーバー
- 統合アプリケーション
- アプリケーション フェイルオーバーの無効化
- 管理タスクおよびアプリケーション フェイルオーバー
- ネットワーク レイテンシ / 帯域に関する考慮

アプリケーション フェイルオーバーの概要

アプリケーション フェイルオーバー機能は、組み込みデータベースまたは Oracle データベースを使用して NNMi をインストールすることで利用できるようになります。システムにアプリケーション フェイルオーバー機能を設定すると、NNMi は NNMi 管理サーバーの障害を検出した場合に、セカンダリ サーバーに NNMi の機能を引き渡します。

NNMi のアプリケーション フェイルオーバー設定では、以下の用語と定義を使用しています。

- **アクティブ** : NNMi プロセスを実行中のサーバー。
- **スタンバイ** ：フェイルオーバーのイベントを待機している NNMi クラスタ内のシステム。このシステムは NNMi プロセスを実行していません。
- **Cluster Member**: クラスタに接続するために JGroups 技術を使用しているシステムで実行中の Java プロセス。1 つのシステムに複数のメンバを登録できます。
- **Postgres**: トポロジ、インシデント、設定情報などの情報を保存するために NNMi が使用する組み込みデータベース。
- **Cluster Manager**: アプリケーション フェイルオーバー機能におけるサーバーの監視と管理に使用される `nnmcluster` プロセスおよびツール。

アプリケーション フェイルオーバーの基本セットアップ

アプリケーション フェイルオーバー機能を導入するには、NNMi を 2 つのサーバーにインストールします。この章では、この 2 つの NNMi 管理サーバーを**アクティブ** サーバーと**スタンバイ** サーバーとして説明します。通常の運用では、アクティブ サーバーのみが NNMi サービスを実行します。

アクティブおよびスタンバイ NNMi 管理サーバーは、各 NNMi 管理サーバーのハートビートを監視するクラスタの一部です。アクティブ サーバーに障害が発生し、そのハートビートが消失すると、スタンバイ サーバーがアクティブ サーバーになります。

アプリケーション フェイルオーバーが正しく機能するには、NNMi 管理サーバーが以下の要件を満たしている必要があります。

- 両方の NNMi 管理サーバーが同じ種類のオペレーティング システムを実行している必要があります。たとえば、アクティブ サーバーが HP-UX オペレーティング システムを実行している場合、スタンバイ サーバーも HP-UX オペレーティング システムを実行している必要があります。
- 両方の NNMi 管理サーバーは同じバージョンの NNMi を実行している必要があります。たとえば、アクティブサーバーで NNMi 9.10 を実行している場合、スタンバイ サーバーでも同一の NNMi バージョンである NNMi 9.10 がインストールされている必要があります。NNMi パッチ レベルについても、同一レベルのパッチが両サーバーに適用されている必要があります。
- 両方の NNMi 管理サーバーのシステム パスワードが同一である必要があります。
- Windows オペレーティング システムの NNMi インストールでは、`%NnmDataDir%` および `%NnmInstallDir%` のシステム変数を同一の値に設定している必要があります。

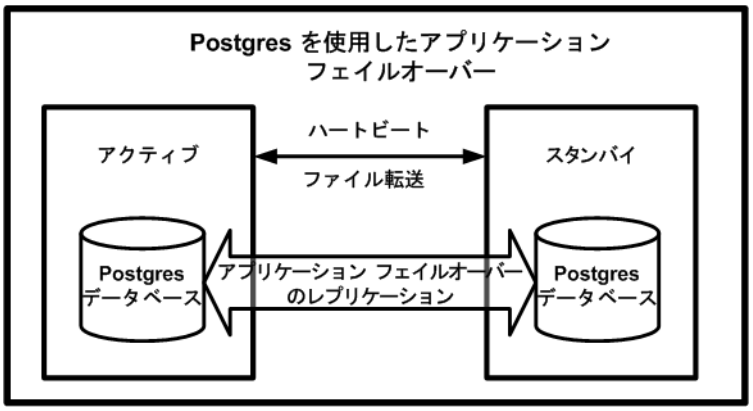
- 両方の NNMi 管理サーバーは同じデータベースを実行している必要があります。たとえば、両方の NNMi 管理サーバーで Oracle を実行しているか、両方の NNMi 管理サーバーで組み込みデータベースを実行している必要があります。アプリケーション フェイルオーバー機能を使用する場合、種類の異なるデータベースを組み合わせて使用することはできません。
- 両方の NNMi 管理サーバーのライセンス属性が同一である必要があります。たとえば、ノード カウントおよびライセンス取得済みの機能が同一である必要があります。
- NNMi が初回検出の高度なステージに入るまで、アプリケーション フェイルオーバーを有効にしないでください。詳細については、69 ページの「検出の評価」を参照してください。

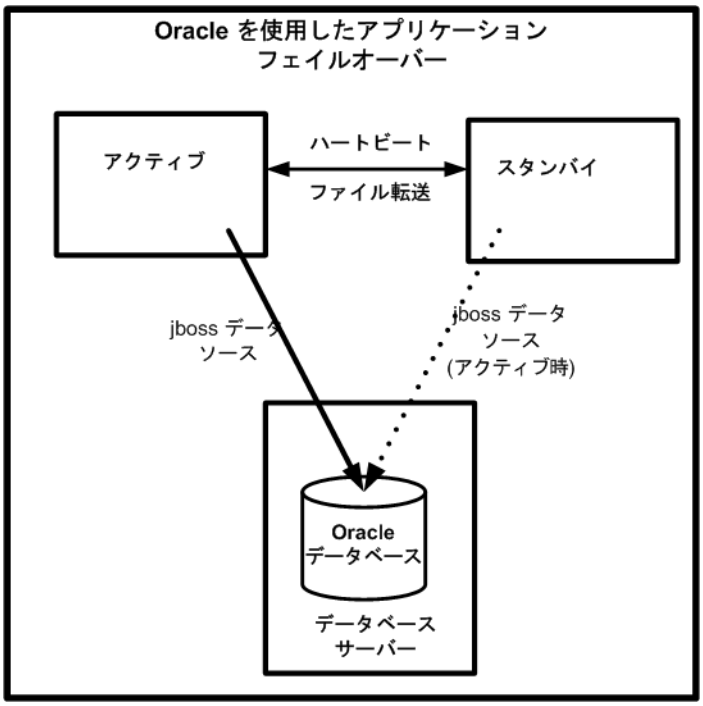
アプリケーション フェイルオーバーが正しく機能するには、アクティブ サーバーとスタンバイ サーバーは相互のネットワーク アクセスに制限のないことが必要です。この条件を満たしたら、270 ページの「アプリケーション フェイルオーバー構成の NNMi の設定」に示した手順を実行してください。詳細については、605 ページの「NNMi 9.10 およびウェルノウン ポート」を参照してください。

ファイルをロックしたり、ネットワークのアクセスを制限したりするソフトウェアが原因で、NNMi の通信の問題が発生する場合があります。こうしたアプリケーションで、NNMi が使用するファイルとポートを無視するように設定します。

アプリケーション フェイルオーバー構成の NNMi の設定

1 NNMi インストール ガイドに記載のとおり、アクティブ サーバー (サーバー X) とスタンバイ サーバー (サーバー Y) に NNMi をインストールします。





2 115 ページの「NNMi ライセンスの取得」に記載されているように、サーバー X の各ライセンスに対し、サーバー Y に使用する同じ非商用のライセンスを取得し、サーバー Y にインストールします。

3 各サーバーで **ovstop** コマンドを実行して NNMi をシャットダウンします。

Oracle データベースでアプリケーション フェイルオーバーを使用している場合は、スタンバイ サーバーの NNMi プロセスはすでに停止しています。

4 `nms-cluster.properties` ファイルに含まれる指示を参考にして、サーバー X (アクティブ) およびサーバー Y (スタンバイ) のアプリケーション フェイルオーバー機能を設定します。以下の手順を実行します。

以下の手順では、ファイルのテキスト ブロックの行のコメントを解除し、テキストを変更することを**編集**と呼びます。

a 以下のファイルを編集します。

— *Windows*:
`%NnmDataDir%¥shared¥nnm¥conf¥props¥nms-cluster.properties`

— *UNIX*: `$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`

b NNMi クラスタに一意の名前を宣言します。アクティブ サーバーとスタンバイ サーバーが同じ名前を使用するように設定します。

`com.hp.ov.nms.cluster.name=`*`MyCluster`*

c nms-cluster.propertiesファイルの`com.hp.ov.nms.cluster.member.hostnames` パラメータに、クラスタのすべてのノードのホスト名を追加します。

`com.hp.ov.nms.cluster.member.hostnames = `*`fqdn_for_active, fqdn_for_standby`*

NNMi 9.0x では、アプリケーション フェイルオーバー機能で UDP ソリューションがサポートされ、クラスタ ホストはネットワークで自動的に検出されました。NNMi 9.10 からは UDP ソリューションが排除され、TCP ソリューションのみがサポートされます。NNMi 9.0x から移行する場合は、アプリケーション フェイルオーバーを機能させるために手順 c を完了してクラスタ ホスト名を定義する必要があります。

d *オプション*。`nms-cluster.properties` ファイル内のその他の com.hp.ov.nms.cluster* パラメータを定義します。各パラメータの変更方法については、`nms-cluster.properties` ファイル内の指示に従ってください。

Oracle データベースでアプリケーション フェイルオーバーを使用している場合、NNMi では `nms-cluster.properties` ファイルに含まれるデータベース パラメータが無視されます。

5 選択した方法によって、124 ページの「自己署名証明書を使用するようにアプリケーション フェイルオーバーを設定する」に示した指示、または、126 ページの「認証機関を使用するようにアプリケーション フェイルオーバーを設定する」に示した指示を実行します。

アプリケーション フェイルオーバー機能を設定するときには、両方のノードの `nnm.keystore` および `nnm.truststore` ファイルの内容をマージして、`nnm.keystore` および `nnm.truststore` を 1 つのファイルにする必要があります。*方法を選択し、手順 5 の 1 セットの指示を完了する必要があります。*

6 以下のファイルをサーバー X からサーバー Y にコピーします。

- *Windows*:
`%NnmDataDir%¥shared¥nnm¥conf¥nnmcluster¥cluster.keystore`
- *UNIX*:
`$NnmDataDir/shared/nnm/conf/nnmcluster/cluster.keystore`

7 次のコマンドをサーバー X とサーバー Y の両方で実行します : **nnmcluster**
各サーバーに、以下のように表示されます。

```
============================== Current cluster state ==============================
State ID: 000000001000000005
Date/Time: 15 Mar 2011 - 09:37:58 (GMT-0600)
Cluster name: ThisCluster (key CRC:626,187,650)
Automatic failover: Enabled
NNM database type: Embedded
NNM configured ACTIVE node is: NO_ACTIVE
NNM current ACTIVE node is: NO_ACTIVE
Cluster members are:

  Local?    NodeType  State                     OvStatus     Hostname/Address
  ------    --------  -----                     --------     ----------------------------
* REMOTE    ADMIN     n/a                       n/a          serverX.xxx.yyy.yourcompany.com/
16.78.61.68:7800
  (SELF)    ADMIN     n/a                       n/a          serverY.xxx.yyy.yourcompany.com/
16.78.61.71:7800
```

画面には、サーバー X とサーバー Y の両方がリストされます。両方のノードの情報が表示されない場合、それらのノードはお互いに通信していません。手順を進める前に、以下の点を確認して、修正してください。

— クラスタ名が、サーバー X とサーバー Y で異なっているかどうか。

— キー CRC が、サーバー X とサーバー Y で異なっているかどうか。サーバー X とサーバー Y の両方で、以下のファイルの内容を確認してください。

Windows: `%NnmDataDir%¥shared¥nnm¥conf¥nnmcluster¥cluster.keystore`

UNIX: `$NnmDataDir/shared/nnm/conf/nnmcluster/cluster.keystore`

— サーバー X またはサーバー Y のファイアウォールによって、ノードの通信が妨げられているかどうか。

— `nnm.keystore` ファイルと `nnm.truststore` ファイルを確実にマージしたかどうか。このエラーが表示されるのは、**nnmcluster** コマンドを実行した後です。

— サーバー X とサーバー Y で、異なるオペレーティングシステムが実行されているかどうか。たとえば、サーバー X で Linux オペレーティングシステムが実行され、サーバー Y で Windows オペレーティングシステムが実行されている場合などです。このエラーが表示されるのは、**nnmcluster** コマンドを実行した後です。

— サーバー X とサーバー Y が、異なるバージョンの NNMi を実行しているかどうか。たとえば、サーバー X が NNMi 9.10 を実行しており、サーバー Y が NNMi 9.10 パッチ 1 (使用可能である場合) を実行している場合などです。このエラーが表示されるのは、**nnmcluster** コマンドを実行した後です。

8 サーバー X で、NNMi クラスタ マネージャを開始します。

nnmcluster -daemon

nnmcluster -daemon コマンドを NNMi 管理サーバー X で実行すると、NNMi クラスタ マネージャが以下の起動ルーチンを実行します。

— NNMi 管理サーバー X をクラスタに接続します。

— ほかの NNMi 管理サーバーが存在しないことを検知します。

— NNMi 管理サーバー X はアクティブ状態に変わります。

— NNMi 管理サーバー X (アクティブ サーバー) の NNMi サービスを開始します。

— データベースのバックアップを作成します。

詳細については、*nnmcluster* リファレンス ページ、または UNIX のマンページを参照してください。

9 サーバー X がクラスタの最初のアクティブ ノードになるまで数分待ちます。サーバー X で **nnmcluster -display** コマンドを実行し、表示された結果から ACTIVE_NNM_STARTING または ACTIVE_SomeOtherState の「ACTIVE」という語を検索します。サーバー X がアクティブ ノードであることを確認するまで手順 10 に進まないでください。

10 サーバー Y で NNMi クラスタ マネージャを開始します。

nnmcluster -daemon

nnmcluster -daemon コマンドを NNMi 管理サーバー Y で実行すると、NNMi クラスタ マネージャが以下の起動ルーチンを実行します。

— NNMi 管理サーバー Y をクラスタに接続します。

— NNMi 管理サーバー X が存在し、アクティブな状態であることが検出されます。ディスプレイに STANDBY_INITIALIZING と表示されます。

— NNMi 管理サーバー Y のデータベース バックアップが NNMi 管理サーバー X のバックアップと比較されます。一致しない場合は、新しいデータベース バックアップが NNMi 管理サーバー X (アクティブ) から NNMi 管理サーバー Y (スタンバイ) に送信されます。ディスプレイに STANDBY_RECV_DBZIP と表示されます。

— NNMi 管理サーバー Y は、スタンバイ状態に該当するバックアップに最低限必要となる、トランザクション ログの最小限のセットを受信します。ディスプレイに STANDBY_RECV_TXLOGS と表示されます。

— NNMi 管理サーバー Y は待機状態になり、新しいトランザクション ログとハートビート信号を NNMi 管理サーバー X から受信し続けます。ディスプレイに STANDBY_READY と表示されます。

詳細については、*nnmcluster* リファレンス ページ、または UNIX のマンページを参照してください。

11 フェイルオーバーが発生した場合、サーバー X の NNMi コンソールは機能しなくなります。サーバー X の NNMi コンソール セッションを閉じて、サーバー Y (新たにアクティブになったサーバー) にログオンします。NNMi ユーザーに、サーバー X (アクティブ NNMi 管理サーバー) とサーバー Y (スタンバイ NNMi 管理サーバー) への 2 つのブックマークを登録するように指示します。フェイルオーバーが発生すると、ユーザーはサーバー Y (スタンバイ NNMi 管理サーバー) に接続できます。

12 ネットワーク オペレーション センター (NOC) の担当者に、サーバー X とサーバー Y の両方にトラップを送信するようにデバイスを設定するように指示します。サーバー X (アクティブ) が実行している間、サーバー X は転送されたトラップを処理し、サーバー Y (スタンバイ) はそのトラップを無視します。

アプリケーション フェイルオーバー機能の使用

両方の NNMi 管理サーバーでクラスタ マネージャが実行しているため (アクティブ ノードとスタンバイ ノード)、クラスタ マネージャを使用してクラスタのステータスを表示できます。クラスタ マネージャには 3 つのモードがあります。

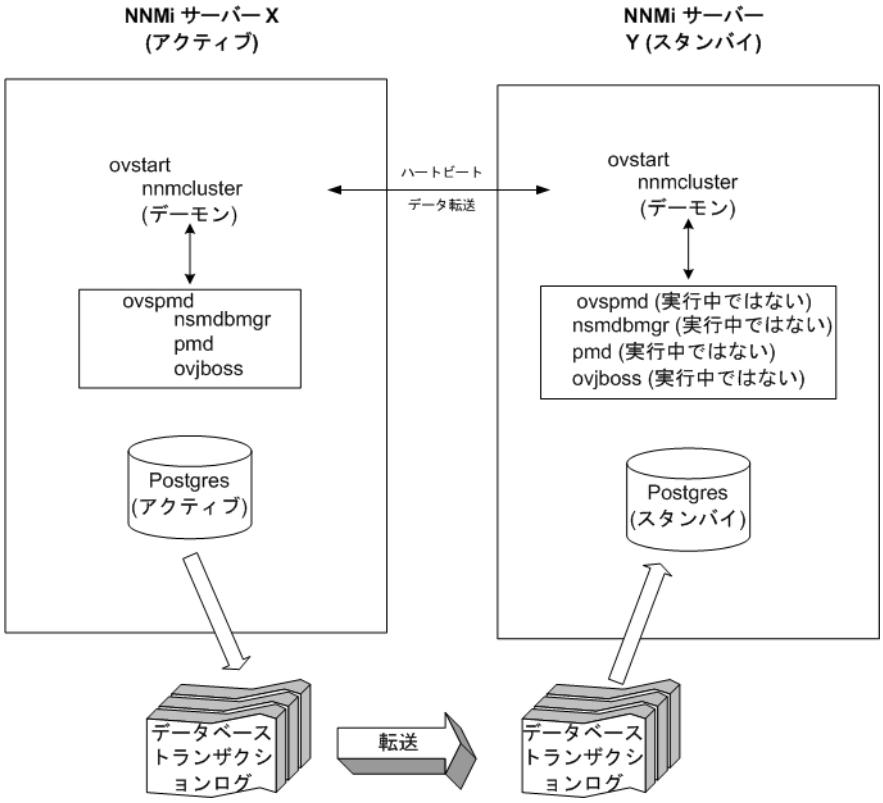
- デーモン モード: クラスタ マネージャのプロセスはバックグラウンドで実行し、**ovstop** および **ovstart** コマンドを使用して NNMi サービスを開始および停止します。
- インタラクティブ モード : クラスタ マネージャは、NNMi 管理者がクラスタの属性を表示および変更できるインタラクティブ セッションを実行します。たとえば、NNMi 管理者はこのセッションを使用して、アプリケーション フェイルオーバー機能を有効または無効にしたり、デーモン プロセスをシャットダウンしたりできます。
- コマンドライン モード : NNMi 管理者は、コマンド プロンプトでクラスタの属性を表示および変更します。

詳細については、*nnmcluster* リファレンス ページ、または UNIX のマンページを参照してください。

組み込みデータベースを使用したアプリケーション フェイルオーバーの動作

図 18 は、組み込みデータベースを使用した 2 つの NNMi 管理サーバーのアプリケーション フェイルオーバー設定を示します。この章の以降のセクションについて、この図を参照してください。

図 18　アプリケーション フェイルオーバーの設定 (組み込みデータベース)



アクティブ ノードとスタンバイ ノードの両方を開始すると、スタンバイ ノードはアクティブ ノードを検知してアクティブ ノードにデータベースのバックアップをリクエストしますが、NNMi サービスは開始しません。このデータベースのバックアップは 1 つの Java-ZIP ファイルとして保存されます。すでにスタンバイ ノードに以前のクラスタ接続から得た ZIP ファイルがあり、NNMi が、そのファイルとアクティブ サーバーの同期が確認された場合は、ファイルは再送されません。

アクティブ ノードとスタンバイ ノードの両方が実行している間、アクティブ ノードは定期的にデータベースのトランザクション ログをスタンバイ ノードに送信します。`nms-cluster.properties` ファイルの `com.hp.ov.nms.cluster.timeout.archive` パラメータの値を変更すると、このデータの転送頻度を変更できます。これらのトランザクション ログはスタンバイ ノードに蓄積されるため、スタンバイからアクティブになったときにすぐに利用することができます。

スタンバイノードがアクティブノードからデータベースの完全バックアップを受信すると、その情報を組み込みデータベースに取り込みます。また、`recovery.conf` ファイルを作成して、受信したすべてのトランザクションログを取り込んでからでないと他のサービスがデータベースを使用できないことを組み込みデータベースに知らせます。

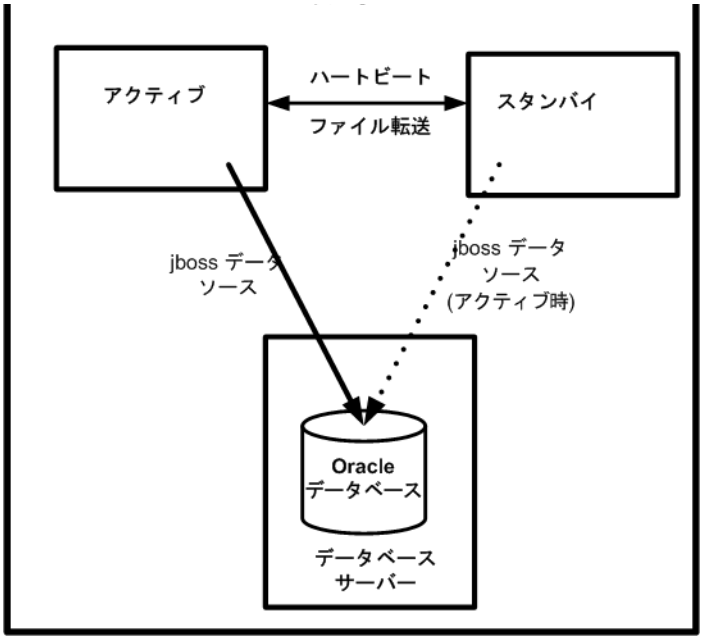
何らかの理由でアクティブ ノードが利用できなくなると、スタンバイ ノードは NNMi サービスを開始する **`ovstart`** コマンドを実行してアクティブになります。スタンバイ NNMi 管理サーバーは、残りの NNMi サービスを開始する前に、トランザクション ログをインポートします。

アクティブ NNMi システムに障害が発生すると、スタンバイ システムは、ディスカバリとポーリング アクティビティを開始します。このトランジションによって、障害が発生したシステムの診断と修理を行う間、NNMi はネットワークを監視およびポーリングし続けます。

Oracle データベースを使用したアプリケーション フェイルオーバーの動作

図 19 は、Oracle データベースを使用した、2 つの NNMi 管理サーバーのアプリケーション フェイルオーバーの設定を示します。この章の以降のセクションについて、この図を参照してください。

図 19　アプリケーション フェイルオーバーの設定 (Oracle データベース)



何らかの理由でアクティブ ノードが利用できなくなると、スタンバイ ノードは NNMi サービスを開始する **ovstart** コマンドを実行してアクティブになります。

アクティブ NNMi システムに障害が発生すると、スタンバイ システムは、ディスカバリとポーリング アクティビティを開始します。このトランジションによって、障害が発生したシステムの診断と修理を行う間、NNMi はネットワークを監視およびポーリングし続けます。

アプリケーション フェイルオーバーの例

アクティブ NNMi 管理サーバーがハートビートを送信しなくなり、フェイルオーバーが発生してしまう原因にはいくつかあります。

- 例 1: アクティブ NNMi 管理サーバーに障害が発生した。
- 例 2: システム管理者がアクティブな NNMi 管理サーバーをシャットダウンまたはリブートした。
- 例 3: NNMi 管理者がクラスタをシャットダウンした。
- 例 4: アクティブ NNMi 管理サーバーとスタンバイ NNMi 管理サーバーの間のネットワーク接続に障害が発生した。

  例 4 では、両方の NNMi 管理サーバーがアクティブな状態で稼動します。ネットワーク デバイスが復旧すると、2 つの NNMi 管理サーバーは自動的にネゴシエーションしてアクティブ ノードとして稼動するサーバーを決定します。

その他の ovstart および ovstop オプション

アプリケーション フェイルオーバーが設定された NNMi 管理サーバーで **ovstop** コマンドおよび **ovstart** コマンドを使用した場合、NNMi は以下のコマンドを実行します。

- ovstart: **nnmcluster -daemon**
- ovstop: **nnmcluster -disable -shutdown**

ovstop コマンドを実行すると、NNMi はスタンバイ ノードにフェイルオーバーしません。**ovstop** コマンドは、メンテナンスによる一時的な停止をサポートするように設計されています。フェイルオーバーを手動で行うには、**ovstop** コマンドに **-failover** オプションを使用します。詳細については、*ovstop* リファレンス ページ、または UNIX のマンページを参照してください。

ovstop コマンドに使用する以下のオプションは、アプリケーション フェイルオーバー クラスタに構成された NNMi 管理サーバーで使用します。

- **ovstop -failover**: ローカルのデーモン モードのクラスタ プロセスを停止し、スタンバイ NNMi 管理サーバーに強制的にフェイルオーバーします。以前にフェイルオーバー モードが無効にされている場合は、このコマンドで有効になります。このコマンドは **nnmcluster -enable -shutdown** と同等です。
- **ovstop -nofailover**: フェイルオーバー モードを無効にし、ローカルのデーモン モードのクラスタ プロセスを停止します。フェイルオーバーは行われません。このコマンドは **nnmcluster -disable -shutdown** と同等です。

- **ovstop -cluster**: アクティブ ノードとスタンバイ ノードを停止し、これらをクラスタから削除します。このコマンドは **nnmcluster -halt** と同等です。

UNIX オペレーティングシステムを実行している NNMi 管理サーバーで **shutdown** コマンドを実行すると、**ovstop** コマンドが自動的に実行され、アプリケーションフェイルオーバーが無効になります。これが最適な設定ではない場合もあります。メンテナンス中にアプリケーションフェイルオーバーを制御するには、shutdown コマンドを実行する前に、**nnmcluster -acquire** コマンドと **nnmcluster -relinquish** コマンドを使用してアクティブノードとスタンバイノードを目的の動作に設定します。詳細については、*nnmcluster* リファレンスページ、または UNIX のマンページを参照してください。

アプリケーション フェイルオーバーのインシデント

nnmcluster プロセスまたは **nnmcluster** コマンドを使用するユーザーが、ノードをアクティブとして開始すると、NNMi ではそのたびに以下のいずれかのインシデントが生成されます。

- *NnmClusterStartup*: NNMi クラスタは、アクティブ ノードがない状態で開始されました。したがって、このノードはアクティブ状態で起動されました。このインシデントの重大度は 「正常域」です。
- *NnmClusterFailover*: NNMi クラスタでアクティブ ノードの障害が検出されました。そのため、スタンバイ ノードがアクティブ ノードになり、そのノードで NNMi サービスが開始されました。このインシデントの重大度は 「重要警戒域」です。

フェイルオーバー後、元の設定に戻る

アクティブ ノードで障害が発生し、スタンバイ ノードがアクティブ ノードとして機能しているとします。以前のアクティブ ノードで問題を解決したら、目的のアクティブ ノードでコマンド **nnmcluster -acquire** を実行し、元の設定に戻ります。詳細については、*nnmcluster* リファレンス ページ、または UNIX のマンページを参照してください。

NNM iSPI およびアプリケーション フェイルオーバー

NNMi と一緒に Smart Plug-in (iSPI) を導入する場合、以下の要件を満たすと iSPI 用のアプリケーション フェイルオーバー機能を使用できます。

- NNM iSPI は NNMi 管理サーバーで動作する。
- NNM iSPI は、NNMi と同じ組み込みデータベース インスタンスを使用する。

NNM iSPI Performance for QA、NNM iSPI Performance for Metrics、および NNM iSPI Performance for Traffic にはこの説明は該当しません。NNMi アプリケーション フェイルオーバー機能を設定する場合は、これらの iSPI を専用サーバーにインストールする必要があります。この場合、iSPI は、フェイルオーバーが発生すると、新しい NNMi 管理サーバーに自動的に接続します。NNMi アプリケーション フェイルオーバー設定の一環として、クラスタの各 NNMi 管理サーバーに NNM iSPI Performance for QA、NNM iSPI Performance for Traffic、または NNM iSPI Performance for Metrics 用のイネーブルメント スクリプトを実行します。

詳細については、NNM iSPI Performance for Metrics、NNM iSPI Performance for QA、または NNM iSPI Performance for Traffic ヘルプの「*アプリケーション フェイルオーバーのサポート*」を参照してください。

NNM iSPI のインストールに関する情報

アプリケーション フェイルオーバー クラスタのすでに一部である NNMi 管理サーバーに NNM iSPI をインストールするには、以下の手順を実行します。

1. 万一に備えて、以降の操作を行う前に、アクティブおよびスタンバイ NNMi 管理サーバーの両方で、**nnmconfigexport.ovpl** スクリプトを実行します。詳細については、40 ページの「ベストプラクティス : 既存の設定を保存」を参照してください。
2. 万一に備えて、以降の操作を行う前に、アクティブおよびスタンバイ NNMi 管理サーバーの NNMi データをバックアップします。詳細については、349 ページの「バックアップ領域」を参照してください。
3. 組み込みデータベースのみ : 万一に備えて、アクティブ NNMi 管理サーバーで、**nnmcluster -dbsync** コマンドを実行し、コマンドが完了するまで待ちます。
4. スタンバイ NNMi 管理サーバーで、以下のコマンドを実行します。

   nnmcluster -shutdown
5. スタンバイ NNMi 管理サーバーの以下のファイルを編集します。
   - *Windows*: `%NnmDataDir%¥shared¥nnm¥conf¥props¥nms-cluster.properties`
   - *UNIX*: `$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`
6. com.hp.ov.nms.cluster.name オプションをコメント アウトし、ファイルを保存します。
7. スタンバイ NNMi 管理サーバーで **ovstart** コマンドを実行します。すると、スタンドアロン (クラスタに属しない) 状態の NNMi サービスが表示されます。
8. 『iSPI インストール ガイド』で説明されているとおりに、スタンバイ NNMi 管理サーバーに NNM iSPI をインストールします。
9. アクティブ NNMi 管理サーバーで **nnmcluster -halt** コマンドを実行します。

10 アクティブ NNMi 管理サーバーの以下のファイルを編集します。

- *Windows*: `%NnmDataDir%¥shared¥nnm¥conf¥props¥nms-cluster.properties`
- *UNIX*: `$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`

11 com.hp.ov.nms.cluster.name オプションをコメント アウトし、ファイルを保存します。

12 アクティブ NNMi 管理サーバーで **ovstart** コマンドを実行します。すると、スタンドアロン (クラスタに属しない) 状態の NNMi サービスが表示されます。

13 『iSPI インストール ガイド』で説明されているとおりに、アクティブ NNMi 管理サーバーに NNM iSPI をインストールします。

14 アクティブおよびスタンバイ NNMi 管理サーバーの**両方**で、以下のファイルを編集します。

- *Windows*: `%NnmDataDir%¥shared¥nnm¥conf¥props¥nms-cluster.properties`
- *UNIX*: `$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`

15 com.hp.ov.nms.cluster.name オプションをコメント解除し、各ファイルを保存します。

16 アクティブ NNMi 管理サーバーで **ovstart** コマンドを実行します。

17 アクティブ NNMi 管理サーバーがクラスタの最初のアクティブ ノードになるまで数分待ちます。アクティブ NNMi 管理サーバーで **nnmcluster -display** コマンドを実行し、表示された結果で、`ACTIVE_NNM_STARTING` または `ACTIVE_`*SomeOtherState* の「`ACTIVE`」という語を検索します。アクティブ NNMi 管理サーバーがアクティブ ノードであることを確認するまで手順 18 に進まないでください。

18 スタンバイ NNMi 管理サーバーで **ovstart** コマンドを実行します。

統合アプリケーション

HP ソフトウェア製品または第三者の製品が NNMi に統合された場合、統合に対する NNMi アプリケーション フェイルオーバー機能の影響は、製品が NNMi と通信する方法によって異なります。詳細については、「NNMi との統合」セクションの該当する章を参照してください。

統合製品の設定に NNMi 管理サーバーに関する情報が必要な場合は、以下の情報が適用されます。

- 将来的に必要であれば、統合する製品の設定で NNMi 管理サーバーの情報を更新できます。詳細については、「NNMi との統合」セクションの該当する章を参照してください。
- 機能停止が一時的なものである場合、サーバー X が復旧した後に統合する製品の使用を再開始できます。サーバー X のサービスを復旧するには、以下の手順に従います。

1 サーバー X で以下のコマンドを実行します。

```
nnmcluster -daemon
```

サーバー X がスタンバイ状態でクラスタに参加します。

2 サーバー X で以下のコマンドを実行します。

```
nnmcluster -acquire
```

サーバー X はアクティブ状態になります。

元のサーバー X がより長期に渡って機能停止となる可能性がある場合は、統合する製品内で、NNMi 管理サーバーの IP アドレスを更新できます。[IP アドレス] フィールドの変更方法については、統合する製品のドキュメントを参照してください。

アプリケーション フェイルオーバーの無効化

アプリケーション フェイルオーバーを設定し、数日間使用した後に、完全に無効化するとします。以下の情報は、アプリケーション フェイルオーバーを完全に無効にする方法を説明しています。アプリケーション フェイルオーバー クラスタに構成された、アクティブおよびスタンバイ NNMi 管理サーバーでのアクションを含め、以下の指示に従ってください。

1 アクティブ NNMi 管理サーバーで **nnmcluster -enable** コマンドを実行します。

2 アクティブ NNMi 管理サーバーで **nnmcluster -shutdown** コマンドを実行します。

3 既存のスタンバイ NNMi 管理サーバーが新しくアクティブ NNMi 管理サーバーになるまで数分待ちます。

4 新しいアクティブ (以前のスタンバイ) NNMi 管理サーバーで **nnmcluster -display** コマンドを実行します。

5 表示された結果で、ACTIVE_NNM_RUNNING ステータスを検索します。ACTIVE_NNM_RUNNING ステータスを確認できるまで、手順 4 を繰り返します。

6 新しいアクティブ (以前のスタンバイ) NNMi 管理サーバーで **nnmcluster -shutdown** コマンドを実行します。

7 DAEMON プロセスがなくなるまで、新しいアクティブ (以前のスタンバイ) で **nnmcluster -display** コマンドを繰り返し実行します。

8 クラスタに構成されている両方の NNMi 管理サーバーで、以下のファイルを編集します。

- *Windows*: %NnmDataDir%¥shared¥nnm¥conf¥props¥nms-cluster.properties
- *UNIX*: $NnmDataDir/shared/nnm/conf/props/nms-cluster.properties

9 両方の NNMi 管理サーバーの com.hp.ov.nms.cluster.name オプションをコメントアウトし、各ファイルを保存します。

10 両方の NNMi 管理サーバーの以下のファイルを編集します。

- *Windows*: %NnmDataDir%¥shared¥nnm¥databases¥Postgres¥postgresql.conf
- *UNIX*: $NnmDataDir/shared/nnm/databases/Postgres/postgresql.conf

11 各ファイルで、archive_command および archive_timeout で始まる行を削除します。これは、Windows NNMi 管理サーバーにおけるこれらの行の表示例です。サーバーによって、表示がやや異なります。

```
archive_command = 'nnmcluster.exe -archive "%p" "C:/Documents
and Settings/All Users/Application Data/HP/HP BTO Software/
shared/nnm/databases/Postgres_standby/TxWALs_send"/%f'

archive_timeout = 900
```

必ず変更を保存してください。

12 Windows NNMi 管理サーバーの場合、[サービス (ローカル)] コンソールに移動し、各サーバーで以下の手順を実行します。

a HP NNM Cluster Manager の [スタートアップの種類] を [無効] に設定します。

b HP Openview Process Manager の [スタートアップの種類] を [自動] に設定します。

13 以前のアクティブ NNMi 管理サーバーのみに **ovstart** コマンドを実行します。アプリケーション フェイルオーバー構成では、このサーバーは恒久 NNMi ライセンスを取得している NNMi 管理サーバーです。

14 以前のスタンバイ サーバーで非商用ライセンスを使用している場合は、その NNMi 管理サーバーで **ovstart** コマンドを実行しないでください。アプリケーション フェイルオーバー構成では、このサーバーは、非商用ライセンスを取得している NNMi 管理サーバーです。この NNMi 管理サーバーをスタンドアロン サーバーとして実行するには、恒久ライセンスを購入し、インストールする必要があります。詳細については、115 ページの「NNMi ライセンスの取得」を参照してください。

15 両方の NNMi 管理サーバーが正常に開始したら、スタンバイおよびアクティブ NNMi 管理サーバーから以下のディレクトリを削除します。

- *Windows*: %NnmDataDir%¥shared¥nnm¥databases¥Postgres_standby
- *UNIX*: $NnmDataDir/shared/nnm/databases/Postgres_standby

このディレクトリはデフォルトのディレクトリで、nms-cluster.properties ファイルにある com.hp.ov.nms.cluster.archivedir パラメータの値です。この手順では、この値が変更されていないことを前提としています。nms-cluster.properties ファイルの com.hp.ov.nms.cluster.archivedir パラメータの値を変更した場合は、変更後の新しい値に相当するディレクトリを削除します。

16 スタンバイおよびアクティブ NNMi 管理サーバーから以下のディレクトリを削除します。

- *Windows*: %NnmDataDir%¥shared¥nnm¥databases¥Postgres.OLD
- *UNIX*: $NnmDataDir/shared/nnm/databases/Postgres.OLD

管理タスクおよびアプリケーション フェイルオーバー

以下は、NNMi 管理サーバーへのパッチ適用や再起動などの管理タスクを行うときに、アプリケーション フェイルオーバーを効果的に管理する方法を説明しています。

アプリケーション フェイルオーバーおよび NNMi 9.10 へのアップグレード

NNMi アプリケーション フェイルオーバー設定で動作している NNMi 9.0x の旧バージョンのアップグレードを計画する場合、サポートされるアップグレード パスは、アプリケーション フェイルオーバーを一時的に設定解除し、それぞれの NNMi 管理サーバーを NNMi 9.10 にアップグレードしてから、アプリケーション フェイルオーバーを再設定します。

アプリケーション フェイルオーバーを設定している NNMi 管理サーバーをアップグレードするには、以下の手順を実行します。

1. 万一に備えて、以降の操作を行う前に、アクティブおよびスタンバイ NNMi 管理サーバーの両方で、**nnmconfigexport.ovpl** スクリプトを実行します。詳細については、40 ページの「ベストプラクティス : 既存の設定を保存」を参照してください。
2. 万一に備えて、以降の操作を行う前に、アクティブおよびスタンバイ NNMi 管理サーバーの NNMi データをバックアップします。詳細については、349 ページの「バックアップ領域」を参照してください。
3. *組み込みデータベースのみ* : 以下の手順をアクティブな NNMi 管理サーバーで実行します。この手順を完了すると、284 ページの手順 7 で示すスタンバイ NNMi 管理サーバーの起動が速くなります。
   a. **nnmcluster** コマンドを実行します。
   b. NNMi に入力を求められたら、「**dbsync**」と入力し、Enter キーを押します。表示される情報に以下のメッセージが含まれていることを確認します。

      ACTIVE_DB_BACKUP: アクティブ NNMi 管理サーバーが新しいバックアップを実行しています。
      ACTIVE_NNM_RUNNING: アクティブ NNMi 管理サーバーが、前のメッセージによって示されたバックアップを完了しました。
      STANDBY_RECV_DBZIP: スタンバイ NNMi 管理サーバーは、アクティブ NNMi 管理サーバーから新しいバックアップを取得しています。
      STANDBY_READY: スタンバイ NNMi 管理サーバーは、アクティブ NNMi 管理サーバーで障害が発生した場合に実行できる準備が整えられています。
4. スタンバイ NNMi 管理サーバーで **nnmcluster -shutdown** コマンドを実行します。すべての nnmcluster プロセスがスタンバイ NNMi 管理サーバーでシャットダウンします。
5. スタンバイ NNMi 管理サーバーで nnmcluster ノードが動作していないことを確認するには、*スタンバイ NNMi 管理サーバーで以下の手順を実行します。*
   a. **nnmcluster** コマンドを実行します。
   b. (SELF) とマークされているもの以外に nnmcluster ノード (ローカル) が存在しないことを確認します。1 つ以上のリモート ノードが存在することがあります。
   c. **exit** または **quit** を実行して、手順 a で開始したインタラクティブ nnmcluster プロセスを停止します。

6 *以下の手順をスタンバイ NNMi 管理サーバーで実行し、アプリケーション フェイルオーバーを一時的に無効にします。*

a 以下のファイルを編集します。

- *Windows*: `%NNM_SHARED_CONF%¥props¥nms-cluster.properties`
- *UNIX*: `$NNM_SHARED_CONF/props/nms-cluster.properties`

b `com.hp.ov.nms.cluster.name` パラメータをコメント アウトします。

c 変更を保存します。

7 スタンバイ NNMi 管理サーバーでプロセスを開始してから停止します。

a スタンバイ NNMi 管理サーバーで **ovstart** コマンドを実行します。**ovstart** コマンドを実行すると、スタンバイ NNMi 管理サーバーはトランザクション ログをアクティブ NNMi 管理サーバーからインポートします。

b **ovstart** コマンドの完了後、**ovstatus -v** コマンドを実行します。すべての NNMi サービスの状態が「`RUNNING`」と表示されます。

c スタンバイ NNMi 管理サーバーで **ovstop** コマンドを実行します。

8 NNMi インストール ガイドの指示に従い、スタンバイ NNMi 管理サーバーを NNMi 9.10 にアップグレードします。

NNMi 9.10 をサポートする iSPI バージョンに、スタンバイ NNMi 管理サーバーでインストールしたすべての iSPI をアップグレードする必要があります。

以前のアクティブ NNMi 管理サーバーが NNMi 9.0x を実行し、以前のスタンバイ NNMi 管理サーバーが NNMi 9.10 を実行しています。両方の NNMi 管理サーバーが個別に動作し、データベースは同期していません。つまり両方の NNMi 管理サーバーがネットワークを並行して監視しています。これらの NNMi 管理サーバーを数時間以上この設定のままにしないでください。この設定は、以前のスタンバイノードにインストールした非商用ライセンスの違反になります。

アップグレードを完了してこの状況を解決するには、以前のアクティブ ノードを NNMi 9.10 にアップグレードする時間を選択します。このアップグレードを完了する間、以前のスタンバイ ノードをオペレータに一時的に使用させてネットワークを監視させます。

この手順の残りの部分では、以前のアクティブ ノードのデータベース情報を維持して、以前のスタンバイ ノードのデータベース情報を破棄することが想定されています。

9 以前のアクティブ NNMi 管理サーバーで **nnmcluster -halt** コマンドを実行します。

10 以前のアクティブ NNMi 管理サーバーで nnmcluster ノードが動作していないことを確認するには、*以前のアクティブ NNMi 管理サーバーで以下の手順を実行します。*

a **nnmcluster** コマンドを実行します。

b `(SELF)` とマークされているもの以外に nnmcluster ノード (ローカル) が存在しないことを確認します。1 つ以上のリモート ノードが存在することがあります。

c **exit** または **quit** を実行して、手順 a で開始したインタラクティブ `nnmcluster` プロセスを停止します。

11 *以下の手順を以前のアクティブ NNMi 管理サーバーで実行し、アプリケーション フェイルオーバーを一時的に無効にします。*

a 以下のファイルを編集します。

- *Windows*: `%NNM_SHARED_CONF%¥props¥nms-cluster.properties`
- *UNIX*: `$NNM_SHARED_CONF/props/nms-cluster.properties`

b `com.hp.ov.nms.cluster.name` パラメータをコメント アウトします。

NNMi インストール ガイドの指示に従い、以前のアクティブ NNMi 管理サーバーを NNMi 9.10 にアップグレードします。

NNMi 9.10 をサポートする iSPI バージョンに、以前のアクティブ NNMi 管理サーバーでインストールしたすべての iSPI をアップグレードする必要があります。

2 つのサーバーで NNMi 9.10 を実行していますが、データベースが同期していないため、まだ個別に動作しています。

12 以前のアクティブ NNMi 管理サーバーで以下の手順を実行します。

a **ovstop** コマンドを実行します。

b 以下のファイルを編集します。

— *Windows*: `%NNM_SHARED_CONF%¥props¥nms-cluster.properties`

— *UNIX*: `$NNM_SHARED_CONF/props/nms-cluster.properties`

c `com.hp.ov.nms.cluster.name` パラメータの値を入力します。

d `com.hp.ov.nms.cluster.name` パラメータのコメントを解除します。

e 変更を保存します。

13 **ovstart** コマンドまたは **nnmcluster -daemon** コマンドを以前のアクティブ NNMi 管理サーバーで実行します。これがアクティブ ノードになりました。

14 アクティブ ノードを使用してネットワークを監視するように、オペレータに指示します。

以前のスタンバイ NNMi 管理サーバーは、284 ページの手順 9 から 285 ページの手順 13 のメンテナンス中に発生したすべてのデータベースアクティビティを破棄します。

15 以前のスタンバイ NNMi 管理サーバーで以下の手順を実行します。

a **ovstop** コマンドを実行します。

b 以下のファイルを編集します。

— *Windows*: `%NNM_SHARED_CONF%¥props¥nms-cluster.properties`

— *UNIX*: `$NNM_SHARED_CONF/props/nms-cluster.properties`

c `com.hp.ov.nms.cluster.name` パラメータのコメントを解除します。

d 変更を保存します。

16 **ovstart** コマンドまたは **nnmcluster -daemon** コマンドを以前のスタンバイ NNMi 管理サーバーで実行します。

この NNMi 管理サーバーはスタンバイ ノードになり、アクティブ ノードからデータベースのコピーを受信します。

17 NNM iSPI Performance for QA、NNM iSPI Performance for Metrics、または NNM iSPI Performance for Traffic をインストールし、アプリケーション フェイルオーバー機能を使用しており、さらに上記のアップグレード プロセスを完了した場合は、アクティブおよびスタンバイ NNMi 管理サーバーの各 NNM iSPI に NNM iSPI イネーブルメント スクリプトを実行します。

18 Linux NNMi 管理サーバーを使用している場合は、アクティブおよびスタンバイ NNMi 管理サーバーの両方で以下のコマンドを実行します。
chmod 777 /var/opt/OV/shared/perfSpi/datafiles/nnm_details.xml

アプリケーション フェイルオーバーおよび NNMi パッチ

両方の NNMi 管理サーバーは、NNMi の同じバージョンとパッチレベルを実行している必要があります。アクティブおよびスタンバイの NNMi 管理サーバーにパッチを追加するには、以下のいずれかの方法を使用します。

- アプリケーションフェイルオーバー用にパッチを適用する (アクティブとスタンバイの両方をシャットダウン)
  ネットワーク監視が中断されても問題にならない場合は、この手順を使用してください。
- アプリケーションフェイルオーバー用にパッチを適用する (1 つのアクティブ NNMi 管理サーバーを保持)
  ネットワーク監視の中断を回避する必要がある場合は、この手順を使用してください。

アプリケーションフェイルオーバー用にパッチを適用する (アクティブとスタンバイの両方をシャットダウン)

この手順を実行すると、パッチプロセスの一定の期間、両方の NNMi 管理サーバーが非アクティブになります。アプリケーション フェイルオーバーを設定している NNMi 管理サーバーにパッチを適用するには、以下の手順を実行します。

1 万一に備えて、以降の操作を行う前に、アクティブおよびスタンバイ NNMi 管理サーバーの両方で、**nnmconfigexport.ovpl** スクリプトを実行します。詳細については、40 ページの「ベストプラクティス : 既存の設定を保存」を参照してください。

2 万一に備えて、以降の操作を行う前に、アクティブおよびスタンバイ NNMi 管理サーバーの NNMi データをバックアップします。詳細については、349 ページの「バックアップ領域」を参照してください。

3 万一に備えて、アクティブ NNMi 管理サーバーで、以下の手順を実行します。

   a **nnmcluster** コマンドを実行します。

   b 組み込みデータベースのみ : NNMi に求められたら、「**dbsync**」と入力し、Enter キーを押します。表示される情報に以下のメッセージが含まれていることを確認します。

   ACTIVE_DB_BACKUP: アクティブ NNMi 管理サーバーが新しいバックアップを実行しています。
   ACTIVE_NNM_RUNNING: アクティブ NNMi 管理サーバーが、前のメッセージによって示されたバックアップを完了しました。
   STANDBY_READY: スタンバイ NNMi 管理サーバーの前のステータスを示します。
   STANDBY_RECV_DBZIP: スタンバイ NNMi 管理サーバーは、アクティブ NNMi 管理サーバーから新しいバックアップを取得しています。
   STANDBY_READY: スタンバイ NNMi 管理サーバーは、アクティブ NNMi 管理サーバーで障害が発生した場合に実行できる準備が整えられています。

4 アクティブ NNMi 管理サーバーで **nnmcluster -halt** コマンドを実行します。アクティブおよびスタンバイ NNMi 管理サーバーのすべての nnmcluster プロセスをシャットダウンします。

5 両方のサーバーで nnmcluster ノードが実行していないことを確認するには、*アクティブおよびスタンバイ NNMi 管理サーバーの両方で以下の手順を実行します。*

   a **nnmcluster** コマンドを実行します。

   b (SELF) とマークされているもの以外に nnmcluster ノードが存在しないことを確認します。

   c **exit** または **quit** を実行して、手順 a で開始したインタラクティブ nnmcluster プロセスを停止します。

6 アクティブ NNMi 管理サーバーで、nms-cluster.properties ファイルの com.hp.ov.nms.cluster.name パラメータをコメントアウトします。

   a 以下のファイルを編集します。

      — *Windows*: %NNM_SHARED_CONF%¥props¥nms-cluster.properties

      — *UNIX*: $NNM_SHARED_CONF/props/nms-cluster.properties

   b com.hp.ov.nms.cluster.name パラメータをコメント アウトします。

   c 変更を保存します。

7 パッチとともに提供された指示に従って、アクティブ NNMi 管理サーバーに NNMi パッチを適用します。

8 アクティブ NNMi 管理サーバーで、nms-cluster.properties ファイルの com.hp.ov.nms.cluster.name パラメータをコメント解除します。

   a 以下のファイルを編集します。

      — *Windows*: %NNM_SHARED_CONF%¥props¥nms-cluster.properties

      — *UNIX*: $NNM_SHARED_CONF/props/nms-cluster.properties

   b com.hp.ov.nms.cluster.name パラメータのコメントを解除します。

   c 変更を保存します。

9 アクティブ NNMi 管理サーバーで **ovstart** コマンドを実行します。

10 NNMi コンソール の **[ヘルプ] > [システム情報]** ウィンドウにある **[製品]** タブで情報を表示し、アクティブ NNMi 管理サーバーにパッチが正しくインストールされたことを確認します。

11 **nnmcluster -dbsync** コマンドを実行して、新しいバックアップを作成します。

12 287 ページの手順 a から 287 ページの手順 c に示されているように、スタンバイ NNMi 管理サーバーで、nms-cluster.properties ファイルの com.hp.ov.nms.cluster.name パラメータをコメントアウトします。

13 NNMi パッチをスタンバイ NNMi 管理サーバーに適用します。

14 287 ページの手順 a から 287 ページの手順 c に示されているように、スタンバイ NNMi 管理サーバーで、nms-cluster.properties ファイルの com.hp.ov.nms.cluster.name パラメータをコメント解除します。

15 スタンバイ NNMi 管理サーバーで **ovstart** コマンドを実行します。

16 NNM iSPI Performance for QA、NNM iSPI Performance for Metrics、または NNM iSPI Performance for Traffic をインストールし、アプリケーション フェイルオーバー機能を使用しており、さらに上記のパッチ プロセスを完了した場合は、アクティブおよびスタンバイ NNMi 管理サーバーの各 NNM iSPI に NNM iSPI イネーブルメント スクリプトを実行します。

17 Linux NNMi 管理サーバーを使用している場合は、アクティブおよびスタンバイ NNMi 管理サーバーの両方で以下のコマンドを実行します。
chmod 777 /var/opt/OV/shared/perfSpi/datafiles/nnm_details.xml

アプリケーションフェイルオーバー用にパッチを適用する (1 つのアクティブ NNMi 管理サーバーを保持)

この手順を実行すると、パッチプロセスの間、1 つの NNMi 管理サーバーが常にアクティブになります。

このプロセスでは、ネットワークが継続的に監視されますが、NNMi でパッチプロセス中に生じたトランザクションログは失われます。

アプリケーションフェイルオーバーを設定している NNMi 管理サーバーに NNMi パッチを適用するには、以下の手順を実行します。

1 万一に備えて、以降の操作を行う前に、アクティブおよびスタンバイ NNMi 管理サーバーの両方で、**nnmconfigexport.ovpl** スクリプトを実行します。詳細については、40 ページの「ベストプラクティス : 既存の設定を保存」を参照してください。

2 万一に備えて、以降の操作を行う前に、アクティブおよびスタンバイ NNMi 管理サーバーの NNMi データをバックアップします。詳細については、349 ページの「バックアップ領域」を参照してください。

3 2 つのデータベースを同期するには、いずれかの NNMi 管理サーバーで以下のコマンドを実行します。
nnmcluster -dbsync

dbsync オプションは、組み込みデータベースを使用する NNMi 管理サーバーで機能します。Oracleデータベースを使用するように設定された NNMi 管理サーバーで、**dbsync** オプションを使用しないでください。

4 進行状況を監視するには、アクティブとスタンバイの両方の NNMi 管理サーバーで以下のコマンドを実行します。
nnmcluster -display
アクティブ NNMi 管理サーバーが ACTIVE_NNM_RUNNING に戻り、スタンバイ NNMi 管理サーバーが STANDBY_READY に戻るまで待機してから、次に進んでください。

5 クラスタを無効にするには、アクティブ NNMi 管理サーバーで以下のコマンドを実行します。
nnmcluster -disable

6 以下のコマンドをスタンバイ NNMi 管理サーバーで実行して、スタンバイ NNMi 管理サーバーのクラスタを停止します。
nnmcluster -shutdown

7 以下のプロセスとサービスが終了しているのを確認してから、次に進みます。

— postgres

— ovjboss

8 nnmcluster プロセスが終了しているのを確認してから、次に進みます。nnmcluster プロセスが終了していない場合、他に方法がなければ、nnmcluster プロセスを手動で強制終了します。

9 スタンバイ NNMi 管理サーバーで、以下のファイルを編集します。

Windows: %nnmDataDir%¥shared¥nnm¥conf¥props¥nms-cluster.properties

UNIX: $nnmDataDir/shared/nnm/conf/props/nms-cluster.properties

10 行の先頭に **#** を入れてクラスタ名をコメントアウトし、変更を保存します。
#com.hp.ov.nms.cluster.name = NNMicluster

11 スタンバイ NNMi 管理サーバーに NNMi パッチをインストールします。

12 アクティブ NNMi 管理サーバーで以下のコマンドを実行して、アクティブ NNMi 管理サーバーのクラスタをシャットダウンします。
nnmcluster -halt

13 nnmcluster プロセスが終了していることを確認します。数分以内に終了しない場合は、nnmcluster プロセスを手動で終了してください。

14 スタンバイ NNMi 管理サーバーで、nms-cluster.properties ファイルからクラスタ名をコメント解除します。

15 以下のコマンドをスタンバイ NNMi 管理サーバーで実行して、スタンバイ NNMi 管理サーバーのクラスタを起動します。
nnmcluster -daemon

16 アクティブ NNMi 管理サーバーに NNMi パッチをインストールします。

17 アクティブ NNMi 管理サーバーで、nms-cluster.properties ファイルのエントリをコメント解除します。

18 以下のコマンドを使用して、アクティブ NNMi 管理サーバーを起動します。
nnmcluster -daemon

19 クラスタを有効にするには、アクティブ NNMi 管理サーバーで以下のコマンドを実行します。
nnmcluster -enable

20 進行状況を監視するには、アクティブとスタンバイの両方の NNMi 管理サーバーで以下のコマンドを実行します。
nnmcluster -display
アクティブ NNMi 管理サーバーが、スタンバイ NNMi 管理サーバーからデータベースの取得を完了するまで待機します。

21 アクティブ NNMi 管理サーバーに STANDBY_READY が表示されたら、アクティブ NNMi 管理サーバーで以下のコマンドを実行します。
nnmcluster -acquire

22 NNM iSPI Performance for QA、NNM iSPI Performance for Metrics、または NNM iSPI Performance for Traffic をインストールし、アプリケーション フェイルオーバー機能を使用しており、さらに上記のパッチ プロセスを完了した場合は、アクティブおよびスタンバイ NNMi 管理サーバーの各 NNM iSPI に NNM iSPI イネーブルメント スクリプトを実行します。

23 Linux NNMi 管理サーバーを使用している場合は、アクティブおよびスタンバイ NNMi 管理サーバーの両方で以下のコマンドを実行します。
chmod 777 /var/opt/OV/shared/perfSpi/datafiles/nnm_details.xml

アプリケーション フェイルオーバーおよび NNMi 管理サーバーの再起動

スタンバイ NNMi 管理サーバーは、いつでも再起動でき、再起動に関する特別な指示はありません。スタンバイとアクティブの両方の NNMi 管理サーバーを再起動する場合は、アクティブ NNMi 管理サーバーを先に再起動してください。

アクティブまたはスタンバイ NNMi 管理サーバーを再起動するには、以下の手順を実行します。

1. NNMi 管理サーバーで **nnmcluster -disable** コマンドを実行し、アプリケーション フェイルオーバー機能を無効にします。
2. NNMi 管理サーバーを再起動します。
   a. NNMi 管理サーバーで **ovstop** コマンドを実行します。
   b. NNMi 管理サーバーで **ovstart** コマンドを実行します。
3. NNMi 管理サーバーで **nnmcluster -enable** コマンドを実行し、アプリケーション フェイルオーバー機能を有効にします。

アプリケーション フェイルオーバーおよび以前のデータベースバックアップから復旧 (組み込みデータベースのみ)

アクティブおよびスタンバイ NNMi 管理サーバーがアプリケーション フェイルオーバー構成の場合に、元のバックアップから NNMi データベースを復旧するには、以下の手順を実行します。

1. アクティブ NNMi 管理サーバーで **nnmcluster -halt** コマンドを実行します。
2. アクティブおよびスタンバイ NNMi 管理サーバーの以下のディレクトリを削除または移動します。
   - *Windows*: `%NnmDataDir%¥shared¥nnm¥databases¥Postgres_standby`
   - *UNIX*: `$NnmDataDir/shared/nnm/databases/Postgres_standby`
3. アクティブ NNMi 管理サーバーでデータベースを復元します。
   a. 以下のファイルのクラスタ名をコメントアウトして変更します。
      — *Windows*: `%NnmDataDir%¥shared¥nnm¥conf¥props¥nms-cluster.properties`
      — *UNIX*: `$NnmDataDir/shared/nnm/conf/props¥nms-cluster.properties`
   b. 通常どおり、データベースを復旧します。352 ページの「NNMi データのリストア」を参照してください。
   c. アクティブ NNMi 管理サーバーで **ovstop** コマンドを実行します。
   d. 以下のファイルでクラスタ名をコメント解除して変更します。
      — *Windows*: `%NnmDataDir%¥shared¥nnm¥conf¥props¥nms-cluster.properties`
      — *UNIX*: `$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`
4. アクティブ NNMi 管理サーバーで **ovstart** コマンドを実行します。
5. アクティブ NNMi 管理サーバーが新しいバックアップを生成するまで待ちます。この手順が完了したことを確認するには、**nnmcluster -display** コマンドを実行し、`ACTIVE_NNM_RUNNING` メッセージを検索します。

6 スタンバイ NNMi 管理サーバーで **ovstart** コマンドを実行します。スタンバイ NNMi 管理サーバーは新しいバックアップをコピーして抽出します。この手順が完了したことを確認するには、**nnmcluster -display** コマンドを実行し、STANDBY_READY メッセージを検索します。

ネットワーク レイテンシ / 帯域に関する考慮

NNMi アプリケーション フェイルオーバーは、クラスタのノード間で継続的なハートビート信号を交換することによって機能します。これには、NNMi 組み込みデータベース、データベース トランザクション ログ、その他の NNMi 設定ファイルなどのデータファイルの交換に使用されるネットワーク チャネルが使用されます。HP は、WAN (広域ネットワーク) に NNMi アプリケーション フェイルオーバーを導入する場合、パフォーマンスが高く、レイテンシが低い接続を使用することをお勧めします。

NNMi 組み込みデータベースは必ず圧縮されていますが、非常に容量が大きくなり、1GB 以上に増大することがあります。また、NNMi は、ビルトインバックアップインターバル (設定パラメータ、デフォルトは 6 時間) の間に膨大な数のトランザクションログを生成します。各トランザクションログのサイズは数メガバイトから、最大 16MB になることもあります。(これらのファイルは圧縮されています)。以下は、HP のテスト環境から収集されたデータの例です。

```
Number of nodes managed: 15,000

Number of interfaces: 100,000

Time to complete spiral discovery of all expected nodes: 12 hours

Size of database: 850MB (compressed)

During initial discovery: ~10 transaction logs per minute (peak of ~15/
min)

-----------------------------

10 TxLogs/minute X 12 hours = 7200 TxLogs @ ~10MB = ~72GB
```

これでは、ネットワークで送信するにはデータ量が多すぎます。2 つのノード間のネットワークが NNMi アプリケーション フェイルオーバーの帯域幅の要求に応じられない場合、スタンバイ ノードへのデータベース ファイルの送信に遅延が発生してしまいます。このため、アクティブ サーバーに障害が発生した場合、潜在的なデータ喪失の可能性が高くなります。

同様に、2 つのノード間のネットワークのレイテンシが高いか信頼性が低い場合、ノード間で*偽*のハートビート喪失となります。たとえば、ハートビート信号が直ちに応答しない場合に、スタンバイ ノードは、アクティブ ノードに障害が発生したと判断します。ハートビート喪失の検出に関与する要素にはいくつかあります。NNMi は、ネットワークがアプリケーション フェイルオーバーのデータ転送の要求に応答できる限り、偽のフェイルオーバー通知を回避します。

マルチサブネット NNMi アプリケーションフェイルオーバーに関する HP の検証では、アクティブサーバーおよびスタンバイサーバーは、それぞれ米国のコロラド州とヒューストンにあり、許容できる帯域幅とレイテンシにより、偽のフェイルオーバーは発生しませんでした。

アプリケーション フェイルオーバーと NNMi 組み込みデータベース

アプリケーション フェイルオーバーは、NNMi 9.10 の組み込みデータベースと Oracle データベースの両方で動作します。ところが Oracle ではデータベースが NNMi 管理サーバーとは別のサーバーに存在します。Oracle データベースと連動するように NNMi を設定すると、データベースのレプリケーションは行われません。このため、Oracle データベースを使用すると、アプリケーション フェイルオーバーのネットワーク要求が減少します。Oracle でアプリケーション フェイルオーバーを使用しているとき、組み込みデータベースのアプリケーション フェイルオーバーを使用しているときと比較すると、ネットワークではネットワーク要求の 1% 未満しか使用されません。このセクションでは、組み込みデータベースを使用するアプリケーション フェイルオーバーに関連する NNMi トラフィック情報について説明します。

アプリケーション フェイルオーバーに組み込みデータベースを使用するように NNMi を設定すると、NNMi は以下のように動作します。

1 アクティブ ノードがデータベース バックアップを実行し、1 つの ZIP ファイルにデータを保存します。

2 NNMi は、ネットワークを通してこの ZIP ファイルをスタンバイ ノードに送信します。

3 スタンバイ ノードは ZIP ファイルを展開し、組み込みデータベースを設定して最初の起動でトランザクション ログをインポートします。

4 アクティブ ノードの組み込みデータベースは、データベース アクティビティにより、トランザクション ログを生成します。

5 アプリケーション フェイルオーバーでは、トランザクション ログがネットワークを通してスタンバイ ノードに送信され、ディスクに蓄積されます。

6 スタンバイ ノードがアクティブになると、NNMi が起動して、データベースがネットワークを通してすべてのトランザクション ログをインポートします。これにかかる時間は、ファイル数、およびそのファイルに保存されている情報の複雑さによって決まります (サイズが同程度でも、一部のファイルのインポートには別のファイルより時間がかかります)。

7 スタンバイ ノードがすべてのトランザクション ログをインポートすると、データベースが使用可能になり、スタンバイ ノードは残りの NNMi プロセスを開始します。

8 元のスタンバイ ノードがアクティブになり、手順 1 の手順がやり直しされます。

アプリケーション フェイルオーバー環境でのネットワーク トラフィック

アプリケーション フェイルオーバー環境では、NNMi はアクティブ ノードからスタンバイ ノードにネットワークを介して多くの項目を転送します。

- データベース アクティビティ : 1 つの ZIP ファイルとしてのデータベース バックアップ。
- トランザクション ログ。
- それぞれのアプリケーション フェイルオーバー ノードが、他方のノードが動作していることを確認するための定期的な*ハートビート*。
- ファイルがアクティブ ノードのものと同期していることをスタンバイ ノードが確認できるようにするファイル比較リスト。
- パラメータの変更 (フェイルオーバーやその他の有効/無効) およびクラスタでのノードの追加や除外などの、その他のイベント。

最初の 2 つの項目により、アプリケーション フェイルオーバーで使用されるネットワーク トラフィックの 99% が生成されます。このセクションでは、この 2 つの項目について詳しく説明します。

データベース アクティビティ : NNMi はすべてのデータベース アクティビティのトランザクション ログを生成します。データベース アクティビティには、NNMi のすべてが含まれます。このアクティビティには以下のデータベース アクティビティが含まれますが、その他にも含まれるものがあります。

- 新しいノードを検出する。
- ノード、インタフェース、VLAN、その他の管理対象オブジェクトに関する属性を検出する。
- 状態ポーリングとステータス変更。
- インシデント、イベント、根本原因分析。
- NNMi コンソールでのオペレータのアクション。

データベース アクティビティを制御することはできません。たとえば、ネットワークが停止すると、NNMi は多くのインシデントとイベントを生成します。このインシデントとイベントにより、ネットワーク上のデバイスの状態ポーリングが開始され、NNMi でデバイスのステータスが更新されます。停止が復旧されると、*ノード開始*インシデントによってステータスがさらに変化します。このすべてのアクティビティにより、データベースのエントリが更新されます。

組み込みデータベース自体はデータベース アクティビティによって拡大しますが、時間の経過とともに拡大は穏やかになり、環境でのサイズは安定します。

データベース トランザクション ログ: 組み込みデータベースは、空の 16 MB のファイルを作成してからデータベース トランザクション情報をそのファイルに書き込むことで動作します。NNMi は、15 分が経過した時点か、16 MB のデータがファイルに書き込まれた時点のいずれかの早い時点でこのファイルを閉じて、アプリケーション フェイルオーバーで使用可能にします。つまり、完全にアイドル状態のデータベースにより、15 分ごとに 1 つのトランザクション ログ ファイルが生成されますが、このファイルは本質的に*空*です。アプリケーション フェイルオーバーでは、すべてのトランザクション ログが圧縮され、空の 16 MB のファイルは 1 MB 未満に圧縮されます。*満杯の* 16 MB のファイルは約 8 MB に圧縮されます。データベース アクティビティが多い期間は、それぞれのファイルがすぐに満杯になるため、アプリケーション フェイルオーバーによって短時間により多くのトランザクション ログが生成されます。

アプリケーション フェイルオーバーのトラフィック テスト

以下のテストでは、1 分ごとにおよそ 2 個のトランザクション ログ ファイルが生成され、1 つのファイルの平均ファイル サイズは 7 MB になります。これは、それぞれのフェイルオーバー イベントで追加される 5000 個のノードの検出に関連するデータベース アクティビティによるものです。このテスト ケースのデータベースは、最終的に約 1.1 GB で安定し (バックアップ ZIP ファイルのサイズで測定)、ノードは 31,000 個、インタフェースは 960,000 個になります。

テスト モード : 最初の 4 時間でテスト担当者が 5,000 個のノードを NNMi にシードして、検出が安定するまで待機しました。4 時間後、テスト担当者がフェイルオーバーを誘発しました (スタンバイ ノードがアクティブになり、以前のアクティブ ノードがスタンバイになりました)。テスト担当者はフェイルオーバー直後に約 5,000 個のノードをさらに追加し、また 4 時間待機して NNMi の検出プロセスを安定させてから、別のフェイルオーバーを誘発しました (以前のアクティブ ノードに戻りました)。テスト担当者は、フェイルオーバー間の時間を、4 時間、6 時間、2 時間というよう変更して、このサイクルを数回繰り返しました。テスト担当者は、それぞれのフェイルオーバー イベント後に、以下の項目を測定します。

- ノードが初めてアクティブになったときに作成されるデータベース バックアップ ZIP ファイルのサイズ。
- トランザクション ログ : ファイル総数、およびディスク容量の使用量。
- フェイルオーバーを誘発する直前の NNMi データベースのノードとインタフェースの数。
- フェイルオーバーが完了するまでの時間。アクティブ ノードで `ovstop` コマンドを最初に実行してから、スタンバイ ノードが完全にアクティブになって NNMi が動作するまでの時間。

結果は表 22 のとおりです。

表 22　アプリケーション フェイルオーバーのテスト結果

時間	DB.zip サイズ (MB)	トランザクションログの数	の数 (GB)	ノード	インタフェース	フェイルオーバーの時間 (分)
4	6.5	50	.3	5,000	15,000	5
8	34	500	2.5	12,000	222,000	10
12	243	500	2.5	17,000	370,000	25
16	400	500	3.5	21,500	477,000	23
20	498	500	3.5	25,500	588,000	32
26	618	1100	7.5	30,600	776,000	30
28	840	400	2.2	30,600	791,000	31
30	887	500	2.5	30,700	800,000	16

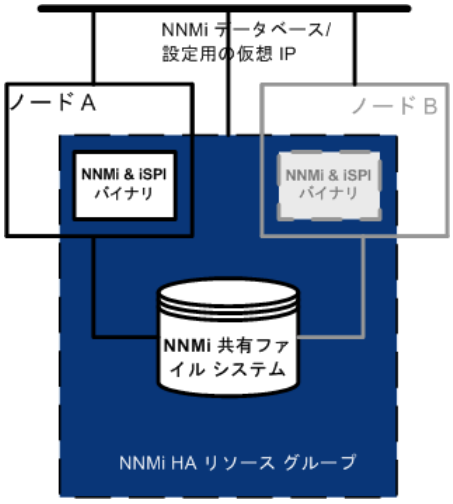
所見 : NNMi がアクティブノードからスタンバイノードにファイルを転送する場合、転送は 4 時間ごとに平均で約 5GB、連続スループットは約 350 KB/s (1 秒あたりのキロバイト数) または 2.8 MB/s (1 秒あたりのメガビット数) になっています。

- このデータには、ハートビート、ファイル整合性チェック、その他のアプリケーション フェイルオーバー通信など、その他のアプリケーション フェイルオーバー トラフィックは含まれていません。このデータでは、パケット ヘッダーなどのネットワーク I/O のオーバーヘッドも除外されています。このデータには、ネットワークで移動する各ファイルの内容の実ネットワーク ペイロードのみが含まれます。
- NNMi のアプリケーション フェイルオーバー環境で生成されるトラフィックは非常に爆発的です。アプリケーション フェイルオーバーでは、5 分ごとにアクティブ ノードで新しいトランザクション ログが識別され、スタンバイ ノードに送信されます。ネットワークの速度により、スタンバイ ノードではすべての新しいファイルが短時間で受信され、この 5 分間隔の残りの間、ネットワークは比較的にアイドル状態となることが多くなります。

アクティブ ノードとスタンバイ ノードがロールを切り替えるたびに (スタンバイ ノードがアクティブになり、アクティブ ノードがスタンバイになる)、新しいアクティブ ノードは完全なデータベース バックアップを生成し、ネットワークを介して新しいスタンバイ ノードに送信します。このデータベース バックアップも定期的に発生し、デフォルトで 24 時間ごとにバックアップされます。NNMi は、新しいバックアップを生成するたびに、このバックアップをスタンバイ ノードに送信します。この新しいバックアップがスタンバイ ノードで使用可能になると、その 24 時間に NNMi が生成したすべてのトランザクション ログがデータベースに反映されて、フェイルオーバー時にインポートする必要がなくなるため、フェイルオーバー時間が短縮されます。

前述の情報により、組み込みデータベースを使用してアプリケーション フェイルオーバーで NNMi を使用するとき、フェイルオーバー後にネットワークがどのようなパフォーマンスになるかを理解できます。

高可用性クラスタに NNMi を設定する



高可用性 (HA) とは、構成された動作中のハードウェアおよびソフトウェアの一部に障害が発生しても中断されないサービスを提供するシステムです。HA クラスタは、フェイルオーバー発生時の機能とデータの継続性を保証するために、協調して動作するハードウェアとソフトウェアのグループ化を定義します。

NNMi では、別途購入が必要な HA 製品を使って構成される HA クラスタ内で NNMi を実行する設定をサポートするようになりました。ほとんどの NNM Smart Plug-ins (iSPI) も、NNM iSPI NET 診断サーバーを除いて、HA で実行できるようになります。

この章では、HA 環境で実行するように NNMi を設定するためのテンプレートについて説明します。この章では、HA 製品の詳細な設定手順については説明しません。NNMi に用意されている HA 設定コマンドは、サポートされる HA 製品用のコマンドに関するラッパーとなります。HA 製品固有のコマンドの代わりに、以下の手順で説明している NNMi のコマンドを使用できます。

NNMi 管理サーバーにいずれかの NNM iSPI をインストールする場合は、その NNM iSPI のマニュアルも参照してください。

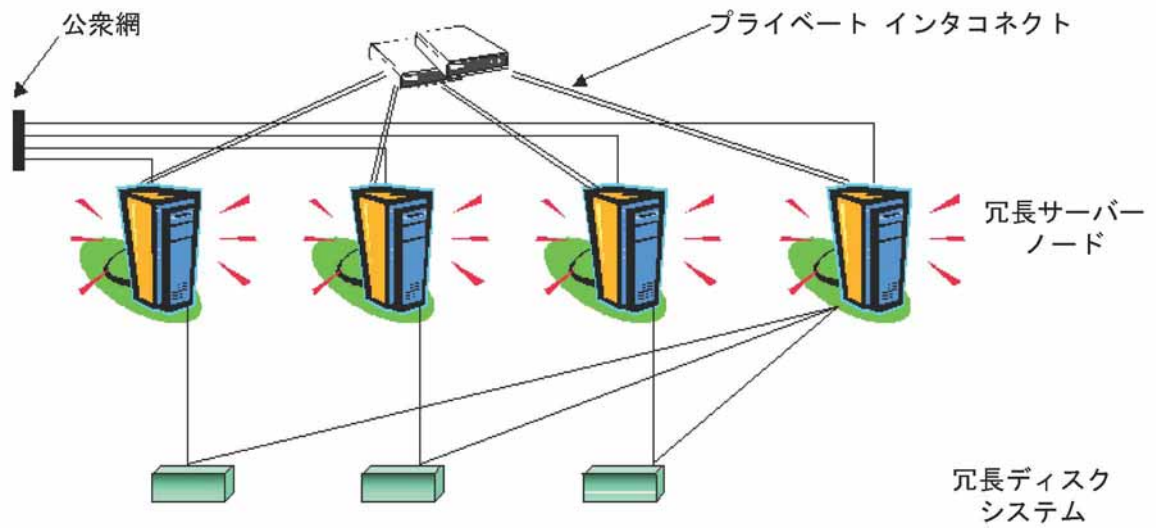
この章には、以下のトピックがあります。

- 298 ページの「HA の概念」
- 303 ページの「HA 用 NNMi を設定するための前提条件の検証」
- 305 ページの「HA の設定」
- 314 ページの「共有 NNMi データ」
- 317 ページの「HA クラスタ内の NNMi のライセンス契約」
- 318 ページの「HA 設定のメンテナンス」
- 322 ページの「HA クラスタ内の NNMi の設定を解除する」
- 326 ページの「HA 下の NNMi のパッチ」
- 327 ページの「HA 下の NNMi を NNMi 9.0x から NNMi 9.10 にアップグレードする」
- 331 ページの「HA 設定のトラブルシューティング」
- 341 ページの「HA 設定リファレンス」

HA の概念

クラスタ アーキテクチャには、クラスタ内の複数のノードのプロセスとリソース用の、単一のグローバルに首尾一貫した管理ビューが備わっています。図 20 に、クラスタ アーキテクチャの例を示します。

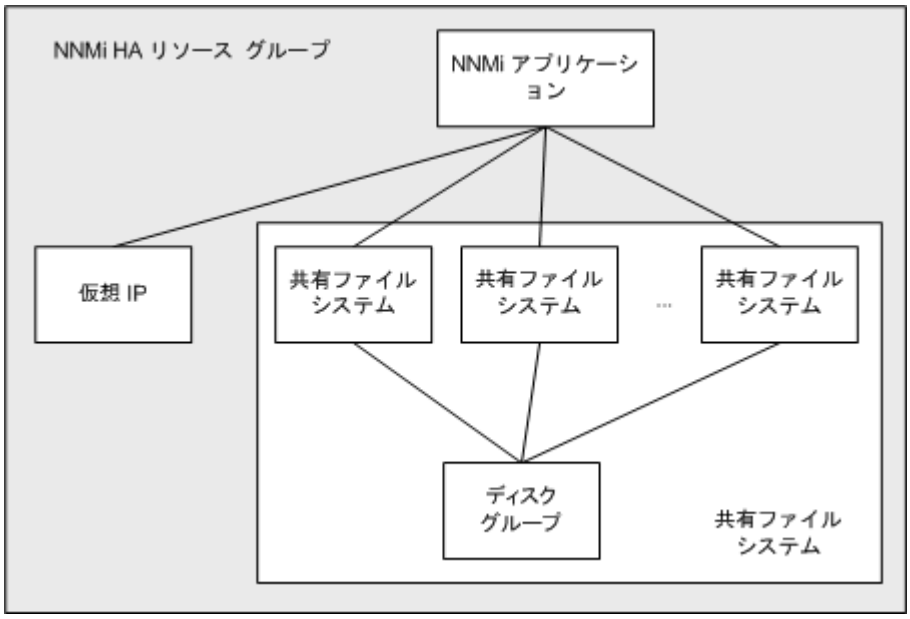
図 20　　高可用性クラスタのアーキテクチャ



クラスタ内の各ノードは、1 つ以上の公衆網と 1 つのプライベート インタコネクト (クラスタ ノード間のデータ伝送用の通信チャネル) に接続されます。

HP Serviceguard、Veritas Cluster Server、Microsoft フェールオーバー クラスタリング、Microsoft クラスタ サービスなどの最新のクラスタ環境では、アプリケーションはリソースの複合体として表現され、単純な操作でアプリケーションをクラスタ環境で実行することができます。リソースは、クラスタ環境で動作するアプリケーションを表す、**HA リソース グループ**に構成されます。図 21 に、HA リソース グループの例を示します。

図 21　典型的な HA リソース グループのレイアウト



このマニュアルでは、各種のクラスタ環境内のリソースの集合を指すために、*HA リソース グループ*という用語を使います。各 HA 製品では、HA リソース グループに対して、異なる名前が使われています。表 23 に、このマニュアルの *HA リソース グループ*に相当する、サポート対象の HA 製品で使われている用語をリストします (各 HA 製品のサポート対象バージョンについては、*NNMi システムおよびデバイスのサポート マトリックス*を参照してください)。

表 23　サポート対象の HA 製品で HA リソース グループに相当する名前

HA 製品	略語	HA リソース グループに相当する名前
Microsoft フェールオーバー クラスタリング	MSFC	リソース グループ
HP Serviceguard	SG	パッケージ
Veritas Cluster Server	VCS	サービス グループ
Red Hat Cluster Suite	RHCS	サービス

HA 用語集

表 24 に、一般的な HA 用語の定義を示します。

表 24　一般的な HA 用語

用語	説明
HA リソース グループ	クラスタ環境内で (HA 製品下で) 動作するアプリケーションです。HA リソース グループは、同時に、クラスタ内のアプリケーションを表すクラスタ オブジェクトでもあります。
ボリューム グループ	1 つの大規模ストレージ エリアを形成するよう設定された 1 つ以上のディスク ドライブです。
論理ボリューム	ボリューム グループ内で、個別のファイル システムまたはデバイス スワップ空間として使われる任意のサイズの領域です。

表 24　一般的な HA 用語 (続く)

用語	説明
プライマリ クラスタ ノード	ソフトウェア製品が最初にインストールされるシステムであり、かつ、HA が最初に設定されるシステムです。 初期セットアップでは、共有ディスクはプライマリ クラスタ ノードにマウントされます。 プライマリ クラスタ ノードは、通常、最初のアクティブなクラスタ ノードになりますが、HA の設定完了後には、プライマリとしての役割を解除できます。HA 設定を変更すると、他のノードをプライマリ クラスタ ノードにできます。
セカンダリ クラスタ ノード	プライマリ クラスタ ノードでの HA 設定の完了後に、HA 設定に追加される任意のシステムです。
アクティブなクラスタ ノード	現在 HA リソース グループを実行中のシステムです。
パッシブなクラスタ ノード	HA 用に設定されているが、現在 HA リソース グループを実行していないシステムです。アクティブなクラスタ ノードで障害が発生すると、HA リソース グループはパッシブなクラスタ ノードの中で利用可能なノードにフェイルオーバーし、そのノードがアクティブなクラスタ ノードになります。

NNMi HA クラスタのシナリオ

NNMi HA 設定では、NNMi は各システムにインストールされ、HA リソース グループの一部になります。NNMi データベースは独立したディスクにインストールされ、各システムで動作中の NNMi プログラムからアクセスされます。(任意の時点で共有ディスクにアクセスできるのは、アクティブなクラスタ ノードである 1 つのシステムだけです。)

このアプローチは、組み込み型のデータベースと他社製データベース ソリューションの場合に有効です。

NNMi データベースのバックアップ スクリプトとリストア スクリプトを実行できるのは、アクティブなクラスタ ノードだけです。

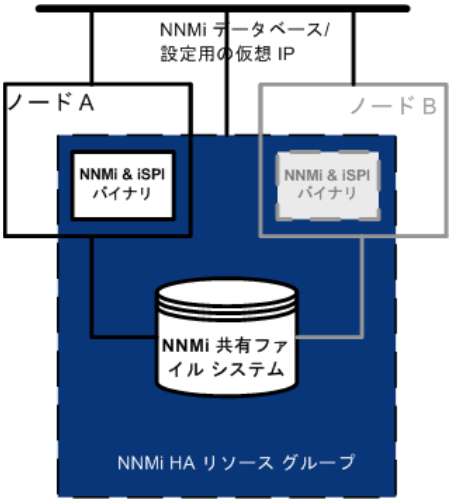
NNMi のみのシナリオ

図 22 に、NNMi HA クラスタのシナリオを図示します。この図では、NNMi HA リソース グループは、NNMi HA クラスタと同義語です。

ノード A とノード B はどちらも、すべてのソフトウェアがインストールされた NNMi 管理サーバーであり、そのシステムで実行する NNMi プログラムと NNM iSPI がすべて含まれています。アクティブなクラスタ ノードが、共有ディスクのランタイム データにアクセスします。他の製品は、HA リソース グループの仮想 IP アドレスを使って NNMi に接続します。

クラスタに 3 つ以上の NNMi ノードがある場合は、追加ノードには図 22 のノード B と同様の設定を行います。

図 22　NNMi HA クラスタ用の基本的なシナリオ

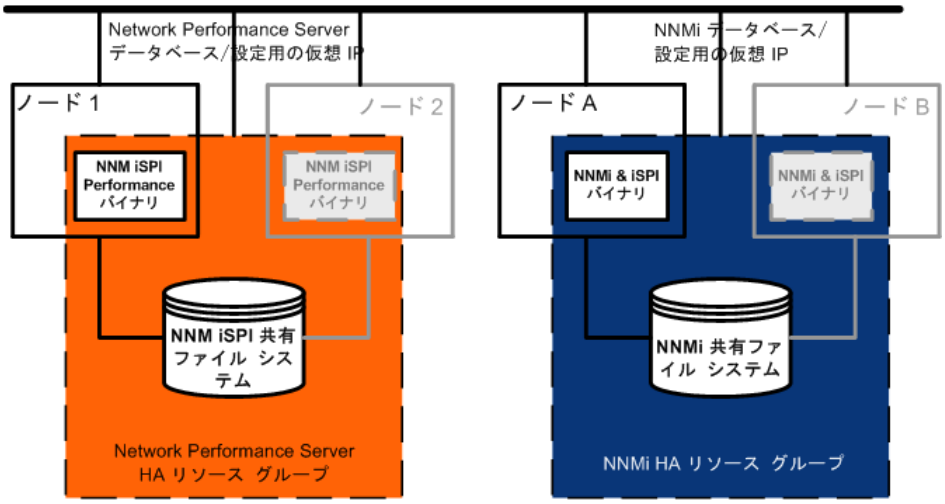


このシナリオの実装方法については、305 ページの「HA 用の NNMi の設定」と 311 ページの「HA 用の NNM iSPI の設定」を参照してください。

スタンドアロン サーバー シナリオでの NNMi および NNM Performance iSPI

いずれかの NNM Performance iSPI 製品をスタンドアロン サーバーで実行する場合は、図 23 に示すように、NNMi HA クラスタ内で別個の HA リソース グループとして実行されるようこの NNM iSPI を設定できます。NNMi HA リソース グループは、NNMi のみのシナリオで説明したものと同じです。

図 23　スタンドアロン サーバーで NNMi と NNM Performance iSPI を実行する場合の HA



このシナリオの実装方法については、305 ページの「HA 用の NNMi の設定」と 311 ページの「HA 用の NNM iSPI の設定」を参照してください。

スタンドアロン サーバーで実行される NNM Performance iSPI のその他の選択肢は以下のとおりです。

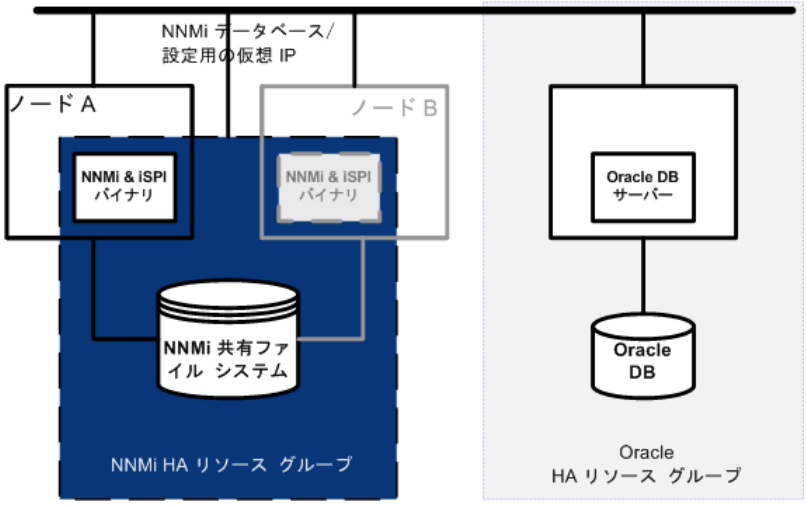
- NNM Performance iSPI を HA を設定していない単一システムで実行します。このアプローチは、NNM iSPI を評価する場合、あるいは、パフォーマンス データが必ずしも必要ではない環境で使用します。
- NNM Performance iSPI を NNMi 用とは異なる HA クラスタ下で実行するように設定します。この場合は、NNM Performance iSPI の NNMi への依存関係を手動で管理する必要があります。

NNMi で Oracle データベースを使う場合のシナリオ

NNMi 実装で Oracle をメイン NNMi データベースとして使う場合は、Oracle データベースは、パフォーマンス上の理由で、図 24 のように、独立したサーバーにインストールする必要があります。そのため、NNMi HA クラスタでは、次の 2 つの HA リソース グループを設定する必要があります。

- NNMi HA リソース グループは、NNMi ノードと、Oracle データベースに格納されない NNMi データ用の共有ディスクで構成します。
- Oracle HA リソース グループは、Oracle データベース サーバーとデータベース ディスクで構成します。

図 24　Oracle データベースを使っている NNMi 用の HA

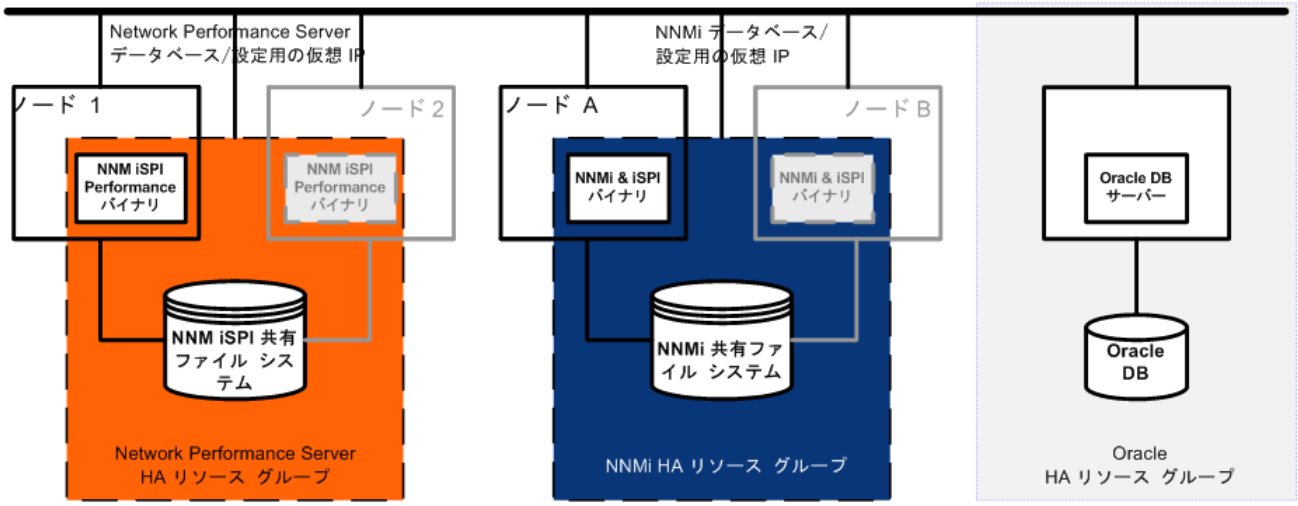


このシナリオの実装方法については、312 ページの「Oracle 環境での HA 用の NNMi の設定」と 311 ページの「HA 用の NNM iSPI の設定」を参照してください。

NNMi で Oracle データベースを使用し、NNM Performance iSPI をスタンドアロン サーバーで実行する場合のシナリオ

NNMi 実装で Oracle をメイン NNMi データベースとして使用し、いずれかの NNM Performance iSPI 製品をスタンドアロン サーバーで実行する場合は、図 25 に示すように、NNMi HA クラスタ内に 3 つの HA リソース グループを設定できます。

図 25　NNMi で Oracle データベースを使用し、NNM Performance iSPI をスタンドアロン サーバーで実行する場合の HA



このシナリオの実装方法については、312 ページの「Oracle 環境での HA 用の NNMi の設定」と 311 ページの「HA 用の NNM iSPI の設定」を参照してください。

マンページ

NNMi マンページには、HA 設定について、以下の内容が含まれています。

- nnm-ha
- nnmhaconfigure.ovpl
- nnmhaunconfigure.ovpl
- nnmhadisk.ovpl
- nnmhaclusterinfo.ovpl
- nnmhastartrg.ovpl
- nnmhastoprg.ovpl

Windows オペレーティング システムでは、これらのマンページはテキスト ファイルで提供されます。

HA 用 NNMi を設定するための前提条件の検証

HA 用 NNMi を正常に設定できるかどうかは、以下のいくつかの要因に依存します。

- 適切なハードウェア
- HA 製品についての理解
- 系統的な設定方法

HA 用 NNMi の設定を開始する前に、以下の準備手順を実行してください。

1. *NNMi システムおよびデバイスのサポート マトリックス*の情報を調べて、使用する HA 製品が NNMi でサポートされているかを確認します。
2. HA 製品のマニュアルを読み、その製品の機能に精通してから設計上の決定を行います。

   HA 製品のマニュアルは頻繁に変更されます。必ず最新版のマニュアルを入手してください。

3. NNMi HA クラスタのノードとして含める各システム (または仮想マシン イメージ) が以下の要件を満たすことを確認します。
   - HA 製品のマニュアルに記載されているすべての要件に適合する。
   - 少なくとも 2 つのネットワーク インタフェース カード (NIC カード) が組み込まれている。

     HA 製品、オペレーティング システム、および NIC カードのマニュアルで調べて、これらの製品を一緒に使用できるかどうか確認してください。

   - HA リソースグループの仮想 IP アドレスの使用をサポートする。この IP アドレスは、NNMi ライセンスで使用される IP アドレスです。

     MSFC では複数の仮想 IP アドレスが必要であり、1 つは HA クラスタ用で、もう 1 つは各 HA リソースグループ用です。この場合、NNMi HA リソース グループの仮想 IP アドレスは、NNMi ライセンスで使用される IP アドレスです。

- 共有ディスクまたはディスク アレイの使用をサポートする

HA 製品、オペレーティング システム、およびディスク製造業者のマニュアルで調べて、関連する SCSI カードを含め、これらの製品を一緒に使用できるかどうか確認してください。

- 「*NNMi システムおよびデバイスのサポート マトリックス*」で説明される、NNMi のすべての要件に適合する。

4 NNMi HA クラスタでいずれかの NNM iSPI を実行する場合は、HA 設定の追加の前提条件について、該当する NNM iSPI のマニュアルをお読みください。

5 以下の仮想 IP アドレスとホスト名を割り当てます。

- HA クラスタに 1 つの仮想 IP アドレス (MSFC のみ)
- 設定する各 HA リソース グループに 1 つの仮想 IP アドレス

6 任意のシステムから、`nslookup` コマンドを使用して、手順 5 で割り当てたすべての IP アドレスとホスト名に対して DNS が正しく応答することを確認します。

7 各システムのオペレーティング システムが、HA 製品と NNMi に適切なバージョンとパッチ レベルになっていることを確認します。

8 必要な場合は、HA 製品をインストールします。

Solaris ゾーン環境の場合、HA 製品をグローバルゾーンにインストールします。

9 315 ページの「共有ディスクの手動準備」に従って、共有ディスクを準備します。

10 HA 製品用のコマンドを使用して、HA クラスタを設定 (必要な場合) およびテストします。

HA クラスタには、アプリケーション ハートビートのチェックやフェイルオーバー起動などの機能が用意されています。HA クラスタ設定には、少なくとも、以下の項目を含める必要があります。

- (UNIX のみ) ssh、remsh、または両方
- (Windows のみ) DNS で解決可能な、HA クラスタ用の仮想 IP アドレス
- DNS で解決可能な、HA クラスタ用の仮想ホスト名
- NNMi 固有の一意のリソース グループ。

NNMi では、必要なすべてのリソースが NNMi HA リソース グループに含まれているが期待されます。不足がある場合は、HA 製品の機能を使用して、NNMi HA リソース グループとその他の HA リソース グループの間の依存関係を管理してください。たとえば、Oracle が別個の HA リソース グループ内で実行されている場合は、HA 製品が NNMi HA リソース グループを起動する前に Oracle HA リソース グループが完全に起動されるように HA 製品を設定します。

- *MSFC*: Failover Cluster Management for Windows Server 2008 のクラスタ作成ウィザードを使用します。
- *ServiceGuard* の場合 :
  - ノードの .rhosts エントリまたは .ssh エントリを追加します。
  - HA 製品 (cmgetconf、cmcheckconf、cmapplyconf) を設定します。クラスタの設定の詳細については、HA 製品の最新のマニュアルを参照してください。
- *VCS*: 不要。製品のインストールにより HA クラスタが作成されました。

- *RHCS*: RHCS のマニュアルの説明に従って、サービス (cman、rgmanager) を追加します。

NNMi HA リソースグループに入れるリソースのテストの詳細については、332 ページの「HA リソース テスト」を参照してください。

HA の設定

このセクションでは、NNMi 用の 新規 HA 設定の設定手順を説明します。内容は以下のとおりです。

- 305 ページの「HA 用の NNMi 証明書の設定」
- 305 ページの「HA 用の NNMi の設定」
- 311 ページの「HA 用の NNM iSPI の設定」
- 312 ページの「Oracle 環境での HA 用の NNMi の設定」

Solaris ゾーン環境で NNMi を実行している場合は、この章で説明されている設定プロセスに従う必要はありません。262 ページの「Solaris ゾーン環境の HA での NNMi の実行」を参照してください。

RHCS の設定では、HA クラスタの各ノード上で、HA クラスタデーモンとすべてのアプリケーションを完全に再起動する必要があります。これを考慮して、設定作業を計画してください。

HA 用の NNMi 証明書の設定

NNMi のインストール プロセスでは、NNMi コンソールと NNMi データベースの間でセキュア通信が行われるよう、自己署名証明書を設定します。NNMi HA を正しく設定するプロセスでは、プライマリ ノードとセカンダリ ノードの間で自己署名証明書を共有します。HA 下で実行される NNMi でデフォルトの証明書を使用するために、追加の手順を実行する必要はありません。

NNMi の通信で別の自己署名証明書または認証機関 (CA) 署名の証明書を使用する場合は、追加の手順を実行する必要があります。新しい証明書を入手してから、128 ページの「新規証明書を使用するように高可用性を設定する」に従って手順を実行します。この手順は、HA 用 NNMi を設定する前または後に実行できます。

HA 用の NNMi の設定

HA 用に NNMi を設定する場合の主な作業は、次の 2 つです。

1. NNMi データ ファイルを共有ディスクにコピーします。
   - 308 ページの「プライマリ クラスタ ノードでの NNMi の設定」の手順 1 ～手順 9 に従って、プライマリ ノードでこの作業を行います。
2. HA 下で NNMi を実行するように、設定します。
   - 308 ページの「プライマリ クラスタ ノードでの NNMi の設定」の手順 10 ～手順 15 に従って、プライマリ ノードでこの作業を行います。
   - また、310 ページの「セカンダリ クラスタ ノードでの NNMi の設定」の説明に従って、セカンダリ ノードでもこの作業を行います。

1 つの HA クラスタ ノードを、プライマリ NNMi 管理サーバーとして割り当てます。これが大部分の時間にアクティブとなるノードです。プライマリ ノードを設定します。次に HA クラスタ内の残りのすべてのノードをセカンダリ ノードとして設定します。

HA 用の NNMi の設定は、複数のクラスタ ノードで同時には*行えません*。1 つのクラスタ ノードで HA 設定プロセスが完了した後、次のクラスタ ノードでの HA 設定プロセスを開始するというように、クラスタ環境内のすべてのノードで HA 用に NNMi を設定するまで、この作業を繰り返します。

フェイルオーバー中には NNMi コンソールは応答しません。フェイルオーバーが完了してから、NNMi ユーザーは、ログオンして NNMi コンソールのセッションを続行する必要があります。

NNMiHA 設定情報

HA 設定スクリプトは、NNMi HA リソース グループに関する情報を収集します。表 25 に、プライマリ ノードの設定で必要になる情報を示します。設定作業を開始する前に、これらの情報を用意してください。

表 25　NNMi HA プライマリ ノードの設定情報

HA 設定項目	説明
HA リソース グループ	NNMi を含む HA クラスタのリソース グループの名前です。この名前は NNMi に対して一意であり、現在使用されていない名前にする必要があります。 例 : nnmtest1
仮想ホストの短い名前	仮想ホストの短い名前です。このホスト名は、HA リソース グループの仮想 IP アドレスにマッピングする必要があります。`nslookup` コマンドで、仮想ホストの短い名前と仮想 IP アドレスを解決できる必要があります。 **注 :** NNMi が仮想ホストの短い名前と仮想 IP アドレスを解決できない場合は、HA 設定スクリプトのためにシステムが不安定な状態になる可能性があります。したがって、NNMi HA の設定中に DNS が利用できない場合に備えて、予備のネーミング ストラテジ (たとえば、Windows オペレーティング システムの場合は、`%SystemRoot%¥system32¥drivers¥etc¥hosts` ファイルに、UNIX オペレーティング システムの場合は、`/etc/hosts` ファイルに、それぞれ情報を記述する) を用意しておくことをお勧めします。
仮想ホストのネットマスク	仮想ホスト IP アドレスで使われるサブネット マスクです。これは、IPv4 アドレスであることが必要です。
仮想ホストのネットワーク インタフェース	仮想ホスト IP アドレスが使われるネットワーク インタフェースです。たとえば、以下のようにします。 • *Windows* の場合 : ローカル エリア接続 • *HP-UX* の場合 : lan0 • *Linux* の場合 : eth0 • *Solaris* の場合 : bge0

表 25　NNMi HA プライマリ ノードの設定情報

HA 設定項目	説明
共有ファイル システムのタイプ	HA リソース グループで使われる共有ディスクの設定タイプです。使用できる値は次のとおりです。 • disk: 共有ディスクは、標準のファイル システム タイプを使う、物理的に接続されたディスクです。HA 設定スクリプトは、共有ディスクを設定できます。詳細については、この表のファイル システム タイプの欄を参照してください。 • none: 共有ディスクには、disk オプションで説明している設定以外の SAN や NFS 構成などを使います。HA 設定スクリプトを実行すると、315 ページの「共有ディスクの手動準備」のように、共有ディスクが設定されます。
ファイル システム タイプ	(UNIX のみ) 共有ディスクのファイル システム タイプです (共有ファイル システムのタイプが disk の場合)。HA 設定スクリプトは、ディスクの検証方法を調べるために、この値を HA 製品に渡します。 以下の共有ディスク フォーマットはテスト済みです。 • *Windows* の場合 : 基本型 (317 ページの「Windows Server での共有ディスク設定についての注記」を参照); SAN • *HP-UX* の場合 : vxfs • *Linux* の場合 : VCS および RHCS には ext2、ext3、および vxfs • *Solaris* の場合 : vxfs 注 : HA 製品は他のファイル システム タイプをサポートしています。テストされていない共有ディスク フォーマットを使用する場合は、HA 下で実行するよう NNMi を設定する前にディスクを準備し、次に NNMi HA 設定スクリプトを実行する間に共有ファイル システム タイプとして none と指定します。
ディスク グループ	(UNIX のみ) NNMi 共有ファイル システムのディスク グループの名前です。この名前は、HA リソース グループの名前をベースにします。 例 : nnmtest1-dg
ボリューム グループ	(UNIX のみ) NNMi 共有ファイル システムのボリューム グループの名前です。この名前は、HA リソース グループの名前をベースにします。 例 : nnmtest1-vol
マウント ポイント	NNMi の共有ディスクをマウントするディレクトリの場所です。このマウント ポイントは、すべてのシステムで同じである必要があります。(つまり、各ノードでは、マウント ポイントに同じ名前を使う必要があります。) たとえば、以下のようにします。 • *Windows*: S:¥ 注 : ドライブ名は完全に指定してください。S および S: は受け入れられないフォーマットであり、共有ディスクにアクセスできません。 • *UNIX*: /nnmmount

プライマリ クラスタ ノードでの NNMi の設定

プライマリ クラスタ ノードで以下の手順を実行します。

メインの NNMi データベースとして Oracle を使用する場合は、まず 312 ページの「Oracle 環境での HA 用の NNMi の設定」を参照してください。

Solaris ゾーン環境で NNMi を実行している場合は、この章で説明されている設定プロセスに従う必要はありません。262 ページの「Solaris ゾーン環境の HA での NNMi の実行」を参照してください。

1. 303 ページの「HA 用 NNMi を設定するための前提条件の検証」の作業を完了していない場合は、完了させます。
2. NNMi がインストールされていない場合は、NNMi を (最新の統合パッチも含めて) インストールしてから、正しく動作することを確認します。
3. この NNMi 管理サーバー上でいずれかの NNM iSPI を実行する場合は、この手順を進める前に 311 ページの「HA 用の NNM iSPI の設定」を参照してください。
4. `nnmbackup.ovpl` コマンド、または別のデータベースコマンドを使用して、NNMi データをすべてバックアップします。たとえば、以下のようにします。

   ```
   nnmbackup.ovpl -type offline -scope all -target nnmi_backups
   ```

   このコマンドの詳細については、347 ページの「NNMi のバックアップおよびリストア ツール」を参照してください。
5. NNMi HA リソース グループ用に、少なくとも 1 つの共有ディスクを含む、ディスク デバイス グループ (および論理ボリューム) を定義します。たとえば、以下のようにします。
   - *MSFC* の場合 : ディスクの管理を使用して、ディスクのマウントポイントを設定し、ディスクをフォーマットします。
   - *Serviceguard* の場合 :

     `pvcreate`、`vgcreate`、および `lvcreate` などの LVM コマンドを使ってディスクの初期化、ボリューム グループの作成、および論理ボリュームの作成を行います。
   - *VCS* の場合 :

     `vxdiskadm`、`vxassist`、および `mkfs` などの VSF コマンドを使用して、ディスクを追加および初期化し、領域ごとにディスクを割り当て、論理ボリュームを作成します。
   - *RHCS* の場合 :

     `pvcreate`、`vgcreate`、および `lvcreate` などの LVM コマンドを使ってディスクの初期化、ボリューム グループの作成、および論理ボリュームの作成を行います。

   UNIX オペレーティング システムの参考 Web サイトは、次のとおりです。
   http://www.unixguide.net/unixguide.shtml

6 ディレクトリのマウントポイント (たとえば、S:¥ または /nnmmount) を作成し、共有ディスクをマウントします。

設定後、HA 製品はディスクのマウントを管理します。このマウントポイントを使用して、ファイルシステムテーブルを更新しないでください。

- *Windows* の場合 : Windows Explorer とディスクの管理を使います。
- *UNIX*:
  - mkdir コマンドおよび mount コマンドを使用します。
  - 共有ディスクのマウントポイントが、ユーザーは root、グループは sys で作成され、パーミッションには 555 が設定されていることを確認します。たとえば、以下のようにします。

    ```
    ls -l /nnmmount
    ```

7 NNMi を停止します。

```
ovstop -c
```

この HA リソース グループに含めるノードに NNMi がすでにインストールされている場合は、このとき、そのノードで ovstop -c も実行します。

8 NNMi データベースを共有ディスクにコピーします。

- *Windows*:

```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhadisk.ovpl NNM ¥
-to <HA_mount_point>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM ¥
-to <HA_mount_point>
```

データベースの破壊を避けるために、この (-to オプションを指定した) コマンドは一回しか実行できません。代替方法については、336 ページの「すべてのクラスタノードを設定解除した後の HA 用 NNMi の再有効化」を参照してください。

9 (UNIX のみ) 共有ディスクをマウント解除し、ディスクグループを非アクティブ化します。

```
umount <HA_mount_point>
vgchange -a n <disk_group>
```

10 NNMi が実行中でないことを確認します。

```
ovstop -c
```

11 (RHCS のみ) NNMi カスタムスクリプトを所定の場所にコピーし、HA クラスタデーモンを再起動します。

a /opt/OV/misc/nnm/ha/NNMscript.sh ファイルを、以下の場所にコピーします。

```
/usr/share/cluster/NNMscript.sh
```

b /sbin/ccsd プロセスを停止して、再起動します。

12 NNMi HA リソース グループを設定します。

- *Windows*:

  %NnmInstallDir%¥misc¥nnm¥ha¥nnmhaconfigure.ovpl NNM

- *UNIX*:

  $NnmInstallDir/misc/nnm/ha/nnmhaconfigure.ovpl NNM

306 ページの表 25 に、このコマンドで必要な情報を示します。

13 (UNIX の場合のみ) NNMi は、デフォルトで、nnmhaconfigure.ovpl コマンドを実行したユーザーのロケールで起動します。NNMi のロケールを変更するには、以下のコマンドを実行します。

$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl ¥
-config NNM -set HA_LOCALE <*locale*>

14 手順 12 で共有ファイル システム タイプとして指定した値に応じて、手順が異なります (306 ページの表 25 の共有ファイル システムのタイプとファイル システム タイプ)。

- タイプ disk を指定した場合は、nnmhaconfigure.ovpl コマンドによって、共有ディスクが設定されています。手順 15 を継続します。
- タイプ none を指定した場合は、315 ページの「共有ディスクの手動準備」の説明に従って共有ディスクを準備し、手順 15 に進みます。

15 NNMi HA リソース グループを起動します。

- *Windows*:

  %NnmInstallDir%¥misc¥nnm¥ha¥nnmhastartrg.ovpl NNM ¥
  <*resource_group*>

- *UNIX*:

  $NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM ¥
  <*resource_group*>

NNMi を正常に起動できなかった場合は、331 ページの「HA 設定のトラブルシューティング」を参照してください。

これで、NNMi が HA 下で動作するようになりました。通常のオペレーションでは、ovstart コマンドや ovstop コマンドは*使わない*でください。これらのコマンドを使うのは、HA のメンテナンスが目的で、使うことが指示された場合だけです。

セカンダリ クラスタ ノードでの NNMi の設定

セカンダリ クラスタ ノードでは 1 つのノードごとに順番に以下の手順を実行します。

1 308 ページの「プライマリ クラスタ ノードでの NNMi の設定」の作業を完了していない場合は、完了させます。

2 303 ページの「HA 用 NNMi を設定するための前提条件の検証」の作業を完了していない場合は、完了させます。

3 NNMi がインストールされていない場合は、NNMi を (最新の統合パッチも含めて) インストールしてから、正しく動作することを確認します。

4 308 ページの「プライマリ クラスタ ノードでの NNMi の設定」の手順 3 でインストールした NNM iSPI をインストールします。

5 NNMi を停止します。

ovstop -c

6 共有ディスクのマウント ポイントを作成します (たとえば、S:¥ または /nnmmount)。

このマウント ポイントでは、手順プライマリ クラスタ ノードでの NNMi の設定の手順 6 で作成したマウント ポイントと同じ名前を使う必要があります。

7 (RHCS のみ) NNMi カスタムスクリプトを所定の場所にコピーし、HA クラスタデーモンを再起動します。

a /opt/OV/misc/nnm/ha/NNMscript.shファイルを、以下の場所にコピーします。

/usr/share/cluster/NNMscript.sh

b /sbin/ccsd プロセスを停止して、再起動します。

8 NNMi HA リソース グループを設定します。

- *Windows*: **%NnmInstallDir%¥misc¥nnm¥ha¥nnmhaconfigure.ovpl NNM**
- *UNIX*: **$NnmInstallDir/misc/nnm/ha/nnmhaconfigure.ovpl NNM**

コマンドの要求に応じて、HA リソース グループ名を指定します。

9 設定が正常に行われたことを確認します。

- *Windows*:

```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhaclusterinfo.ovpl ¥
-group <resource_group> -nodes
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl ¥
-group <resource_group> -nodes
```

このコマンドの出力には、指定した HA リソース グループ用に設定されたノードがすべてリストされます。

10 必要に応じて、プライマリ ノードの NNMi HA リソース グループをオフラインにし、セカンダリ ノードの NNMi HA リソース グループをオンラインにすることで、設定をテストします。

HA 用の NNM iSPI の設定

NNMi 管理サーバー上でいずれかの NNM iSPI を実行する場合は、NNMi を HA 下で実行する設定を行う前に、このセクションをお読みください。

NNM iSPI Performance for Metrics、NNM iSPI Performance for QA、および NNM iSPI Performance for Traffic

NNM Performance iSPI (NNM iSPI Performance for Metrics、NNM iSPI Performance for QA、および NNM iSPI Performance for Traffic) は、NNMi 管理サーバーかスタンドアロン サーバーにインストールできますが、この 2 つのオプションを組み合わせることはできません。

- NNM Performance iSPI を NNMi 管理サーバー上に配置する場合は、HA 下で実行するように NNMi を設定する前に、この製品をインストールします。
- NNM Performance iSPI 製品をスタンドアロン サーバー上に配置する場合は、製品をインストールする前に、HA 下で実行するよう NNMi を設定します。NNM iSPI のインストール プロセス中に、NNMi HA リソース グループ仮想ホスト名を NNMi 管理サーバー名として指定します。

NNM iSPI for MPLS、NNM iSPI for IP Multicast、および NNM iSPI for IP Telephony

NNM iSPI for MPLS、NNM iSPI for IP Multicast、および NNM iSPI for IP Telephony は、NNMi 管理サーバーにのみインストールできます。HA 下で NNMi を実行するよう設定する前に、これらの製品をインストールします。

HA 下で実行するように NNM iSPI を設定する場合の詳細については、該当する NNM iSPI のマニュアルを参照してください。

HA 下で実行中の NNM iSPI Network Engineering Toolset Software と NNMi

NNM iSPI Network Engineering Toolset Software SNMP トラップ分析と Microsoft Visio エクスポート機能は、NNMi と一緒に自動的にインストールされます。これらのツールを HA 下で実行するには、これ以上の作業は不要です。

NNM iSPI NET 診断サーバーは、NNMi HA リソース グループに含めることはできません。このコンポーネントは、NNMi 管理サーバーにインストールしないでください。NNM iSPI NET 診断サーバーを NNMi HA リソース グループ外のシステム上で実行するには、以下の手順を実行します。

1. NNMi HA リソース グループを完全に設定します。
2. NNM iSPI NET 診断サーバーを NNMi HA リソース グループ外のシステムに、インストールします。NNM iSPI NET 診断サーバー のインストール プロセス中に、NNMi HA リソース グループ仮想ホスト名を NNM サーバー ホスト名として指定します。

   詳細は、『*NNM iSPI Network Engineering Toolset Software Planning and Installation Guide*』を参照してください。

NNM iSPI NET 診断サーバーがすでに HA 下で実行される NNMi 管理サーバーにインストールされている場合、HA 下で実行する NNMi を設定する前に NNM iSPI NET 診断サーバーをアンインストールします。

NNM iSPI NET 診断サーバーをアンインストールすると、既存のレポートがすべて削除されます。

ここで説明するように既存のレポートを保存することもできますが、次の手順はテストされていません。

1. MySQL Workbench を使って、既存の `nnminet` データベースのバックアップを行う。

   MySQL Workbench は、**dev.mysql.com** のダウンロード領域から入手できます。
2. NNM iSPI NET 診断サーバーをアンインストールします。
3. HA 下で NNMi を実行するように、設定します。
4. 別のシステムに NNM iSPI NET 診断サーバーをインストールします。
5. フローを実行する前に、MySQL Workbench を使って、新しいインストール先にある `nnminet` データベースを復旧します。

Oracle 環境での HA 用の NNMi の設定

ここでは、Oracle データベースを使っている NNMi を HA 下で実行するための設定作業の概要を説明します。Oracle の設定方法は多数あり、Oracle のリリースによっても異なります。Oracle を HA 下で実行するための設定方法と Oracle HA リソース グループで

の NNMi の依存関係の作成方法については、HA 製品マニュアルを参照してください。Oracle の Web サイト (**www.oracle.com**) でも、HA 製品用の Oracle 設定方法が紹介されています。

Oracle での NNMi の依存関係

Oracle と NNMi の両方を HA 下で実行する場合は、NNMi HA リソース グループに、Oracle データベースに格納されていない NNMi データ用の共有ディスクを含める必要があります。また、以下の情報を考慮してください。

- HA 製品が依存関係をサポートする場合、各製品を別々の HA リソース グループ内で実行されるように設定するのが推奨される方法です。Oracle HA リソース グループは、NNMi HA リソース グループを起動する前に、完全に起動している必要があります。両方の HA リソース グループが同じ HA クラスタに含まれている場合は、クラスタ設定を変更してリソース グループの起動順序を設定します。それぞれの HA リソースグループが異なる HA クラスタに含まれている場合は、Oracle HA リソースグループに対するNNMiHAリソースグループの依存関係が満たされているかを確認します。
- HA 製品が依存関係をサポートしない場合は、Oracle システムと NNMi システムを NNMi HA リソース グループに含めてください。

Oracle 環境での HA 用の NNMi の設定

1. Oracle を HA 下で実行することを予定している場合は、最初に、以下の手順を実行します。
2. NNMi 用のに空の Oracle データベース インスタンスを作成します。
3. プライマリ NNMi ノードに、(最新の統合パッチも含めて) NNMi をインストールします。インストールの間に、以下を実行します。
   a. **[Oracle]** データベース タイプを選択してから、**[プライマリ サーバーのインストール]** を選択します。
   b. Oracle HA リソース グループ用の仮想 IP アドレスまたは仮想ホスト名を指定します。
4. プライマリ NNMi ノードで、308 ページの「プライマリ クラスタ ノードでの NNMi の設定」に従って、NNMi を HA 下で実行できるように設定します。
5. Oracle HA リソース グループでの NNMi の依存関係を設定します。

   具体的な手順については、HA 製品のマニュアルを参照してください。
6. セカンダリ NNMi ノードに、(最新の統合パッチも含めて) NNMi をインストールします。インストールの間に、以下を実行します。
   - **[Oracle]** データベース タイプを選択してから、**[セカンダリ サーバーのインストール]** を選択します。
   - Oracle HA リソース グループ用の仮想 IP アドレスまたは仮想ホスト名を指定します。
7. セカンダリ NNMi ノードで、310 ページの「セカンダリ クラスタ ノードでの NNMi の設定」に従って、NNMi を HA 下で実行するように設定します。
8. 各セカンダリ NNMi ノードで、手順 6 と手順 7 を繰り返します。

共有 NNMi データ

HA 下で実行する NNMi 実装では、HA クラスタ内のすべての NNMi ノード間でファイルを共有するために、独立したディスクを使う必要があります。

Oracle をプライマリ データベースとして使っている NNMi の実装でも、共有データ用に独立したディスクを使う必要があります。

NNMi の共有ディスク内のデータ

ここでは、NNMi を HA 下で実行する場合に、共有ディスクで管理される NNMi のデータ ファイルをリストします。

ファイルの場所は、次のように、共有ディスク内の場所にマッピングされます。

- *Windows*:
  - `%NnmInstallDir%` は、`%HA_MOUNT_POINT%¥NNM¥installDir` にマッピングされます。
  - `%NnmDataDir%` は、`%HA_MOUNT_POINT%¥NNM¥dataDir` にマッピングされます。
- *UNIX*:
  - `$NnmInstallDir` は、`$HA_MOUNT_POINT/NNM/installDir` にマッピングされます。
  - `$NnmDataDir` は、`$HA_MOUNT_POINT/NNM/dataDir` にマッピングされます。

共有ディスクに移動されるディレクトリは、以下のとおりです。

- *Windows*:
  - `%NnmDataDir%¥shared¥nnm¥databases¥Postgres`
    組み込みデータベース。Oracle データベースを使用する場合は存在しません。
  - `%NnmDataDir%¥log¥nnm`
    NNMi のロギング ディレクトリ。
  - `%NnmDataDir%¥shared¥nnm¥databases¥eventdb`
    pmd イベント データベース。
  - `%NnmInstallDir%¥nonOV¥jboss¥nms¥server¥nms¥data`
    ovjboss で使われるトランザクション ストア。
- *UNIX*:
  - `$NnmDataDir/shared/nnm/databases/Postgres`
    組み込みデータベース。Oracle データベースを使用する場合は存在しません。
  - `$NnmDataDir/log/nnm`
    NNMi のロギング ディレクトリ。
  - `$NnmDataDir/shared/nnm/databases/eventdb`
    pmd イベント データベース。
  - `$NnmInstallDir/nonOV/jboss/nms/server/nms/data`
    ovjboss で使われるトランザクション ストア。

これらのファイルは、`nnmhadisk.ovpl` コマンドによって、共有ディスク間でコピーされます。この章の手順に従って、このコマンドを実行します。コマンド構文の概要については、*nnm-ha* マンページを参照してください。

設定ファイルの複製

NNMi HA の実装では、ファイル レプリケーションを使って、HA クラスタ内のすべての NNMi ノードの NNMi 設定ファイルのコピーを管理します。デフォルトでは、NNMi コマンド nnmdatareplicator.ovpl がファイル レプリケーションを管理します。このコマンドは、フェイルオーバー プロセス中に、アクティブ ノードからパッシブ ノードに NNMi 設定ファイルをコピーします。nnmdatareplicator.conf ファイルには、データ レプリケーションに含める NNMi のフォルダーとファイルを指定します。

データ レプリケーション プロセスの詳細については、*nnm-ha* マンページを参照してください。

共有ディスクの手動準備

共有ディスクがHPのテスト済みフォーマット (306 ページの表 25にリスト) である場合は、HA 設定スクリプトによって共有ディスクが準備されるため、以下の手順はスキップしてください。

共有ディスクで、HA 製品によってサポートされているディスクフォーマットなど、未検証の設定が使用されている場合は、共有ディスクを手動で準備する必要があります。HA の設定作業時に、ファイル システム タイプの値として none と入力してから、共有ディスクと NNMi HA リソース グループでの共有ディスクの使用を設定します。

ディスクの設定は、NNMi HA リソースグループを設定する前、または後に実行できます。

共有ディスクを手動で準備するには、以下の手順を実行します。

1. 315 ページの「SAN または物理的に接続されたディスクの設定」の説明に従って、共有ディスクを設定します。
2. 以下の両方の手順を実行して、ディスクを認識するように NNMi HA リソースグループを設定します。
   - 316 ページの「ov.conf ファイルへの HA 変数の設定」
   - 316 ページの「NNMi HA リソースグループへの共有ディスクの移動」

SAN または物理的に接続されたディスクの設定

ディスクを、vxfs または ext3 ファイルシステムに接続およびフォーマットします。SAN または物理的に接続されたディスクを設定するには、以下の手順を実行します。

1. 共有ディスクがシステム ブート時にマウントされるように設定されていないことを確認します。

   リソース グループには、共有ディスクをマウントする役割があります。
2. 以下のように、デバイスを接続します。
   - SAN ディスクの場合、SAN デバイスをネットワークに追加します。

     SAN ディスクの論理ボリュームは、排他モードが使用できる場合には、排他モードである必要があります。
   - 物理的に接続されたディスクの場合、Yケーブルを使用してディスクを接続します。
3. オペレーティングシステムエントリを、すべてのクラスタノード (ディスクグループ、論理ボリューム、ボリュームグループ、およびディスク) に追加します。
   - SAN ディスクの場合、エントリは SAN を参照します。
   - 物理的に接続されたディスクの場合、エントリはディスクハードウェアを参照します。
4. 306 ページの表 25 にあるディスク フォーマットを使用してディスクをフォーマットします。

5 SAN がマウントされていることを確認します。

UNIX システムの参考 Web サイトは、次のとおりです。**http://www.unixguide.net/unixguide.shtml**

6 ディスクをマウント解除してデポートします。

7 設定をテストするには、ディスクをリソース グループに追加し、フェイルオーバーを開始します。

ov.conf ファイルへの HA 変数の設定

NNMi HA リソースグループは、以下の変数を使用して共有ディスクにアクセスします。

- `HA_POSTGRES_DIR=<HA_mount_point>/NNM/dataDir/shared/nnm/databases/Postgres`
- `HA_EVENTDB_DIR=<HA_mount_point>/NNM/dataDir/shared/nnm/eventdb`
- `HA_NNM_LOG_DIR=<HA_mount_point>/NNM/dataDir/log`
- `HA_JBOSS_DATA_DIR=<HA_mount_point>/NNM/installDir/nonOV/jboss/nms/server/nms/data`
- `HA_MOUNT_POINT=<HA_mount_point>`
- `HA_CUSTOMPOLLER_DIR=<HA_mount_point>/NNM/dataDir/shared/nnm/databases/custompoller`

NNMi HA リソースグループで NNM iSPI を実行する場合は、それらの NNM iSPI ごとに ov.conf 変数も設定します。詳細については、該当する NNM iSPI のマニュアルを参照してください。

`ov.conf` ファイルで共有ディスクにアクセスするための製品の変数を設定するには、前述の各変数に対して、以下のコマンドを実行します。

- *Windows*:

```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhaclusterinfo.ovpl ¥
-config NNM -set <variable> <value>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl ¥
-config NNM -set <variable> <value>
```

NNMi HA リソースグループへの共有ディスクの移動

製品マニュアルに従ってディスク設定ファイルを変更し、共有ディスクを NNMi HA リソース グループに移動します。たとえば、以下のようにします。

このプロセスを使用して、NIC カードやバックアップ ディスクなどの他のリソースを NNMi HA リソース グループに追加することもできます。

- *MSFC*: フェイルオーバー管理を使用して、リソースをリソースグループに追加します。
- *ServiceGuard* の場合 :

  `/etc/cmcluster/<resource_group>/<resource_group>.cntl`

- *VCS* の場合 : ディスク エントリーを追加し、`/opt/VRTSvcs/bin/hares` コマンドを使って HA 設定ファイルにリンクします。たとえば、以下のようにします。
- *RHCS* の場合 :

  `/etc/cluster/cluster.conf`

Windows Server での共有ディスク設定についての注記

Microsoft Knowledge Base の文書 237853 によれば、Windows Server 2008 のクラスタリングではダイナミックディスクはサポートされていません。正しくディスクを設定するには、以下の Web サイトの情報を参照してください。

- **http://support.microsoft.com/kb/237853**
- **http://www.petri.co.il/difference_between_basic_and_dynamic_disks_in_windows_xp_2000_2003.htm**

HA クラスタ内の NNMi のライセンス契約

NNMi を HA 下で実行する場合、NNMi の非商用ライセンスは NNMi HA リソース グループの仮想 IP アドレスが対象になります。NNMi ライセンス キーは、共有ディスクで管理されます。このため、各 NNMi HA リソースグループで、別個にライセンス契約された各製品に必要なのは非商用ライセンスキーのみです。

HA クラスタで NNMi のライセンスを設定する場合、アクティブ ノードのライセンス ファイルにある新しい情報で共有ディスクの `licenses.txt` *ファイルを更新する必要があります。HA クラスタで NNMi のライセンスを正しく設定するには、以下の手順を実行します。*

HA クラスタで NNMi のライセンスを正しく設定するには、アクティブな NNMi クラスタ ノードで以下の手順を実行します。

1. 115 ページの「NNMi ライセンスの取得」の説明に従って、注文した製品ごとに非商用の恒久ライセンス キーを入手してインストールします。NNMi 管理サーバーの IP ドレスを入力するよう求められたら、NNMi HA リソース グループの仮想 IP アドレスを入力します。
2. アクティブ ノードの `licenses.txt` ファイルにある新しい情報で、共有ディスクの `LicFile.txt` ファイルを更新します。以下のいずれかを行います。
   - `licenses.txt` ファイルが共有ディスクの `NNM` ディレクトリにある場合は、アクティブ ノードの `LicFile.txt` 内の新しいライセンス キーを共有ディスクの `licenses.txt` に追加します。
   - `licenses.txt` ファイルが共有ディスクにない場合は、アクティブ ノードから共有ディスクの `NNM` ディレクトリ内の `licenses.txt` に、`LicFile.txt` をコピーします。

   アクティブ ノードでは、`LicFile.txt` ファイルが以下の場所にあります。

   - *Windows*: `%AUTOPASS_HOME%¥data¥LicFile.txt`

     `%AUTOPASS_HOME%` の値を調べるには、システム環境変数を参照します。
   - *UNIX*: `/var/opt/OV/HPOvLIC/LicFile.txt`

   共有ディスクでは、`licenses.txt` ファイルの場所は、たとえば以下のとおりです。

   - *Windows*: `S:¥NNM¥licenses.txt`
   - *UNIX*: `/nnmount/NNM/licenses.txt`

HA 設定のメンテナンス

メンテナンス モード

NNMi のパッチまたは更新プログラムを新しいバージョンの NNMi に適用する必要がある場合は、NNMi HA リソース グループをメンテナンス モードにし、処理中のフェイルオーバーを回避します。NNMi HA リソース グループがメンテナンス モードにある場合、ユーザー (またはインストール スクリプト) は必要に応じて、プライマリ (アクティブ) クラスタ ノード上で ovstop コマンドや ovstart コマンドを実行できます。

ovstart コマンドや ovstop コマンドは、セカンダリ (バックアップ) クラスタ ノードでは絶対に実行しないでください。

HA リソース グループをメンテナンス モードにする

HA リソース グループをメンテナンス モードにすると、HA リソース グループの監視が無効になります。HA リソース グループがメンテナンス モードになっていると、その HA リソース グループの製品の停止や起動を行ってもフェイルオーバーは行われません。

HA リソース グループをメンテナンス モードにするには、アクティブ ノードで以下のファイルを作成します。

- *Windows*: `%NnmDataDir%¥hacluster¥<resource_group>¥maintenance`
- *UNIX*: `$NnmDataDir/hacluster/<resource_group>/maintenance`

maintenance ファイルの内容は以下のとおりです。

- HA リソースグループの監視を無効にするには、maintenance ファイルを作成します。このファイルは空にすることもできますし、キーワード NORESTART を含めることもできます。
- 設定手順を行っている間に NNMi が開始しないようにするには、maintenance ファイルの最初の行に以下の 1 語のみを記載してください。
  NORESTART

HA リソース グループのメンテナンス モードを解除する

HA リソース グループのメンテナンス モードを解除すると、HA リソース グループの監視が再び有効になります。HA リソース グループの製品を停止すると、HA リソース グループはパッシブなクラスタ ノードへフェイルオーバーします。

HA リソースグループのメンテナンスモードを解除するには、以下の手順を実行します。

1. NNMi が正しく実行してい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。

2. メンテナンスが開始される前にアクティブクラスタノードであったノードから、maintenance ファイルを削除します。このファイルについては、HA リソース グループをメンテナンス モードにする を参照してください。

HA クラスタ内の NNMi のメンテナンス

NNMi の起動と停止

NNMi を HA 下で実行している場合は、HA のメンテナンスが目的の指示がない限り、`ovstart` コマンドや `ovstop` コマンドは、*使わない*でください。通常のオペレーションでは、NNMi に用意されている HA コマンドまたは HA 製品の適切なコマンドを使用して、HA リソース グループの起動や停止を行います。

クラスタ環境で NNMi のホスト名や IP アドレスを変更する

クラスタ環境内のノードは、複数の IP アドレスやホスト名を持つことができます。ノードが別のサブネットのメンバーになった場合は、IP アドレスを変更する必要があります。それにより、IP アドレスや完全修飾ドメイン名が変更されます。

たとえば、UNIX システムでは、IP アドレスと関連ホスト名は、通常、次のいずれかの方法を使って設定されています。

- /etc/hosts
- ドメイン ネーム サービス (DNS)
- ネットワーク情報サービス (HP-UX または Linux では NIS、Solaris では NIS+)

NNMi は、管理対象ノードが参照できるように、NNMi データベース内に管理サーバーのホスト名と IP アドレスを格納します。

ネーム サーバーがない環境からネーム サーバー (すなわち、DNS や BIND) がある環境に移行した場合は、ネーム サーバーが新しい IP アドレスを解決することを確認してください。

ホスト名は、IP ネットワーク内で管理対象ノードを特定するために使われます。ノードには複数の IP アドレスが設定されていることがありますが、ホスト名は特定のノードを指定するために使われます。システムのホスト名は、`hostname` コマンドを使ったときに返される文字列です。

NNMi HA リソース グループの仮想ホスト名または IP アドレスを変更する場合は、アクティブ ノードのライセンス ファイルにある新しい情報で、共有ディスクの `licenses.txt` *ファイルを更新する必要があります。HA 設定を正しく更新するには、以下の手順を実行します。*

NNMi HA リソース グループの仮想ホスト名または IP アドレスを変更するには、アクティブな NNMi クラスタ ノードで以下の手順を実行します。

1. NNMi HA リソースグループの以前の仮想 IP アドレスの非商用恒久ライセンスキーを、NNMi HA リソースグループの新しい仮想 IP アドレスに変換します。

   この時点で、新しいライセンスキーをインストール*しない*でください。

2. 318 ページの「HA リソース グループをメンテナンス モードにする」の説明に従って、NNMi HA リソース グループをメンテナンス モードにします。

3 NNMi HA リソース グループを停止します。

- *Windows*:

  %NnmInstallDir%¥misc¥nnm¥ha¥nnmhastoprg.ovpl NNM ¥ *<resource_group>*

- *UNIX*:

  $NnmInstallDir/misc/nnm/ha/nnmhastoprg.ovpl NNM ¥ *<resource_group>*

4 NNMi HA リソースグループの IP アドレスまたはノード名を変更します。

a ov.conf ファイルの NNM_INTERFACE エントリーを編集して、新しいホスト名または IP アドレスに変更します。

b ovspmd.auth ファイル内の旧ホスト名を含む行を編集して、新しいホスト名を含むようにします。

ov.conf ファイルと ovspmd.auth ファイルは、以下の場所にあります。

- *Windows*: %NnmDataDir%¥shared¥nnm¥conf
- *UNIX*: $NnmDataDir/shared/nnm/conf

5 NNMi HAリソースグループのノード名を変更した場合、nnmsetofficialfqdn.ovpl コマンドを使用して、NNMi HA リソースグループの新しい完全修飾ドメイン名を使用するように、NNMi を設定します。たとえば、以下のようにします。

```
nnmsetofficialfqdn.ovpl newnnmi.servers.example.com
```

詳細については、*nnmsetofficialfqdn.ovpl* リファレンス ページ、または UNIX のマンページを参照してください。

6 新しい IP アドレスを使うように、クラスタ設定を変更します。

- *MSFC* の場合 :

  Failover Cluster Management で、***<resource_group>*** を開きます。

  ***<resource_group>*-ip** をダブルクリックして、**[パラメータ]** を選択し、新しい IP アドレスを入力します。

- *Serviceguard* の場合 :

  アクティブな HA クラスタノードで、/etc/cmcluster/*<resource_group>*/*<resource_group>*.cntl ファイルを編集して、IP[0]=*<old_IP_address>* を IP[0]=*<new_IP_address>* に置き換えます。(NNMi HA リソースグループを別のサブネットに移動した場合は、SUBNET[0]=*<old_subnet_mask>* も SUBNET[0]=*<new_subnet_mask>* に置き換えます。) そして、cmapplyconf を使って残りのシステムをすべてアップデートします。

- *VCS* の場合 :

  $NnmInstallDir/misc/nnm/ha/nnmhargconfigure.ovpl NNM ¥ *<resource_group>* -set_value *<resource_group>*-ip ¥ Address *<new_IP_address>*

- *RHCS* の場合 :

  アクティブな HA クラスタノードで、/etc/cluster/cluster.conf ファイルを編集して、ip address="*<old_IP_address>*" を ip address="*<new_IP_address>*" に置き換えます。次に、ccs_tool update /etc/cluster/cluster.conf を実行して、残りのシステムをすべて更新します。

7 115 ページの「NNMi ライセンスの取得」の説明に従って、NNMi HA リソースグループの新しい仮想IPアドレスの非商用恒久ライセンスキーをインストールします。

8 アクティブ ノードの licenses.txt ファイルにある新しい情報で、共有ディスクの LicFile.txt ファイルを更新します。以下のいずれかを行います。

- licenses.txt ファイルが共有ディスクの NNM ディレクトリにある場合は、アクティブ ノードの LicFile.txt 内の新しいライセンス キーを共有ディスクの licenses.txt に追加します。
- licenses.txt ファイルが共有ディスクにない場合は、アクティブ ノードから共有ディスクの NNM ディレクトリ内の licenses.txt に、LicFile.txt をコピーします。

アクティブ ノードでは、LicFile.txt ファイルが以下の場所にあります。

- *Windows*: %AUTOPASS_HOME%¥data¥LicFile.txt

  %AUTOPASS_HOME% の値を調べるには、システム環境変数を参照します。
- *UNIX*: /var/opt/OV/HPOvLIC/LicFile.txt

共有ディスクでは、licenses.txt ファイルの場所は、たとえば以下のとおりです。

- *Windows*: S:¥NNM¥licenses.txt
- *UNIX*: /nnmount/NNM/licenses.txt

9 NNMi HA リソース グループを起動します。

- *Windows*:

  %NnmInstallDir%¥misc¥nnm¥ha¥nnmhastartrg.ovpl NNM ¥ *<resource_group>*

- *UNIX*:

  $NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM ¥ *<resource_group>*

10 NNMi を正常に起動できたことを確認します。

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。

11 318 ページの「HA リソース グループのメンテナンス モードを解除する」の説明に従って、NNMi HA リソース グループのメンテナンス モードを解除します。

フェイルオーバーを行わせないように NNMi を停止する

NNMi のメンテナンスを行う必要がある場合は、アクティブ クラスタ ノードの NNMi を、パッシブ ノードへフェイルオーバーさせないように停止できます。アクティブ クラスタ ノードで以下の手順を実行します。

1 318 ページの「HA リソース グループをメンテナンス モードにする」の説明に従って、NNMi HA リソース グループをメンテナンス モードにします。

2 NNMi を停止します。

ovstop -c

メンテナンス後に NNMi を再起動する

フェイルオーバーしないように NNMi を停止した場合は、以下の手順を実行して、NNMi と HA 監視を再起動します。

1 NNMi を起動します。

```
ovstart -c
```

2 NNMi を正常に起動できたことを確認します。

```
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。

3 318 ページの「HA リソース グループのメンテナンス モードを解除する」の説明に従って、NNMi HA リソース グループのメンテナンス モードを解除します。

NNMi HA クラスタ内のアドオン NNM iSPI のメンテナンス

NNM iSPI は、NNMi に密接にリンクしています。アドオン NNM iSPI を NNMi HA クラスタ内のノードにインストールする場合は、NNMi HA クラスタのメンテナンス手順を使います。

HA クラスタ内の NNMi の設定を解除する

HA クラスタ内の NNMi の設定を解除する

NNMi ノードを HA クラスタから削除する手順には、NNMi のインスタンスの HA 設定を解除する手順も含まれます。設定を解除すると、NNMi のインスタンスをスタンドアロン管理サーバーとして実行できます。また、そのノードから NNMi をアンインストールできます。

高可用性用の NNMi の設定を維持するには、HA クラスタに、NNMi を実行中の 1 つのノードと、少なくとも、1 つのパッシブ NNMi ノードが必要です。HA クラスタから NNMi を完全に削除するには、クラスタ内のすべてのノードで HA 機能の設定を解除します。

HA クラスタの NNMi の設定を完全に解除するには、以下の手順に従います。

1 HA クラスタ内のアクティブなノードを特定します。スタンバイで、以下のコマンドを実行します。

- *Windows*:

```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhaclusterinfo.ovpl ¥
-group <resource_group> -activeNode
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl ¥
-group <resource_group> -activeNode
```

2 各パッシブ ノードで、HA クラスタから任意のアドオン NNM iSPI の設定を解除します。

詳細については、各 NNM iSPI のマニュアルを参照してください。

3 HA クラスタ内の任意のノードで、すべてのパッシブ ノード上のアドオン NNM iSPI が HA クラスタから設定解除されていることを確認します。

- *Windows*:

```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhaclusterinfo.ovpl ¥
-config NNM -get NNM_ADD_ON_PRODUCTS
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl ¥
-config NNM -get NNM_ADD_ON_PRODUCTS
```

コマンドの出力には、アドオン iSPI の設定が *<iSPI_PM_Name>*[*hostname_list*] のフォーマットでリストされます。たとえば、以下のようにします。

```
PerfSPIHA[hostname1, hostname2]
```

このとき、アクティブ ノードのホスト名のみが出力に表示されます。パッシブ ノードのホスト名が出力に表示される場合は、このコマンドの出力にアクティブ ノードのホスト名のみが表示されるようになるまで、手順 2 を繰り返します。

4 各パッシブ ノードで、HA クラスタから NNMi の設定を解除します。

- *Windows*:

```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhaunconfigure.ovpl NNM ¥
<resource_group>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM ¥
<resource_group>
```

このコマンドにより、共有ディスクへのアクセスが削除されますが、ディスク グループやボリューム グループは設定解除されません。

5 各パッシブノードで、NNMi HA リソースグループ固有のファイルを安全に保持できるように別の場所に移動します。

NNMi HA リソースグループを再設定する予定がない場合は、これらのファイルのコピーを保存する必要はありません。この時点でファイルを削除して構いません。

- *MSFC* の場合 : Windows Explorer で、%NnmDataDir%¥hacluster¥*<resource_group>*¥ フォルダを削除します。
- *Serviceguard* の場合 :

```
rm -rf /var/opt/OV/hacluster/<resource_group>
rm -rf /etc/cmcluster/<resource_group>
```

- *VCS* の場合 :

```
rm -rf /var/opt/OV/hacluster/<resource_group>
```

- *RHCS* の場合 :

```
rm -rf /var/opt/OV/hacluster/<resource_group>
```

6 アクティブ ノードで、HA クラスタからアドオン NNM iSPI の設定を解除します。

詳細については、各 NNM iSPI のマニュアルを参照してください。HA クラスタ内の任意のノードで、すべてのノード上のアドオン NNM iSPI が HA クラスタから設定解除されていることを確認します。

- *Windows*:

```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhaclusterinfo.ovpl ¥
-config NNM -get NNM_ADD_ON_PRODUCTS
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl ¥
-config NNM -get NNM_ADD_ON_PRODUCTS
```

ホスト名が出力に表示される場合は、このコマンドの出力が iSPI が設定されていないことを示すまで、手順 6 を繰り返します。

7 アクティブ ノードで、NNMi HA リソース グループを停止します。

- *Windows*:

```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhastoprg.ovpl NNM ¥
<resource_group>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhastoprg.ovpl NNM ¥
<resource_group>
```

このコマンドでは、共有ディスクへのアクセス権は削除しません。また、ディスク グループやボリューム グループの設定も解除しません。

8 各アクティブ ノードで、HA クラスタから NNMi の設定を解除します。

- *Windows*:

```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhaunconfigure.ovpl NNM ¥
<resource_group>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM ¥
<resource_group>
```

このコマンドにより、共有ディスクへのアクセスが削除されますが、ディスク グループやボリューム グループは設定解除されません。

9 アクティブノードで、NNMi HA リソースグループ固有のファイルを安全に保持できるように別の場所に移動します。

NNMi HA リソースグループを再設定する予定がない場合は、これらのファイルのコピーを保存する必要はありません。この時点でファイルを削除して構いません。

- *MSFC* の場合 : Windows Explorer で、`%NnmDataDir%¥hacluster¥<resource_group>¥` フォルダを削除します。
- *Serviceguard* の場合 :

```
rm -rf /var/opt/OV/hacluster/<resource_group>
rm -rf /etc/cmcluster/<resource_group>
```

- *VCS* の場合 :

```
rm -rf /var/opt/OV/hacluster/<resource_group>
```

- *RHCS* の場合 :

  rm -rf /var/opt/OV/hacluster/<*resource_group*>

10 共有ディスクをマウント解除します。

- NNMi HA クラスタの再設定を予定している場合は、ディスクを現状のままで保管できます。
- 共有ディスクを別の目的で使用する場合は、保存するデータをすべてコピーして (325 ページの「HA の外部の既存データベースを使用した NNMi の実行」の説明を参照) から、HA 製品のコマンドを使用し、ディスクグループとボリュームグループの設定を解除します。

HA の外部の既存データベースを使用した NNMi の実行

NNMi を HA の外部の任意のノードで既存のデータベースを使って実行する場合は、以下の手順を実行します。

1 アクティブ ノードで (存在する場合)、NNMi が実行中ではないことを確認します。

ovstop

あるいは、タスク マネージャ (Windows) または ps コマンド (UNIX) を使って、ovspmd プロセスのステータスをチェックします。

2 現在のノード (HA の外部で NNMi の実行を予定しているノード) で、NNMi が実行中ではないことを確認します。

ovstop

データの破壊を避けるために、NNMi のインスタンスが動作中ではないことや、共有ディスクにアクセス中ではないことを確認します。

3 (UNIX のみ) ディスク グループをアクティブ化します。

vgchange -a e <*disk_group*>

4 適切なオペレーティング システムのコマンドを使って、共有ディスクをマウントします。たとえば、以下のようにします。

- *Windows* の場合 : Windows Explorer を使用します。
- *UNIX*: `mount /dev/vgnnm/lvnnm /nnmmount`

5 共有ディスクからノードに、NNMi ファイルをコピーします。

- *Windows*:

```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhadisk.ovpl NNM ¥
-from <HA_mount_point>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM ¥
-from <HA_mount_point>
```

6 適切なオペレーティング システムのコマンドを使って、共有ディスクのマウントを解除します。たとえば、以下のようにします。

- *Windows* の場合 : Windows Explorer を使用します。
- *UNIX*: `umount /nnmmount`

7 (UNIX のみ) ディスク グループを非アクティブ化します。

vgchange -a n <*disk_group*>

8 115 ページの「NNMi ライセンスの取得」の説明に従って、この NNMi 管理サーバーの物理 IP アドレスの非商用恒久ライセンスキーを取得し、インストールします。

9 NNMi を起動します。

```
ovstart -c
```

従来、NNMi HA リソース グループで使われていたデータベースのコピーを使って、NNMi が起動されます。この NNMi 管理サーバーから管理対象としないノードの NNMi 設定を手動で削除します。

HA 下の NNMi のパッチ

パッチを NNMi に適用するには、HA メンテナンス モードで作業します。以下の手順に従ってください。

1 HA クラスタ内のアクティブなノードを特定します。

- *Windows*:

```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhaclusterinfo.ovpl ¥
-group <resource_group> -activeNode
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl ¥
-group <resource_group> -activeNode
```

2 318 ページの「HA リソース グループをメンテナンス モードにする」の説明に従って、アクティブノードで、NNMi HAリソースグループをメンテナンスモードにします。

NORESTART キーワードを組み込みます。

3 318 ページの「HA リソース グループをメンテナンス モードにする」の説明に従って、すべてのパッシブノードで、NNMi HA リソースグループをメンテナンスモードにします。

NORESTART キーワードを組み込みます。

4 アクティブ ノードで、以下の手順を実行します。

a NNMi を停止します。

```
ovstop -c
```

b ディスク コピーを実行して、共有ディスクをバックアップします。

c *オプション。* nnmbackup.ovpl コマンドまたはその他のデータベース コマンドを使って、NNMi データをすべてバックアップします。たとえば、以下のようにします。

```
nnmbackup.ovpl -type offline -scope all -target nnmi_backups
```

このコマンドの詳細については、347 ページの「NNMi のバックアップおよびリストア ツール」を参照してください。

d 該当する NNMi および NNM iSPI のパッチをシステムに適用します。

e NNMi を起動します。

```
ovstart -c
```

f NNMi を正常に起動できたことを確認します。

```
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。

5 各パッシブノードで、該当するパッチをシステムに適用します。

ovstart コマンドや ovstop コマンドは、セカンダリ (バックアップ) クラスタ ノードでは絶対に実行しないでください。

6 318 ページの「HA リソース グループのメンテナンス モードを解除する」の説明に従って、すべてのパッシブノードで、NNMi HA リソースグループをメンテナンスモードから解除します。

7 アクティブ ノードで、318 ページの「HA リソース グループのメンテナンス モードを解除する」の説明に従って、NNMi HA リソース グループをメンテナンス モードから解除します。

HA 下の NNMi を NNMi 9.0x から NNMi 9.10 にアップグレードする

環境に応じて、適切な手順に従ってください。

- 327 ページの「Windows、Linux、または Solaris オペレーティングシステムでの組み込みデータベースを使用した NNMi のアップグレード」
- 329 ページの「HP-UX オペレーティングシステムでの組み込みデータベースを使用した NNMi のアップグレード」
- 330 ページの「サポートされるすべてのオペレーティングシステムでの Oracle を使用した NNMi のアップグレード」

Windows、Linux、または Solaris オペレーティングシステムでの組み込みデータベースを使用した NNMi のアップグレード

NNMi 9.10 では、Linux オペレーティングシステムで、Serviceguard はサポートされなくなりました。NNMi が現在 Serviceguard HA で実行中の場合、このセクションの手順は使用できません。代わりに、322 ページの「HA クラスタ内の NNMi の設定を解除する」の説明に従って、HA から NNMi の設定を解除し、すべてのノードで NNMi をアップグレードしてから、305 ページの「HA 用の NNMi の設定」の説明に従って、サポートされる HA 製品で実行するように NNMi を設定してください。あるいは、297 ページの「高可用性クラスタに NNMi を設定する」の説明に従って、NNMi アプリケーション フェイルオーバーに対応するように NNMi を設定できます。

Windows、Linux、または Solaris オペレーティングシステムで、HA 下の NNMi 9.0x を HA 下の NNMi 9.10 にアップグレードするには、パッシブノードをアップグレードし、アクティブノードからパッシブノードにフェイルオーバーしてから、2 つ目のノードをアップグレードします。以下の手順に従ってください。

1 それぞれのパッシブ ノードに、順番にフェイルオーバーを強制的に実行して、すべての HA ノードで NNMi 9.0x の設定が一貫するようにします。

2 以下のようにして、NNMi 9.0x HA クラスタでアクティブなノードを判別します。

- *Windows*:

```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhaclusterinfo.ovpl ¥
-group <resource_group> -activeNode
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl ¥
-group <resource_group> -activeNode
```

この手順の残りの部分では、現在アクティブなノードをサーバー X とし、現在パッシブなノードをサーバー Y とします。

3 サーバー Y で、NNMi をアップグレードします。

a 以下のメンテナンス ファイルを作成して、HA リソース グループのモニタリングを無効にします。

— *Windows*: `%NnmDataDir%¥hacluster¥<resource_group>¥maintenance`

— *UNIX*: `$NnmDataDir/hacluster/<resource_group>/maintenance`

ファイルは空で構いません。

b 391 ページの「NNMi 9.0x からのアップグレード」の説明に従って、NNMi を最新バージョンにアップグレードします。

c エラーを生じずに、アップグレードが完了したことを確認します。

d すべてのアドオン NNM iSPI をバージョン 9.10 にアップグレードします。

詳細については、各 NNM iSPI のマニュアルを参照してください。

使用環境にスタンドアロン NNM iSPI が含まれる場合は、正常に機能させるためにそれらの製品もバージョン 9.10 にアップグレードする必要があります。それらの製品のアップグレードは、この手順の完了後に実行できます。

e メンテナンス ファイルを削除します。

— *Windows*: `%NnmDataDir%¥hacluster¥<resource_group>¥maintenance`

— *UNIX*: `$NnmDataDir/hacluster/<resource_group>/maintenance`

4 HA クラスタに複数のパッシブノードが含まれている場合、パッシブノードごとに手順 3 を繰り返します。

5 サーバー X で、NNMi をアップグレードします。

サーバー Y へのフェイルオーバー中にデータベースがアップグレードされている間、NNMi はおよそ 20 分間から 60 分間使用できません。システムメンテナンスの都合のいい時間にこの手順を実行するように計画できます。

a サーバー Y へのフェイルオーバーを強制的に実行します。

共有ディスクの NNMi データベースは、この時点で最新の NNMi 製品バージョンのフォーマットにアップグレードされます。

b 以下のメンテナンス ファイルを作成して、HA リソース グループのモニタリングを無効にします。

— *Windows*: `%NnmDataDir%¥hacluster¥<resource_group>¥maintenance`

— *UNIX*: `$NnmDataDir/hacluster/<resource_group>/maintenance`

ファイルは空で構いません。

c 391 ページの「NNMi 9.0x からのアップグレード」の説明に従って、NNMi を最新バージョンにアップグレードします。

d エラーを生じずに、アップグレードが完了したことを確認します。

e すべてのアドオン NNM iSPI をバージョン 9.10 にアップグレードします。

詳細については、各 NNM iSPI のマニュアルを参照してください。

f メンテナンス ファイルを削除します。

— *Windows*: `%NnmDataDir%¥hacluster¥<resource_group>¥maintenance`

— *UNIX*: `$NnmDataDir/hacluster/<resource_group>/maintenance`

6 オプション。サーバー Y からサーバー X へのフェイルオーバーを強制的に実行し、アップグレード プロセスの前にアクティブだったノードを再びアクティブ ノードにできるようにします。

HP-UX オペレーティングシステムでの組み込みデータベースを使用した NNMi のアップグレード

HP-UX オペレーティングシステムで NNMi をアップグレードするには、Postgres データベースを 32 ビットバージョンから 64 ビットバージョンに移行する必要があります。このため、アップグレードプロセスの間、NNMi の操作を停止する必要があります。

このアップグレードプロセスの間、NNMi はおよそ 30 分間から 60 分間使用できません。

HP-UX オペレーティングシステムで、HA 下の NNMi 9.0x を HA 下の NNMi 9.10 にアップグレードするには、アクティブノードをアップグレードして組み込みデータベースを更新してから、NNMi がメンテナンスモードである間にパッシブノードをアップグレードします。以下の手順に従ってください。

1 それぞれのパッシブ ノードに、順番にフェイルオーバーを強制的に実行して、すべての HA ノードで NNMi 9.0x の設定が一貫するようにします。

2 すべてのノードで、NNMi 9.0x パッチ 2 (9.01)、または NNMi 9.0x のそれ以上のバージョンが実行されていることを確認します。

   必要に応じて、各システムを最新の NNMi 9.0x 統合パッチにアップグレードします。NNMi 9.0x の最新版の『NNMi デプロイメント リファレンス』にある「高可用性クラスタに NNMi を設定する」の章の「HA 下の NNMi を NNMi 8.1x から NNMi 9.01 にアップグレードする」セクションの指示に従います。

3 以下のようにして、NNMi 9.0x HA クラスタでアクティブなノードを判別します。

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl ¥
-group <resource_group> -activeNode
```

   この手順の残りの部分では、現在アクティブなノードをサーバー X とし、現在パッシブなノードをサーバー Y とします。

4 サーバー X で、以下のメンテナンスファイルを作成して、HA リソースグループの監視を無効にします。

```
$NnmDataDir/hacluster/<resource_group>/maintenance
```

   ファイルは空で構いません。

5 サーバー X で、NNMi をアップグレードします。

   a 391 ページの「NNMi 9.0x からのアップグレード」の説明に従って、NNMi を最新バージョンにアップグレードします。

      この手順の実行中に、データベースがアップグレードされます。

   b 以下のコマンドを入力して、アップグレードが正常に完了したことを確認します。

```
ovstart
```

      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。

c すべてのアドオン NNM iSPI をバージョン 9.10 にアップグレードします。

詳細については、各 NNM iSPI のマニュアルを参照してください。

使用環境にスタンドアロン NNM iSPI が含まれる場合は、正常に機能させるためにそれらの製品もバージョン 9.10 にアップグレードする必要があります。それらの製品のアップグレードは、この手順の完了後に実行できます。

6 サーバー Y で、NNMi をアップグレードします。

a 391 ページの「NNMi 9.0x からのアップグレード」の説明に従って、NNMi を最新バージョンにアップグレードします。

b エラーを生じずに、アップグレードが完了したことを確認します。

c すべてのアドオン NNM iSPI をバージョン 9.10 にアップグレードします。

詳細については、各 NNM iSPI のマニュアルを参照してください。

7 HA クラスタに複数のパッシブノードが含まれている場合、パッシブノードごとに手順 6 を繰り返します。

8 サーバー X で、メンテナンス ファイルを削除します。

```
$NnmDataDir/hacluster/<resource_group>/maintenance
```

サポートされるすべてのオペレーティングシステムでの Oracle を使用した NNMi のアップグレード

Oracle 環境で HA に対応するように NNMi をアップグレードするには、327 ページの「Windows、Linux、または Solaris オペレーティングシステムでの組み込みデータベースを使用した NNMi のアップグレード」で説明されている手順に従います。

HA 設定のトラブルシューティング

この項では、以下のトピックについて説明します。

- 331 ページの「一般的な設定の誤り」
- 332 ページの「HA リソース テスト」
- 333 ページの「一般的な HA のトラブルシューティング」
- 335 ページの「NNMi 固有の HA のトラブルシューティング」
- 340 ページの「NNM iSPI 固有の HA のトラブルシューティング」

一般的な設定の誤り

HA 設定における一般的な誤りの一部を以下に示します。

- 正しくないディスク設定
  - VCS: リソースをプローブできない場合は、設定に何らかの間違いがあります。ディスクをプローブできない場合、オペレーティング システムはディスクにアクセスできなくなる可能性があります。
  - 手動でディスク設定をテストし、設定が適切であることを HA のマニュアルの記載内容と照合して確認してください。
- ディスクが使用中で、HA リソース グループで起動できない。

  HA リソース グループを起動する前に、ディスクがアクティブでないことを必ず確認してください。
- MSFC: ネットワーク設定が正しくない

  ネットワーク トラフィックが複数の NIC カード上を流れる場合は、NNMi ovjboss プロセスなどのネットワーク帯域幅を大量に消費するプログラムをアクティブ化すると RDP セッションが失敗します。
- 一部の HA 製品がブート時に自動的に再起動しない。

  ブート アップ時の自動再起動の設定方法については、HA 製品のマニュアルを確認してください。
- NFS または他のアクセスが OS に直接追加される (リソース グループ設定でこの動作を管理している必要があります)。
- フェイルオーバーの間、または HA リソース グループをオフラインにする間に、共有ディスクのマウント ポイントに存在している。

  HA は、共有ディスクのマウント解除を阻止するプロセスをすべて抹消します。
- HA クラスタの仮想 IP アドレスを HA リソースの仮想 IP アドレスとして再使用している (一方のシステムで有効で、他方では無効)
- タイムアウトが短すぎる。製品に不具合があると、HA 製品は HA リソースをタイムアウトさせ、フェイルオーバーが実行されます。

  MSFC: Failover Cluster Management で、**[リソースが開始するまでの待機時間]** の設定値を確認します。NNMi では、この値は 15 分に設定されます。この値を増やすことができます。

- メンテナンス モードを使用していない

  メンテナンスモードは、HA の障害をデバッグするために作成されました。リソースグループがシステムでオンラインに設定され、その後すぐにフェイルオーバーを実行する場合、メンテナンスモードは、システムでリソースグループを維持し、実際に障害のある部分を見つけるのに役立ちます。

- クラスタログを再確認していない (クラスタログで多くの一般的な間違いを確認できます)。

HA リソース テスト

このセクションでは、NNMi HA リソースグループに入れるリソースのテストを行うための一般的な方法を説明します。このテストによって、ハードウェア設定の問題が特定されます。HA の下で実行するように NNMi を設定する*前に*、このテストを実行することをお勧めします。好ましい結果を出した設定値を記録しておき、NNMi HA リソースグループの完全な設定を行うときに、それらの値を使用します。

ここに記載されているコマンドについての詳細は、HA 製品の最新マニュアルを参照してください。

HA リソースをテストするには、以下の手順を実行します。

1. 必要に応じて、HA クラスタを起動します。
2. (Windows のみ) HA クラスタに、以下の仮想 IP アドレスが定義されていることを確認します。
   - HA クラスタの仮想 IP アドレス
   - 各 HA リソースグループの仮想 IP アドレス

   これらの各 IP アドレスは、別の場所で使用しないでください。
3. HA リソース グループを HA クラスタに追加します。

   この HA リソースグループには、`test` など、非商用名を使用してください。
4. HA リソースグループへの接続をテストします。
   a. 仮想 IP アドレスと、リソースグループに対応する仮想ホスト名を、リソースとして HA リソースグループに追加します。

      後で NNMi HA リソースグループに関連付ける値を使用します。
   b. アクティブ クラスタ ノードからパッシブ クラスタ ノードにフェイルオーバーし、HA クラスタが正常にフェイルオーバーすることを確認します。
   c. 新しいアクティブ クラスタ ノードから新しいパッシブ クラスタ ノードにフェイルオーバーし、フェイルバックを確認します。
   d. リソースグループが正しくフェイルオーバーしない場合、アクティブノードにログオンして、IP アドレスが正しく設定され、アクセス可能であることを確認します。また、ファイアウォールによって IP address.v がブロックされていないかも確認します。
5. 315 ページの「SAN または物理的に接続されたディスクの設定」の説明に従って、共有ディスクを設定します。
6. 共有ディスクへの接続をテストします。
   a. 316 ページの「NNMi HA リソースグループへの共有ディスクの移動」の説明に従って、共有ディスクをリソースとして HA リソースグループに追加します。
   b. アクティブ クラスタ ノードからパッシブ クラスタ ノードにフェイルオーバーし、HA クラスタが正常にフェイルオーバーすることを確認します。

c 新しいアクティブ クラスタ ノードから新しいパッシブ クラスタ ノードにフェイルオーバーし、フェイルバックを確認します。

d リソースグループが正しくフェイルオーバーしない場合、アクティブノードにログオンして、ディスクがマウントされ、使用可能であることを確認します。

7 共有ディスクの設定に使用したコマンドおよび入力値の記録を取っておきます。NNMi HA リソースグループを設定するときに、この情報が必要になる場合があります。

8 各ノードからリソースグループを削除します。

a IP アドレスエントリを削除します。

b リソースグループをオフラインに設定して、ノードからリソースグループを削除します。

この時点で、NNMi に付属しているツールを使用して、HA 下で実行するように NNMi を設定することができます。

一般的な HA のトラブルシューティング

このセクションのトピックは、NNMi および NNM iSPI の HA 設定に適用されます。以下の内容が含まれます。

- エラー : 引数の数が正しくない
- リソースをホストするサブシステムプロセスが予期せず停止する (Windows Server 2008 R2)
- 製品の起動タイムアウト (Solaris)
- アクティブなクラスタ ノードのログ ファイルが更新されない
- NNMi HA リソース グループを特定のクラスタ ノードで起動できない

エラー : 引数の数が正しくない

Perl モジュール製品の名前は、大部分の NNMi HA 設定コマンドで必須パラメータになりました。

- NNMi では、値として `NNM` を使用します。
- NNM iSPI で使用する値を調べるには、その NNM iSPI のマニュアルを参照してください。

リソースをホストするサブシステムプロセスが予期せず停止する (Windows Server 2008 R2)

Windows Server 2008 R2 オペレーティングシステムを実行しているコンピュータで HA クラスタリソースを起動すると、リソースをホストするサブシステム (`Rhs.exe`) プロセスが予期せずに停止します。

この既知の問題の詳細については、Microsoft サポート Web サイトの記事「*Windows Server 2008 R2 では、クラスター リソースを起動すると、リソースをホストするサブシステム (Rhs.exe) プロセスが予期せず停止します*」(**http://support.microsoft.com/kb/978527**) を参照してください。

NNMi リソースを実行するときは、必ず、リソースグループに固有の別個のリソースモニタ (rhs.exe) で実行してください。

製品の起動タイムアウト (Solaris)

1 つ以上の /var/adm/messages* ファイルに、次の例のようなメッセージが含まれます。

```
VCS ERROR V-16-1-13012 Thread(…) Resource(<resource group>-app):
online procedure did not complete within the expected time.
```

このメッセージは、製品が Veritas タイムアウト値の範囲内で完全には起動できなかったことを示しています。NNMi に付属した HA 設定スクリプトでは、タイムアウトは 15 分と定義されています。

Solaris オペレーティング システムでの Veritas タイムアウト値を変更するには、以下のコマンドを、以下の順番で、実行します。

```
/opt/VRTSvcs/bin/haconf -makerw
/opt/VRTSvcs/bin/hares -modify <resource_group>-app OnlineTimeout <value in seconds>
/opt/VRTSvcs/bin/haconf -dump -makero
```

アクティブなクラスタ ノードのログ ファイルが更新されない

これは正常です。ログ ファイルは、共有ディスクにリダイレクトされているため、このような状況になります。

NNMi の場合は、ov.conf ファイル内の HA_NNM_LOG_DIR で指定された場所にあるログ ファイルを調べてください。

NNMi HA リソース グループを特定のクラスタ ノードで起動できない

nnmhastartrg.ovpl コマンドまたは nnmhastartrg.ovpl コマンドで、NNMi HA リソースグループを正常に起動、停止、または切り替えできない場合は、以下の事柄を調べてください。

- *MSFC* の場合 :
  - Failover Cluster Management で、NNMi HA リソースグループと基盤リソースの状態を調べてください。
  - イベント ビューアのログにエラーが記録されていないか調べてください。
- *Serviceguard の場合:*

  <resource_group>.cntl.log ファイルと syslog ファイルにエラーが記録されていないか調べてください。良くある原因は、リソースを追加できない状態 (たとえば、ディスク グループの設定を誤っているため、アクティブにできない) のままで、システムが放置されていることです。

  /etc/cmcluster/*<resource_group>*/*<resource_group>*.cntl.log
- *VCS* の場合 :
  - **/opt/VRTSvcs/bin/hares -state** を実行してリソース状態を確認します。
  - 障害が発生しているリソースでは、障害が発生しているリソース用の /var/VRTSvcs/log/*<resource>*.log ファイルを調べます。リソースは、IP*.log、Mount*.log、Volume*.log などのエージェント タイプで指定します。
- *RHCS:*

  <resource_group>.cntl.log ファイルと syslog ファイルにエラーが記録されていないか調べてください。良くある原因は、リソースを追加できない状態 (たとえば、ディスク グループの設定を誤っているため、アクティブにできない) のままで、システムが放置されていることです。

  /etc/cmcluster/*<resource_group>*/*<resource_group>*.cntl.log

問題の原因を特定できない場合は、HA 製品のコマンドを使用して NNMi HA リソース グループを手動で起動できます。

1 共有ディスクをマウントします。

2 仮想ホストをネットワーク インタフェースに割り当てます。

- *MSF* の場合 :
  - Failover Cluster Management を起動します。
  - リソース グループを展開します。
  - **[*<resource_group>*-ip]** を右クリックして、**[Bring Online]** をクリックします。
- *Serviceguard の場合 :* `/usr/sbin/cmmodnet` を実行して、IP アドレスを追加します。
- *VCS* の場合 : **`/opt/VRTSvcs/bin/hares -online <resource_group>-ip ¥ -sys <local_hostname>`**
- *RHCS の場合 :* `/usr/sbin/cmmodnet` を実行して、IP アドレスを追加します。

3 NNMi HA リソース グループを起動します。たとえば、以下のようにします。

- *Windows*:

  ```
  %NnmInstallDir%¥misc¥nnm¥ha¥nnmhastartrg.ovpl NNM ¥
  -start <resource_group>
  ```

- *UNIX*:

  ```
  $NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM ¥
  -start <resource_group>
  ```

リターン コード 0 は、NNMi を正常に起動できたことを意味します。

リターン コード 1 は、NNMi を正常に起動できなかったことを意味します。

NNMi 固有の HA のトラブルシューティング

この項の内容が適用されるのは、NNMi のみの HA 設定です。以下の内容が含まれます。

- すべてのクラスタ ノードを設定解除した後の HA 用 NNMi の再有効化
- NNMi を HA 下で正常に起動できない
- NNMi データへの変更がフェイルオーバーの後に表示されない
- HA の設定後、nmsdbmgr を起動できない
- HA の設定後、pmd を起動できない
- NNMi が 1 つの HA クラスタ ノードでのみ正常に実行される (Windows)
- ディスク フェイルオーバーが行われない
- 共有ディスクにアクセスできない (Windows)
- 共有ディスクに最新データが含まれない
- フェイルオーバー後にセカンダリ ノードが共有ディスク ファイルを見つけられない

すべてのクラスタ ノードを設定解除した後の HA 用 NNMi の再有効化

すべての NNMi HA クラスタ ノードの設定を解除した場合は、NNMi の共有ディスクのマウント ポイントへのリンクが、ov.conf ファイルから削除されます。共有ディスク内のデータを上書きすることなく、マウント ポイントへのリンクを作成しなおすには、プライマリ ノードで以下の手順を実行します。

1 NNMi が実行中であれば、停止します。

```
ovstop -c
```

2 共有ディスクへのリンクを削除します。

- *Windows*:

```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhadisk.ovpl NNM ¥
-setmount <HA_mount_point>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM ¥
-setmount <HA_mount_point>
```

3 ov.conf ファイルの HA マウント ポイント関連のエントリーを確認します。

ov.conf ファイルの場所は、341 ページの「NNMi HA 設定ファイル」を参照してください。

NNMi を HA 下で正常に起動できない

NNMi が正しく起動しない場合、問題が仮想 IP アドレスまたはディスクに関するハードウェアの問題であるのか、ある種のアプリケーション障害の問題であるのかをデバッグする必要があります。このデバッグプロセスの間、NORESTART キーワードを設定しないで、システムをメンテナンスモードにします。

1 HA クラスタのアクティブノードで、以下のメンテナンスファイルを作成して、HA リソースグループの監視を無効にします。

- *Windows*: %NnmDataDir%¥hacluster¥<*resource_group*>¥maintenance
- *UNIX*: $NnmDataDir/hacluster/<*resource_group*>/maintenance

2 NNMi を起動します。

```
ovstart
```

3 NNMi を正常に起動できたことを確認します。

```
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。このように表示されない場合、正しく開始していないプロセスをトラブルシューティングします。

4 トラブルシューティングが完了したら、メンテナンスファイルを削除します。

- *Windows*: %NnmDataDir%¥hacluster¥<*resource_group*>¥maintenance
- *UNIX*: $NnmDataDir/hacluster/<*resource_group*>/maintenance

NNMi データへの変更がフェイルオーバーの後に表示されない

NNMi の設定で、NNMi を実行中のシステム以外のシステムを指しています。この問題を解決するには、ov.conf ファイルに以下の項目に対応した適切なエントリーがあるか確認します。

- NNM_INTERFACE=<*virtual_hostname*>
- HA_RESOURCE_GROUP=<*resource_group*>
- HA_MOUNT_POINT=<*HA_mount_point*>
- NNM_HA_CONFIGURED=YES
- HA_POSTGRES_DIR=<*HA_mount_point*>/NNM/dataDir/shared/nnm/databases/Postgres
- HA_EVENTDB_DIR=<*HA_mount_point*>/NNM/dataDir/shared/nnm/eventdb
- HA_CUSTOMPOLLER_DIR=<*HA_mount_point*>/NNM/dataDir/shared/nnm/databases/custompoller
- HA_NNM_LOG_DIR=<*HA_mount_point*>/NNM/dataDir/log
- HA_JBOSS_DATA_DIR=<*HA_mount_point*>/NNM/installDir/nonOV/jboss/nms/server/nms/data
- HA_LOCALE=C

ov.conf ファイルの場所は、341 ページの「NNMi HA 設定ファイル」を参照してください。

HA の設定後、nmsdbmgr を起動できない

この状況は、通常、nnmhaconfigure.ovpl コマンドを実行したが、-to オプションを指定して nnmhadisk.ovpl コマンドを実行せずに NNMi を起動した場合に発生します。この状況では、ov.conf ファイルの HA_POSTGRES_DIR エントリは、共有ディスクの組み込みデータベースの場所を指していますが、この場所は NNMi からはアクセスできません。

この問題を解決するには、以下の手順を実行します。

1. HA クラスタのアクティブノードで、以下のメンテナンスファイルを作成して、HA リソースグループの監視を無効にします。
   - *Windows*: %NnmDataDir%¥hacluster¥<*resource_group*>¥maintenance
   - *UNIX*: $NnmDataDir/hacluster/<*resource_group*>/maintenance
2. NNMi データベースを共有ディスクにコピーします。
   - *Windows*:

     ```
     %NnmInstallDir%¥misc¥nnm¥ha¥nnmhadisk.ovpl NNM ¥
     -to <HA_mount_point>
     ```

   - *UNIX*:

     ```
     $NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM ¥
     -to <HA_mount_point>
     ```

データベースの破壊を避けるために、この (-to オプションを指定した) コマンドは一回しか実行できません。代替方法については、336 ページの「すべてのクラスタノードを設定解除した後の HA 用 NNMi の再有効化」を参照してください。

3 NNMi HA リソース グループを起動します。

- *Windows*:

  %NnmInstallDir%¥misc¥nnm¥ha¥nnmhastartrg.ovpl NNM ¥ *<resource_group>*

- *UNIX*:

  $NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM ¥ *<resource_group>*

4 NNMi を起動します。

ovstart

5 NNMi を正常に起動できたことを確認します。

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。

6 トラブルシューティングが完了したら、メンテナンスファイルを削除します。

- *Windows*: %NnmDataDir%¥hacluster¥*<resource_group>*¥maintenance
- *UNIX*: $NnmDataDir/hacluster/*<resource_group>*/maintenance

HA の設定後、pmd を起動できない

この状況は、通常、共有ディスクを正しく設定しなかったなどの設定エラー後に発生します。pmd プロセスの障害は、ovjboss プロセスを完全に起動できなかった場合に発生します。

以下のログ ファイルを調べてください。

- *Windows*: %HA_MOUNT_POINT%¥NNM¥dataDir¥log¥nnm¥jbossServer.log
- *UNIX*: $HA_MOUNT_POINT/NNM/dataDir/log/nnm/jbossServer.log

NNMi が 1 つの HA クラスタ ノードでのみ正常に実行される (Windows)

Windows オペレーティング システムには、2 つの異なる仮想 IP アドレス (HA クラスタ用に 1 つと、HA リソース グループ用に 1 つ) が必要です。HA クラスタの仮想 IP アドレスと NNMi HA リソース グループの仮想 IP アドレスが同じ場合、NNMi は、HA クラスタの IP アドレスと関連付けられているノードでのみ正常に実行されます。

この問題を修正するには、HA クラスタの仮想 IP アドレスをネットワークで一意の値に変更します。

ディスク フェイルオーバーが行われない

この状況は、オペレーティングシステムが共有ディスクをサポートしていない場合に発生します。HA 製品、オペレーティング システム、ディスクのメーカーのマニュアルで調べて、これらの製品を混在させて使用できるか確認してください。

ディスク障害が発生すると、NNMi はフェイルオーバーでは起動しません。nmsdbmgr が失敗する理由の多くは、HA_POSTGRES_DIR ディレクトリが存在しないことです。共有ディスクがマウント済みであり、該当するファイルにアクセスできる状態になっていることを確認してください。

共有ディスクにアクセスできない (Windows)

nnmhaclusterinfo.ovpl -config NNM -get HA_MOUNT_POINT コマンドを実行しても何も戻されません。

共有ディスクのマウント ポイントのドライブは、HA 設定時に完全に指定する必要があります (たとえば、S:¥)。

この問題を修正するには、HA クラスタの各ノードで nnmhaconfigure.ovpl コマンドを実行します。共有ディスクのマウントポイントのドライブを完全に指定します。

共有ディスクに最新データが含まれない

ディスクタイプについての nnmhaconfigure.ovpl コマンドの質問にテキスト none で応答すると、ov.conf ファイルでディスク関連の変数を設定するコードがバイパスされます。この状況を修正するには、315 ページの「共有ディスクの手動準備」の手順に従います。

フェイルオーバー後にセカンダリ ノードが共有ディスク ファイルを見つけられない

この状況は、通常、共有ディスクがマウントされていないときに、-to オプションを付けた nnmhadisk.ovpl コマンドを実行した場合に発生します。この場合には、データ ファイルはローカル ディスクにコピーされ、共有ディスクには格納されません。

この問題を解決するには、以下の手順を実行します。

1. HA クラスタのアクティブノードで、以下のメンテナンスファイルを作成して、HA リソースグループの監視を無効にします。
   - *Windows*: %NnmDataDir%¥hacluster¥*<resource_group>*¥maintenance
   - *UNIX*: $NnmDataDir/hacluster/*<resource_group>*/maintenance
2. アクティブノードにログオンして、ディスクがマウントされ、使用可能であることを確認します。
3. NNMi を停止します。

   ovstop
4. NNMi データベースを共有ディスクにコピーします。
   - *Windows*:

     %NnmInstallDir%¥misc¥nnm¥ha¥nnmhadisk.ovpl NNM ¥
     -to *<HA_mount_point>*
   - *UNIX*:

     $NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM ¥
     -to *<HA_mount_point>*

データベースの破壊を避けるために、この (-to オプションを指定した) コマンドは一回しか実行できません。代替方法については、336 ページの「すべてのクラスタノードを設定解除した後の HA 用 NNMi の再有効化」を参照してください。

5 NNMi HA リソース グループを起動します。

- *Windows*:

  %NnmInstallDir%¥misc¥nnm¥ha¥nnmhastartrg.ovpl NNM ¥ *<resource_group>*

- *UNIX*:

  $NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM ¥ *<resource_group>*

6 NNMi を起動します。

  ovstart

7 NNMi を正常に起動できたことを確認します。

  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。

8 トラブルシューティングが完了したら、メンテナンスファイルを削除します。

- *Windows*: `%NnmDataDir%¥hacluster¥<resource_group>¥maintenance`
- *UNIX*: `$NnmDataDir/hacluster/<resource_group>/maintenance`

NNM iSPI 固有の HA のトラブルシューティング

HA 下で実行中の NNM iSPI のトラブルシュートについては、その NNM iSPI のマニュアルを参照してください。

HA 設定リファレンス

NNMi HA 設定ファイル

表 26 に、NNMi HA 設定ファイルを示します。これらのファイルは、NNMi 管理サーバー上の NNMi とアドオン NNM iSPI に適用されます。これらのファイルは、以下の場所にインストールされます。

- *Windows*: `%NnmDataDir%¥shared¥nnm¥conf`
- *UNIX*: `$NnmDataDir/shared/nnm/conf`

表 26　NNMi HA 設定ファイル

ファイル名	説明
ov.conf	このファイルは、NNMi HA 実装の状態を示し、`nnmhaclusterinfo.ovpl` コマンドによって更新されます。NNMi の各プロセスは、このファイルを読み取って、HA 設定を確認します。
nnmdatareplicator.conf	このファイルは、`nnmdatareplicator.ovpl` コマンドで、アクティブ ノードからパッシブ ノードへのデータ レプリケーションに含む NNMi のフォルダーとファイルを調べるために使われます。NNMi 設定のレプリケーション用に異なる手段を実装する場合は、含めるデータのリストは、このファイルを参照してください。 詳細については、このファイルのコメントを参照してください。

NNMi に付属している HA 設定スクリプト

表 27 と 表 28 に、NNMi に付属している HA 設定スクリプトを示します。表 27 に示した NNMi 付属のスクリプトは、カスタマ Perl モジュールを持つすべての製品に HA を設定する場合に使うことができる便利なスクリプトです。必要に応じて、HA 製品に付属しているコマンドを使って、NNMi 用に HA を設定できます。

NNMi 管理サーバーでは、NNMi に付属している HA 設定スクリプトは、以下の場所にインストールされます。

- *Windows*: `%NnmInstallDir%¥misc¥nnm¥ha`
- *UNIX*: `$NnmInstallDir/misc/nnm/ha`

表 27　NNMi HA 設定スクリプト

スクリプト名	説明
nnmhaconfigure.ovpl	NNMi または NNM iSPI を HA クラスタ用に設定します。 このスクリプトは、HA クラスタ内のすべてのノードで実行してください。
nnmhaunconfigure.ovpl	HA クラスタの NNMi または NNM iSPI の設定を解除します。 必要に応じて、HA クラスタ内の 1 つ以上のノードでこのスクリプトを実行します。
nnmhaclusterinfo.ovpl	NNMi に関するクラスタ情報を取得します。 このスクリプトは、必要に応じて、HA クラスタ内の任意のノードで実行します。

表 27　NNMi HA 設定スクリプト (続く)

スクリプト名	説明
nnmhadisk.ovpl	データ ファイルを、NNMi および NNM iSPI と共有ディスクの間でコピーします。 HA の設定時には、このスクリプトはプライマリ ノードで実行します。 それ以外の場合は、この章の手順に従って、このスクリプトを実行します。
nnmhastartrg.ovpl	HA クラスターで NNMi HA リソースグループを起動します。 HA の設定時には、このスクリプトはプライマリ ノードで実行します。
nnmhastoprg.ovpl	HA クラスターで NNMi HA リソースグループを停止します。 HA の設定解除時には、このスクリプトはプライマリ ノードで実行します。

表 28 に示した NNMi 付属のスクリプトは、341 ページの表 27 に示したスクリプトで使用します。表 28 に示したスクリプトは直接実行しないでください。

表 28　NNMi HA サポート スクリプト

スクリプト名	説明
nnmdatareplicator.ovpl	`nnmdatareplicator.conf` 設定ファイルを調べて、リモート システムに送信するファイルの変更やコピーを確認します。
nnmharg.ovpl	HA クラスタの NNMi を起動 / 停止 / 監視します。 Serviceguard 設定では、*<resource_group>*`.cntl` で使用します。 VCS 設定では、VCS の起動、停止、および監視のスクリプトで使用します。(`nnmhargconfigure.ovpl` で、この使用法を設定します。) また、トレースを有効 / 無効にするために、`nnmhastartrg.ovpl` でも使われます。
nnmhargconfigure.ovpl	HA のリソースとリソース グループを設定します。`nnmhaconfigure.ovpl` と `nnmhaunconfigure.ovpl` で使われます。
nnmhastart.ovpl	HA クラスタで NNMi を起動します。`nnmharg.ovpl` で使われます。
nnmhastop.ovpl	HA クラスタの NNMi を停止します。`nnmharg.ovpl` で使われます。
nnmhamonitor.ovpl	HA クラスタの NNMi プロセスを監視します。`nnmharg.ovpl` で使われます。
nnmhamscs.vbs	MSFC HA クラスタで、NNMi プロセスを起動、停止、および監視するスクリプトを作成するためのテンプレートです。生成されるスクリプトは MSFC によって使用され、次の場所に保存されます : `%NnmDataDir%¥hacluster¥`*<resource_group>*`¥hamscs.vbs`

NNMi HA 設定のログ ファイル

以下のログ ファイルは、NNMi 管理サーバー上の NNMi とアドオン NNM iSPI 用の HA 設定に適用されます。

- *Windows* 設定 :
  - %NnmDataDir%¥tmp¥HA_nnmhaserver.log
  - %NnmDataDir%¥log¥haconfigure.log
- *UNIX* 設定 :
  - $NnmDataDir/tmp/HA_nnmhaserver.log
  - $NnmDataDir/log/haconfigure.log
- *Windows* 実行時 :
  - イベント ビューアのログ
  - %HA_MOUNT_POINT%¥NNM¥dataDir¥log¥nnm¥ovspmd.log
  - %HA_MOUNT_POINT%¥NNM¥dataDir¥log¥nnm¥public¥postgres.log
  - %HA_MOUNT_POINT%¥NNM¥dataDir¥log¥nnm¥public¥nmsdbmgr.log
  - %HA_MOUNT_POINT%¥NNM¥dataDir¥log¥nnm¥jbossServer.log
  - %SystemRoot%¥Cluster¥cluster.log
    これは、リソースとリソース グループの追加 / 削除、他の設定上の問題点、起動 / 停止上の問題点を含む、クラスタ実行時の問題点に関するログ ファイルです。
- *HP-UX* 実行時 :
  - /etc/cmcluster/*<resource_group>*/*<resource_group>*.cntl.log
    これは、リソース グループ用のログ ファイルです。
  - /var/adm/syslog/syslog.log
  - /var/adm/syslog/OLDsyslog.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/ovspmd.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/postgres.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/nmsdbmgr.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/jbossServer.log

- VCS 用の *Linux* または *Solaris* の場合 :

リソース	ログ ファイル
<resource_group>-app	• /var/VRTSvcs/log/Application_A.log • $HA_MOUNT_POINT/NNM/dataDir/log/nnm/ovspmd.log • $HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/postgres.log • $HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/nmsdbmgr.log • $HA_MOUNT_POINT/NNM/dataDir/log/nnm/jbossServer.log • /var/adm/messages*
<resource_group>-dg *<resource_group>*-volume *<resource_group>*-mount	• /var/VRTSvcs/log/DiskGroup_A.log • /var/VRTSvcs/log/Volume_A.log • /var/VRTSvcs/log/Mount_A.log • /var/adm/messages*
<resource_group>-ip	• /var/VRTSvcs/log/IP_A.log • /var/adm/messages*
オペレーティング システム固有の HA リソース関連の問題は、/var/adm/messages* ファイルを調べてください。*<resource_group>*-app では、プロセスを起動できなかったことに関するメッセージを探してください。	

- RCHS 用の *Linux* 実行時 :
  - /var/adm/syslog/syslog.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/ovspmd.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/postgres.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/nmsdbmgr.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/jbossServer.log

NNMi のメンテナンス

この項では以下の章について説明します。

- NNMi のバックアップおよびリストア ツール
- NNMi の保守
- NNMi ロギング
- NNMi 管理サーバーの変更
- Xen 仮想化環境での NNMi の実行

NNMi のバックアップおよびリストア ツール

どのようなビジネスでも、中断することなく業務を確実に継続して行うには、バックアップおよびリストアに関して優れた方針を持つことが重要です。HP Network Node Manager i Software (NNMi) は、ネットワークを運用する上で重要な資産であり、定期的にバックアップする必要があります。

NNMi インストールに関連した重要データは、以下の 2 種類です。

- ファイル システム内のファイル
- リレーショナル データベース (組み込みまたは外部) のデータ

この章では、重要な NNMi ファイルおよびデータをバックアップおよびリストアするために NNMi で装備しているツールについて説明しています。

この章には、以下のトピックがあります。

- バックアップ コマンドとリストア コマンド
- NNMi データのバックアップ
- NNMi データのリストア
- バックアップとリストアの方針
- 組み込みデータベースのみをバックアップおよびリストアする

バックアップ コマンドとリストア コマンド

NNMi には、NNMi データをバックアップおよびリストアするために以下のスクリプトがあります。

- nnmbackup.ovpl - 必要なすべてのファイル システム データ (設定情報を含む) と NNMi 組み込みデータベースに保管されたデータをバックアップします。
- nnmrestore.ovpl - nnmbackup.ovpl スクリプトを使用して作成されたバックアップをリストアします。
- nnmbackupembdb.ovpl - NNMi 組み込みデータベース (ファイル システム データではない) の完全バックアップを、NNMi の稼働中に作成します。
- nnmrestoreembdb.ovpl - nnmbackupembdb.ovpl スクリプトを使用して作成されたバックアップをリストアします。
- nnmresetembdb.ovpl - NNMi 組み込みデータベース テーブルをドロップします。ovstart コマンドを実行してテーブルを再作成します。

コマンド構文については、該当するリファレンス ページまたは UNIX のマンページを参照してください。

NNMi データのバックアップ

NNMi バックアップ コマンド (nnmbackup.ovpl) は、主要な NNMi ファイル システム データ、および NNMi Postgres データベースのテーブルの一部またはすべてを、指定されたターゲット ディレクトリにコピーします。NNMi バックアップ コマンドにより、バックアップ データの tar アーカイブを作成したり、独自のツールを使用してバックアップ ファイルを圧縮したりできます。これで、適切なツールを使用してバックアップのコピーを保存できます。

NNMi 実装で Oracle をメイン NNMi データベースとして使用する場合は、NNMi ファイル システム データでのみ NNMi バックアップ コマンドとリストア コマンドを使用できます。外部データベースの保守は、既存のデータベース バックアップおよびリストア手順の一環として扱う必要があります。

バックアップ データとリストア データには、ご使用のネットワーク環境にインストールされている NNM iSPI すべてのデータが含まれていることも、含まれていないこともあります。詳細については、各 NNM iSPI に付属のドキュメントで確認してください。

ファイルをロックするソフトウェア (たとえば、ウイルス対策ソフトウェアやシステム バックアップソフトウェア) は、すべて NNMi データベースへの NNMi のアクセスを妨害する可能性があります。これにより、ウイルス対策アプリケーションなど、他のプロセスで使用されているファイルに対する読み取りまたは書き込みができなくなるような問題が生じる可能性があります。NNMi Postgres データベースの場合は、NNMi データベース ディレクトリ (Windows の %NNM_DB%、UNIX の $NNM_DB) を除外するようにアプリケーションを設定してください。NNMi データベースを定期的にバックアップするには、nnmbackup.ovpl を使用します。

バックアップ タイプ

NNMi のバックアップ コマンドでは、2 種類のバックアップがサポートされます。

- オンライン バックアップは NNMi の稼働中に行われます。NNMi では、バックアップされたデータ内でデータベース テーブルが確実に同期されます。オンライン バックアップ中でも、オペレータは制約を受けることなく NNMi コンソールを使用することができ、他のプロセスは NNMi データベースとやりとりできます。オンライン

バックアップを実行することにより、バックアップ領域に記載されているように、機能に応じて NNMi のデータすべてまたはデータの一部のみをバックアップできます。組み込み NNMi データベースの場合は、nmsdbmgr サービスが実行されている必要があります。外部データベースの場合、このバックアップには NNMi ファイルシステムデータが含まれます。外部データベースをバックアップするために、NNMi プロセスが実行されている必要はありません。

- オフライン バックアップは、NNMi が完全に停止している間に行われます。オフライン バックアップでは、バックアップ領域がファイル システムのファイルにのみ適用されます。オフライン バックアップには、バックアップ領域に関係なく、必ず NNMi データベースの全体が含まれます。組み込み NNMi データベースの場合、このバックアップでは Postgres データベースのファイルがコピーされます。外部データベースの場合、このバックアップには NNMi ファイル システム データのみが含まれます。

バックアップ領域

NNMi バックアップ コマンドでは、NNMi のバックアップ量を定義する領域をいくつか指定できます。

設定領域

設定領域 (-scope config) は、大まかには NNMi コンソールの **[設定]** ワークスペース内の情報と一致します。

設定領域には以下のデータが含まれます。

- オンライン バックアップの場合は、NNMi 設定情報を保存している組み込みデータベース テーブルのみ。
- オフライン バックアップの場合は、組み込みデータベース全体。
- 全バックアップの場合は、表 29 のリストに示すファイル システム内の NNMi 設定情報。

トポロジ領域

トポロジ領域 (-scope topology) は、大まかには NNMi コンソールの **[インベントリ]** ワークスペース内の情報と一致します。ネットワーク トポロジが依存している設定はそのトポロジの検出に使用されているため、トポロジ領域には設定領域が含まれます。

トポロジ領域には以下のデータが含まれます。

- オンライン バックアップの場合は、NNMi 設定情報とネットワーク トポロジ情報を保存している組み込みデータベース テーブルのみ。
- オフライン バックアップの場合は、組み込みデータベース全体。
- 全バックアップの場合は、表 29 のリストに示すファイル システム内の NNMi 設定情報。現在、トポロジ領域に関連付けられているファイル システムのファイルはありません。

イベント領域

イベント領域 (-scope event) は、大まかには NNMi コンソールの **[インシデントの参照]** ワークスペース内の情報と一致します。イベントはこれらのイベントに関連したネットワーク トポロジに依存しているため、イベント領域には設定領域とトポロジ領域が含まれます。

イベント領域には以下のデータが含まれます。

- オンライン バックアップの場合は、NNMi 設定情報、ネットワーク トポロジ情報、およびイベント情報を保存している組み込みデータベース テーブルのみ。
- オフライン バックアップの場合は、組み込みデータベース全体。
- 全バックアップの場合は、表 29 のリストに示すファイル システム内の NNMi 設定情報と、表 30 のリストに示す NNMi イベント情報。

全領域

完全バックアップ (-scope all) には、NNMi のすべての重要ファイルと組み込みデータベース全体が含まれます。

表 29　設定領域ファイルとディレクトリ

ディレクトリまたはファイル名	説明
%NnmInstallDir%/conf (Windows のみ)	設定情報
%NnmInstallDir%¥misc¥nms¥lic $NnmInstallDir/misc/nms/lic	その他のライセンス情報
%NnmInstallDi%r¥nonOV¥jboss¥nms¥server¥nms¥conf $NnmInstallDir/nonOV/jboss/nms/server/nms/conf	jboss の設定
%NnmDataDir%¥conf $NnmDataDir/conf	他の HP 製品が共有する設定
%NnmDataDir%¥conf¥nnm¥props $NnmDataDir/conf/nnm/props	ローカル NNMi 設定のプロパティ ファイル
• *Windows Server 2008*: *<drive>*:¥ProgramData¥Hewlett-Packard¥HPOvLIC¥data¥LicFile.txt • *UNIX*: $NnmDataDir/HPOvLIC/LicFile.txt	ライセンス情報
%NnmDataDir%¥NNMVersionInfo $NnmDataDir/NNMVersionInfo	NNMi バージョン情報ファイル
%NnmDataDir%¥shared¥nnm¥user-snmp-mibs $NnmDataDir/shared/nnm/user-snmp-mibs	共有されるユーザー追加の SNMP MIB 情報
%NnmDataDir%¥shared¥nnm¥actions $NnmDataDir/shared/nnm/actions	共有されるライフサイクルの移行アクション
%NnmDataDir%¥shared¥nnm¥certificates $NnmDataDir/shared/nnm/certificates	共有 NNMi SSL 証明書
%NnmDataDir%¥shared¥nnm¥conf $NnmDataDir/shared/nnm/conf	共有 NNMi 設定情報
%NnmDataDir%¥shared¥nnm¥conf¥licensing $NnmDataDir/shared/nnm/conf/licensing	共有 NNMi ライセンス設定情報
%NnmDataDir%¥shared¥nnm¥lrf $NnmDataDir/shared/nnm/lrf	共有される NNMi コンポーネント登録ファイル
%NnmDataDir%¥shared¥nnm¥conf¥props $NnmDataDir/shared/nnm/conf/props	共有される NNMi 設定のプロパティ ファイル
%NnmDataDir%¥shared¥nnm¥www¥htdocs¥images $NnmDataDir/shared/nnm/www/htdocs/images	共有される NNMi ノード グループ マップの背景イメージ

このコンテキストで、共有ディレクトリのファイルは、NNMi アプリケーション フェイルオーバーまたは高可用性環境の別の NNMi 管理サーバーと共有されるファイルです。

表 30　イベント領域ファイルとディレクトリ

ディレクトリまたはファイル名	説明
$NnmDataDir/log/nnm/signin.0.0.log	NNMi コンソール サインイン ログ

NNMi データのリストア

NNMi リストア スクリプト (nnmrestore.ovpl) は、バックアップ データを NNMi 管理サーバーに配置します。バックアップの種類と領域により、NNMi でリストア可能なバックアップ データが決まります。

nnmrestore.ovpl スクリプトを使用してデータベース レコードを 2 番目の NNMi 管理サーバー に配置する場合は、どちらの NNMi 管理サーバー も同じタイプのオペレーティング システム、NNMi バージョン、およびパッチ レベルである必要があります。

ある NNMi 管理サーバーから 2 番目の NNMi 管理サーバーにバックアップデータを配置すると、これらの両方のサーバーに同じデータベース UUID が存在することになります。2 番目の NNMi 管理サーバーに NNMi をリストアしたら、元の NNMi 管理サーバーから NNMi をアンインストールします。

- オンライン バックアップをリストアするため、NNMi は、ファイル システム データを正しい場所にコピーし、バックアップのデータベース テーブルの内容を上書きします。上書きするのは、バックアップのリストア以後に削除されたオブジェクトと、バックアップの削除以後に作成されたオブジェクトです。また、バックアップの実行後に変更されたすべてのオブジェクトは、バックアップ時の状態に戻されます。組み込み NNMi データベースの場合は、nmsdbmgr サービスが実行されている必要があります。外部データベースの場合、リストアには NNMi ファイル システム データのみが含まれ、実行中の NNMi プロセスが存在しないようにする必要があります。
- オフライン バックアップをリストアするため、NNMi は、ファイル システム内の Postgres ファイルを上書きし、データベース ファイルをバックアップ データで完全に置き換えます。外部データベースの場合、このバックアップには NNMi ファイル システム データのみが含まれます。

-force オプションを指定すると、nnmrestore.ovpl コマンドはすべての NNMi プロセスを停止し、nmsdbmgr サービスを開始し (NNMi 組み込みデータベースのオンライン バックアップからのリストアの場合)、データをリストアし、その後すべての NNMi プロセスを再開始します。

指定されたソースが tar ファイルの場合は、NNMi リストア コマンドにより、現在の作業ディレクトリの一時フォルダに tar ファイルが抽出されます。この場合、現在の作業ディレクトリに十分な記憶領域があるため一時フォルダを使用できることを確認するか、リストア コマンドを実行する前にアーカイブを抽出してください。

NNMi のあるバージョンから次のバージョンへデータベースのスキーマが変わる恐れがあるため、データ バックアップを NNMi の異なるバージョン間で共有することはできません。

同じシステムでのリストア

1 つのシステムでバックアップ コマンドとリストア コマンドを使用することにより、データを復旧できます。バックアップの実行時からリストアの実行時までの間に、以下の項目が変更されていないようにする必要があります。

- NNMi のバージョン (パッチを含む)
- オペレーティングシステムタイプ
- キャラクタ セット (言語)
- ホスト名
- ドメイン

異なるシステムでのリストア

バックアップ コマンドとリストア コマンドを使用して、NNMi 管理サーバーから他の管理サーバーへデータを転送することができます。異なるシステムでのリストアの用途には、システム障害からの復旧や、オペレーティング システムのアップグレード時の NNMi の異なるシステムへの転送などがあります。

ベストプラクティス

NNMi UUID がデータベースのリストア中にターゲット システムにコピーされるため、ソースとターゲットの両システムが NNMi の同じインスタンスを実行しているようです。ソース システムから NNMi をアンインストールしてください。

グローバル ネットワーク管理を導入する間など、同様の設定で機能する NNMi 管理サーバーを複数作成するには、`nnmconfigexport.ovpl` および `nnmconfigimport.ovpl` コマンドを使用します。

異なるシステムのリストアでは、両方のシステムで以下の項目を同じにする必要があります。

- NNMi のバージョン (パッチを含む)
- OS のタイプとバージョン
- キャラクタ セット (言語)

以下の項目は、2 つのシステム間で異なっていてもかまいません。

- ホスト名
- ドメイン

異なるシステムでのリストアの場合、`nnmrestore.ovpl` コマンドはライセンス情報を新規システムにコピーしません。新しい NNMi 管理サーバーの新規ライセンスを取得して適用してください。詳細については、115 ページの「NNMi ライセンスの取得」を参照してください。

バックアップとリストアの方針

すべてのデータを定期的にバックアップする

ディザスタ リカバリ計画には、すべての NNMi データの完全バックアップを定期的に実行するスケジュールを含めてください。このバックアップを作成するために NNMi を停止する必要はありません。バックアップをスクリプトに組み込む場合は、`-force` オプションを使用して、バックアップが開始される前に NNMi が正しい状態になるようにしてください。たとえば、以下のようにします。

```
nnmbackup.ovpl -force -type online -scope all -archive
  -target nnmi_backups¥periodic
```

ハードウェアの障害のために NNMi データを復旧することが必要になった場合は、以下の手順を実行します。

1. ハードウェアを再構成するか、新規ハードウェアを取得します。
2. バックアップ データの場合と同じバージョンおよびパッチ レベルの NNMi をインストールします。
3. NNMi データをリストアします。
   - リカバリ NNMi 管理サーバーが 352 ページの「同じシステムでのリストア」の一覧にある要件を満たす場合は、以下の例のようなコマンドを実行します。

     ```
     nnmrestore.ovpl -force -lic
     -source nnmi_backups¥periodic¥newest_backup
     ```

- リカバリ NNMi 管理サーバーが同じシステムでのリストアを行うのに適格ではなくても、353 ページの「異なるシステムでのリストア」の一覧にある要件を満たす場合は、以下の例に似たコマンドを実行します。

  ```
  nnmrestore.ovpl -force
    -source nnmi_backups¥periodic¥newest_backup
  ```

  必要に応じてライセンスを更新します。

設定変更前のデータのバックアップ

設定変更を開始する前に、領域を限定したバックアップ (349 ページの「バックアップ領域」で説明) を必要に応じて実施してください。このようにすると、設定を変更しても期待した効果が見られない場合、周知の作動設定に戻すことが可能になります。たとえば、以下のようにします。

```
nnmbackup.ovpl -type online -scope config
-target nnmi_backups¥config
```

このバックアップを同じ NNMi 管理サーバーにリストアするには、すべての NNMi プロセスを停止してから、以下の例のようなコマンドを実行します。

```
nnmrestore.ovpl -force -source nnmi_backups¥config¥newest_backup
```

NNMi またはオペレーティング システムのアップグレード前のバックアップ

大規模なシステム変更 (NNMi またはオペレーティング システムのアップグレードを含む) を行う前に、すべての NNMi データの完全バックアップを実行します。バックアップの実行後 NNMi データベースに対する変更が何も行われないようにするため、すべての NNMi プロセスを停止し、オフライン バックアップを作成してください。たとえば、以下のようにします。

```
nnmbackup.ovpl -type offline -scope all
-target nnmi_backups¥offline
```

システムの変更後に NNMi が正常に実行されなくなった場合は、変更をロールバックするか、または異なる NNMi 管理サーバーをセットアップし、353 ページの「異なるシステムでのリストア」の一覧にある要件が確実に満たされるようにしてください。その後、以下の例に似たコマンドを実行します。

```
nnmrestore.ovpl -lic -source nnmi_backups¥offline¥newest_backup
```

ファイル システムのファイルのみのリストア

データベース テーブルに影響を与えることなく NNMi ファイルを上書きするには、以下の例に似たコマンドを実行します。

```
nnmrestore.ovpl -partial
-source nnmi_backups¥offline¥newest_backup
```

このコマンドは、NNMi 実装のメイン NNMi データベースとして Oracle を使用する場合に役立ちます。

組み込みデータベースのみをバックアップおよびリストアする

NNMi では、nnmbackupembdb.ovpl コマンドと nnmrestoreembdb.ovpl コマンドにより、NNMi 組み込みデータベースのみをバックアップおよびリストアします。この機能は、NNMi の設定においてデータのスナップショットを作成する場合に便利です。nnmbackupembdb.ovpl コマンドと nnmrestoreembdb.ovpl コマンドは、オンラインバックアップのみを実行します。最低でも、nmsdbmgr サービスが実行されている必要があります。

ベストプラクティス

nnmresetembdb.ovpl コマンドは、組み込みデータベースにデータをリストアする前に実行してください。このコマンドによりデータベースにエラーが含まれないようになるため、データベース制約違反が発生する可能性がなくなります。組み込みデータベース リセット コマンドの実行については、*nnmresetembdb.ovpl* リファレンス ページか UNIX のマンページを参照してください。

NNMi の保守

NNMi 管理サーバーが機能するようになったら、複数の NNMi 機能を最適化するためにメンテナンス作業を実施することができます。

この章には、以下のトピックがあります。

- 358 ページの「カスタム ポーラー収集エクスポートの管理」
- 359 ページの「インシデント アクションの管理」
- 362 ページの「trapFilter.conf ファイルによるインシデントのブロック」
- 363 ページの「NNMi コンソールとの HTTPS 専用通信を設定する」
- 363 ページの「NNMi 正規化プロパティの変更」
- 365 ページの「同時 SNMP 要求の変更」
- 365 ページの「NNMi 自己監視」
- 366 ページの「特定ノードの検出プロトコルの使用を抑える」
- 369 ページの「大規模スイッチの VLAN インデックス付けの使用を抑制する」
- 371 ページの「NAT 環境における管理アドレスの ICMP ポーリングの概要」

カスタム ポーラー収集エクスポートの管理

カスタム ポーラー機能では、SNMP MIB 式を使用して NNMi がポーリングする必要のある追加情報を指定することによって、積極的にネットワーク管理を行えます。**カスタム ポーラー収集**は、収集 (ポーリング) する情報およびそれらの情報の NNMi による処理方法を定義します。詳細については、NNMi ヘルプの「*カスタム ポーラー収集を作成する*」および「*カスタム ポーリングを設定する*」を参照してください。

CustomPoller 機能を使用する場合でも、処理が終わったファイルをエクスポート ディレクトリから削除するのはユーザーの責任です。長期の保存にエクスポート ファイルを使用しないでください。設定された最大ディスク容量を超えると、NNMi によって古いファイルが削除され、新しいファイルが作成されます。これらのファイルを別の場所に保存していないと、ファイルは失われます。

カスタム ポーラー収集のエクスポート ディレクトリの変更

NNMi は、ユーザーがエクスポートした収集データを以下のディレクトリに書き込みます。

- *Windows*: `%NNM_DATA%¥shared¥nnm¥databases¥custompoller¥export`
- *UNIX*: `$NNM_DATA/shared/nnm/databases/custompoller/export`

NNMi がカスタム ポーラー ファイルを書き込むディレクトリを変更するには、以下の手順を実行します。

1. 以下のファイルを編集します。
   - *Windows*: `%NNM_PROPS%¥nms-custompoller.properties`
   - *UNIX*: `$NNM_PROPS/nms-custompoller.properties`
2. `exportdir` エントリを特定します。このエントリは以下の行のように記述されています。

   `#!com.hp.nnm.custompoller.exportdir=<base directory to export custom poller metrics>`

   NNMi がカスタム ポーラー収集情報を `C:¥CustomPoller` ディレクトリに書き込むように設定するには、以下のように行を変更します。

   `com.hp.nnm.custompoller.exportdir=C:¥CustomPoller`
3. NNMi 管理サーバーを再起動します。
   a. NNMi 管理サーバーで **`ovstop`** コマンドを実行します。
   b. NNMi 管理サーバーで **`ovstart`** コマンドを実行します。

カスタム ポーラー収集のエクスポートに使用する最大ディスク容量の変更

`collection_name``.csv` ファイルにデータをエクスポートするときに NNMi が使用する最大ディスク容量を変更するには、以下の手順を実行します。

1. 以下のファイルを編集します。
   - *Windows*: `%NNM_PROPS%¥nms-custompoller.properties`
   - *UNIX*: `$NNM_PROPS/nms-custompoller.properties`

2 maxdiskspace エントリを特定します。このエントリは以下の行のように記述されています。

#!com.hp.nnm.custompoller.maxdiskspace=1000

各 *collection_name*.csv ファイルに最大 2,000 MB (2 GB) のストレージ容量を確保するように NNMi を設定するには、その行を以下のように変更します。

#!com.hp.nnm.custompoller.maxdiskspace=2000

3 NNMi 管理サーバーを再起動します。

a NNMi 管理サーバーで **ovstop** コマンドを実行します。

b NNMi 管理サーバーで **ovstart** コマンドを実行します。

カスタム ポーラー メトリックスの累積周期の変更

NNMi は、データをファイルに書き込む前に、カスタム ポーラー収集メトリックスを累積する期間を分単位で設定します。

カスタム ポーラー メトリックスの累積周期を変更するには、以下の手順に従います。

1 以下のファイルを編集します。

- *Windows*: %NNM_PROPS%¥nms-custompoller.properties
- *UNIX*: $NNM_PROPS/nms-custompoller.properties

2 以下のような行を特定します。

#!com.hp.nnm.custompoller.accumulationinterval=5

デフォルト値である 5 分間ではなく 10 分間、メトリックスを収集するように NNMi を設定するには、その行を以下のように変更します。

com.hp.nnm.custompoller.accumulationinterval=10

3 NNMi 管理サーバーを再起動します。

a NNMi 管理サーバーで **ovstop** コマンドを実行します。

b NNMi 管理サーバーで **ovstart** コマンドを実行します。

インシデント アクションの管理

アクションは、インシデントライフサイクルの任意の時点で自動的に実行されるように設定することができます。たとえば、設定しているタイプのインシデントが生成されるときにあるアクションが発生するように設定するとします。詳細については、NNMi ヘルプの「*インシデントのアクションを設定する*」を参照してください。

アクションのパラメータを調整するには、以下のセクションに示す手順に従ってください。

同時アクション数の設定

Solaris NNMi 管理サーバー で同時アクションの数を増加すると、NNMi のパフォーマンスが低下します。

NNMi が実行できる同時アクション数を変更するには、以下の手順に従います。

1 以下のファイルを編集します。

- *Windows*: `%NNM_PROPS%¥shared¥nnmaction.properties`
- *UNIX*: `$NNM_PROPS/shared/nnmaction.properties`

2 以下のような行を特定します。

`#!com.hp.ov.nms.events.action.numProcess=10`

デフォルト値ではなく、20 個の同時アクションを実行できるように NNMi を設定するには、その行を以下のように変更します。

`com.hp.ov.nms.events.action.numProcess=20`

行の始めにある **`#!`** 文字を必ず削除してください。

3 NNMi 管理サーバーを再起動します。

a NNMi 管理サーバーで **`ovstop`** コマンドを実行します。

b NNMi 管理サーバーで **`ovstart`** コマンドを実行します。

Jython アクションのスレッド数の設定

jython スクリプトを実行するためにアクション サーバーが使用するスレッド数を変更するには、以下の手順を実行します。

1 以下のファイルを編集します。

- *Windows*: `%NNM_PROPS%¥shared¥nnmaction.properties`
- *UNIX*: `$NNM_PROPS/shared/nnmaction.properties`

2 以下のような行を探します。

`#!com.hp.ov.nms.events.action.numJythonThreads=10`

デフォルトのスレッド数ではなく、20 個のスレッドで jython スクリプトを実行できるように NNMi を設定するには、その行を以下のように変更します。

`com.hp.ov.nms.events.action.numJythonThreads=20`

行の始めにある **`#!`** 文字を必ず削除してください。

3 NNMi 管理サーバーを再起動します。

a NNMi 管理サーバーで **`ovstop`** コマンドを実行します。

b NNMi 管理サーバーで **`ovstart`** コマンドを実行します。

アクション サーバー名のパラメータの設定

Windows NNMi 管理サーバー でアクション サーバーを実行するユーザー名を変更するには、`HP NNM Action Server` サービスの `LogOn` プロパティを変更します。

アクション サーバーを実行するユーザー名を変更するには、以下の手順を実行します (HP-UX、Solaris、および Linux NNMi 管理サーバーに該当)。

1 以下のファイルを編集します。

   `$NNM_PROPS/shared/nnmaction.properties`

2 以下のような行を特定します。

   `#!com.hp.ov.nms.events.action.userName=bin`

   デフォルト値ではなく、システム がアクション サーバーを実行するように NNMi を設定するには、その行を以下のように変更します。

   `com.hp.ov.nms.events.action.userName=system`

   行の始めにある **`#!`** 文字を必ず削除してください。

3 変更を保存します。

アクション サーバーのキュー サイズを変更する

トラップ ストームへの応答など、高実行率で Long アクション コマンド文字列を使用するアクションの場合、アクション サーバーは多くのメモリを使用する可能性があります。アクション サーバーのパフォーマンスを上げるために、HP ではアクション サーバーで使用可能なメモリ サイズが制限されています。

Solaris NNMi 管理サーバーの場合、NNMi の稼動状態情報でアクション キュー サイズが大きくなっていることが示されると、パフォーマンスを上げるために最大メモリー サイズが削減されます。

これらの制限を変更するには、以下の手順を実行します。

1 以下のファイルを編集します。
   - `%NNM_PROPS%¥shared¥nnmaction.properties`
   - `$NNM_PROPS/shared/nnmaction.properties`

2 以下のような 2 行を探します。

   `com.hp.ov.nms.events.action.jvmargs.minMemsize=-Xms6m`

   `com.hp.ov.nms.events.action.jvmargs.maxMemsize=-Xmx30m`

3 上記のパラメータでは、最小メモリー サイズが 6MB に、最大が 30MB に設定されていることがわかります。これらのパラメータをニーズに合わて調整します。

4 変更を保存します。

5 NNMi 管理サーバーを再起動します。

   a NNMi 管理サーバーで **`ovstop`** コマンドを実行します。

   b NNMi 管理サーバーで **`ovstart`** コマンドを実行します。

trapFilter.conf ファイルによるインシデントのブロック

NNMi 管理サーバーに流れるインシデントの数が一定のレートに達して、新しく到着するインシデントを NNMi がブロックすることになったとします。

これが発生すると、NNMi は `TrapStorm` インシデントを生成し、インシデントがブロックされていることを示します。NNMi は主要なヘルス メッセージも生成し、インシデント レートが高くてインシデントがブロックされていることを示すことがあります。

これを解決するには、`nnmtrapd.conf` ファイルを使用し、インシデントが NNMi に入るのをブロックしてインシデント トラフィックを減らしてみてください。ただし `nnmtrapd.conf` ファイルによる方法を使用すると、NNMi は依然としてこれらのインシデントを使用してトラップ レートを計算し、トラップ バイナリ ストアに書き込みます。`nnmtrapd.conf` ファイルによる方法を使用しても、インシデントがデータベースで作成されたり保存されたりすることを停止することしかできません。詳細については、*nnmtrapd.conf* リファレンス ページまたは UNIX のマンページを参照してください。

この問題を解決する方法には、`nnmtrapd.conf` ファイルを使用する方法より適切な方法があります。NNMi にはフィルタリング メカニズムがあり、NNMi イベント パイプラインで早期にインシデントがブロックされ、このインシデントがトラップ レート計算で分析されること、または NNMi トラップ バイナリ ストアに保存されることが回避されます。デバイスの IP アドレスまたは OID を `trapFilter.conf` ファイルに追加すると、この大量のインシデントをブロックして、インシデントのボリュームの問題を回避できます。詳細については、*trapFilter.conf* リファレンス ページまたは UNIX のマンページを参照してください。

NNMi コンソールとの HTTPS 専用通信を設定する

NNMi コンソールへの HTTP アクセスを防止する最も効果的な方法は、保護されたシステムへの HTTPS アクセスのみを許可するファイアウォールの後ろに NNMi 管理サーバーを配置することです。

HTTP アクセスを防止するファイヤウォール設定により、Web サービスを使用して NNMi と通信し、HTTP のみをサポートする統合で問題が発生することがあります。統合製品のマニュアルを参照し、HTTPS をサポートしているかどうかを確認します。

より安全性に劣る方法では、以下の手順によって、HTTP ポートからの NNMi コンソール アクセス リクエストを HTTPS ポートにリダイレクトします。

1 以下のファイルを編集します。
   - *Windows*: `%NNM_PROPS¥nms-ui.properties`
   - *UNIX*: `$NNM_PROPS/nms-ui.properties`
2 文字列 `https` を検索し、以下の行が含まれるテキスト ブロックを探します。

```
#! com.hp.ov.nms.ui.https.only=false
```

3 以下の行をコメント解除し、以下のように編集します。

```
com.hp.ov.nms.ui.https.only=true
```

4 `ovjboss` を再起動します。

```
ovstop ovjboss
ovstart ovjboss
```

このプロパティを設定して HTTP 要求を NNMi コンソールの HTTPS にリダイレクトすると、NNMi にクロス起動するアプリケーションに問題が発生することがあります。このような問題が発生する場合は、この HTTPS リダイレクトを無効にします。

NNMi 正規化プロパティの変更

NNMi では、ホスト名とノード名の両方が大文字と小文字を区別して保存されます。NNMi コンソール のすべての検索、ソート、およびフィルタの結果も大文字と小文字を区別して返されます。使用する DNS サーバーが、すべて大文字、すべて小文字、大文字と小文字の混合などのように大文字と小文字を区別してさまざまなノード名とホスト名を返す場合、最良の結果が得られない場合があります。

ユーザーの特定のニーズに合うように、NNMi の正規化プロパティを変更できます。NNMi の初期検出シードを行う前に、これらの変更を行うことをお勧めします。HP は、導入中の初期検出を実行する前に、このセクションの設定を調整することを推奨します。

初期検出を実行してから正規化プロパティの変更を行う場合は、完全な検出を開始する **nnmnoderediscover.ovpl -all** スクリプトを実行できます。詳細については、*nnmnoderediscover.ovpl* のリファレンス ページまたは UNIX のマンページを参照してください。

以下のプロパティを変更できます。

- 検出されるノード名を、UPPERCASE、LOWERCASE、または OFF に正規化します。
- 検出されるホスト名を UPPERCASE、LOWERCASE、または OFF に正規化します。

正規化プロパティを変更するには、以下の手順に従います。

1 以下のファイルを編集します。
   - *Windows*: %NNM_PROPS%¥nms-topology.properties
   - *UNIX*: $NNM_PROPS/nms-topology.properties
2 検出される名称を正規化するように NNMi を設定するには、以下のような行を探します。

   #!com.hp.ov.nms.topo.NAME_NORMALIZATION=OFF

   a プロパティをコメント解除します。

   com.hp.ov.nms.topo.NAME_NORMALIZATION=OFF

   プロパティをコメント解除するには、行の先頭から #! 文字を削除します。

   b OFF を LOWERCASE または UPPERCASE に変更します。

   c 変更を保存します。
3 検出されるホスト名を正規化するように NNMi を設定するには、以下のような行を特定します。

   #!com.hp.ov.nms.topo.NAME_NORMALIZATION=OFF

   a プロパティをコメント解除します。

   com.hp.ov.nms.topo.HOSTNAME_NORMALIZATION=OFF

   b OFF を LOWERCASE または UPPERCASE に変更します。

   c 変更を保存します。
4 NNMi 管理サーバーを再起動します。

   a NNMi 管理サーバーで **ovstop** コマンドを実行します。

   b NNMi 管理サーバーで **ovstart** コマンドを実行します。

初期検出後の正規化プロパティの変更

初期検出を実行した後に正規化プロパティを変更すると、NNMi は、次回検出までプロパティ変更との食い違いが続きます。これを解消するには、NNMi 正規化プロパティを変更した後に、**nnmnoderediscover.ovpl -all** スクリプトを実行して完全検出を開始します。

NNMi がフル検出を完了したら、以下の動作が正常に戻ります。以下はすべての例ではなく、NNMi 正規化プロパティを変更する場合に考慮する必要のある項目の一部を挙げています。

同時 SNMP 要求の変更

NNMi では、1 つのノードに対して同時 SNMP 要求が 3 個に制限されています。これにより、ノードの SNMP エージェントが応答をドロップするリスクが減ります。

この値をより高く調整し、検出速度を高めることができます。ただしこの値を高く設定しすぎると、応答がドロップされるリスクが増して、検出精度が落ちます。

この制限を変更する必要がある場合は、以下の手順を実行します。

1 以下のファイルを編集します。
   - *Windows*: `%NNM_PROPS%¥nms-communication.properties`
   - *UNIX*: `$NNM_PROPS/nms-communication.properties`
2 1 つのノードに対する同時 SNMP 要求の現在の数を増やすには、以下を実行します。
   a 以下のような行を特定します。
   `#!com.hp.ov.nms.comm.snmp.maxConcurrentRequests=3`
   b プロパティをコメント解除します。
   `com.hp.ov.nms.comm.snmp.maxConcurrentRequests=3`

   プロパティをコメント解除するには、行の先頭から `#!` 文字を削除します。

   c 1 つのノードに対する同時 SNMP 要求の目的の数に、既存の値を変更します。
   d 変更を保存します。
3 NNMi 管理サーバーを再起動します。
   a NNMi 管理サーバーで **ovstop** コマンドを実行します。

NNMi 管理サーバーで **ovstart** コマンドを実行します。

NNMi 自己監視

NNMi では、メモリ、CPU、ディスク リソースなどの自己監視チェックが実行されます。NNMi 管理サーバーのリソースが少なくなる、または重大な状態が検出されると、NNMi によってインシデントが生成されます。

NNMi の稼動状態情報を表示するには、以下のいずれかの方法を使用します。

- NNMi コンソールで、**[表示] > [システム情報]** をクリックしてから、**[稼動状態]** タブをクリックします。
- 自己監視の詳細レポートについては、**[ツール] > [NNMi システム ヘルス レポート]** を選択します。
- **nnmhealth.ovpl** スクリプトを実行します。

NNMi が自己監視稼動状態の例外を検出すると、NNMi コンソールの下部とフォームの上部にステータス メッセージが表示されます。NNMi 以下の手順を実行すると、この警告メッセージを無効にできます。

1 以下のファイルを編集します。
   - *Windows*: `%NNM_PROPS¥nms-ui.properties`
   - *UNIX*: `$NNM_PROPS/nms-ui.properties`
2 以下の行を含むテキスト ブロックを探します。

   `#!com.hp.nms.ui.health.disablewarning=false`
3 以下の行をコメント解除し、以下のように編集します。

   `com.hp.nms.ui.health.disablewarning==true`
4 `ovjboss` を再起動します。
   a **`ovstop ovjboss`**
   b **`ovstart ovjboss`**

特定ノードの検出プロトコルの使用を抑える

NNMi では複数のプロトコルを使用し、ネットワーク デバイス間のレイヤー 2 接続を検出しています。定義されている検出プロトコルは多数あります。たとえば *Link Layer Discovery Protocol* (LLDP) は業界標準プロトコルですが、Cisco デバイス用の *Cisco Discovery Protocol* (CDP) のように、ベンダー固有のプロトコルも多数あります。

指定したデバイスの検出プロトコル収集を抑制するように NNMi を設定できます。検出プロトコル収集を抑制することで解決できる、特別な状況があります。

以下に例を挙げます。

- *Enterasys デバイス* : SNMP を使用して *Enterasys Discovery Protocol* (EnDP) および LLDP のテーブルから一部の Enterasys デバイスに関する情報を収集すると、NNMi でメモリが不足するという問題が発生することがあります。このようなデバイスで EnDP および LLDP の処理をスキップするように NNMi を設定すると、これを防止できます。これを実行するには、検出プロトコル収集の使用の抑制に示すように、デバイスの管理アドレスを `disco.SkipXdpProcessing` ファイルに追加します。

  一部の Enterasys デバイスの新バージョンのオペレーティング システムでは、**`set snmp timefilter break`** コマンドがサポートされます。このような Enterasys デバイスでは、**`set snmp timefilter break`** コマンドを実行します。このコマンドを使用してデバイスを設定した場合、このデバイスを `disco.SkipXdpProcessing` ファイルにリストする必要はありません。

- *Nortel デバイス* : 多くの Nortel デバイスでは *SynOptics Network Management Protocol* (SONMP) を使用し、レイヤー 2 レイアウトおよび接続を検出します。一部のデバイスでは複数のインタフェースで同一 MAC アドレスを使用するため、このプロトコルで適切に動作しません。相互接続した 2 つの Nortel デバイスがインタフェースの誤ったセット間でレイヤー 2 接続を示し、接続が接続ソース `SONMP` を示す場合、この問題が発生することがあります。
  この例では、SONMP プロトコルを使用しないように NNMi を設定し、デバイスのレイヤー 2 接続を引き出して、誤った接続に関与しているとして表示しないことを推奨します。これを実行するには、検出プロトコル収集の使用の抑制で示すように、2 つのデバイスの管理アドレスを `disco.SkipXdpProcessing` ファイルに追加します。

検出プロトコル収集の使用の抑制

この収集を抑制する必要がある場合は、以下の手順を実行します。

1 以下のファイルを作成します。

- *Windows*: `%NnmDataDir%¥shared¥nnm¥conf¥disco¥disco.SkipXdpProcessing`
- *UNIX*: `$NnmDataDir/shared/nnm/conf/disco/disco.SkipXdpProcessing`

  `disco.SkipXdpProcessing` ファイルでは、大文字と小文字が区別されます。

2 プロトコル収集を抑制するすべてのデバイスで、デバイスの IP アドレスを `disco.SkipXdpProcessing` ファイルに追加します。*disco.SkipXdpProcessing* リファレンス ページ、または UNIX のマンページの指示に従ってください。

3 NNMi 管理サーバーを再起動します。

   a NNMi 管理サーバーで **`ovstop`** コマンドを実行します。

   b NNMi 管理サーバーで **`ovstart`** コマンドを実行します。.

1 つまたは複数のノードの検出プロトコル処理を抑制すると、管理対象ネットワークのレイヤー 2 レイアウトの精度が多少落ちることがあります。HP はこの精度低下の責任を負いません。

`ovjboss` サービスは起動時に `disco.SkipXdpProcessing` ファイルを読み取ります。NNMi の起動後に変更を行った場合は、この手順で示すように NNMi を再起動してください。

Enterasys デバイスで **`set snmp timefilter break`** コマンドを実行した場合は、デバイスのアドレスを `disco.SkipXdpProcessing` ファイルから削除し、この手順で示すように NNMi を再起動します。NNMi は、検出プロトコルを使用したとき、より正確なレイヤー 2 マップを表示します。

詳細については、*disco.SkipXdpProcessing* リファレンス ページまたは UNIX のマンページを参照してください。

NAT 環境における管理アドレスの ICMP ポーリングの管理

このセクションの情報は、HP NNMi 9.0x パッチ 2 の『NNMi デプロイメント リファレンス』公開バージョンには含まれていません。新しい機能を使用する必要のあるお客様と、この情報を共有することができます。

ネットワークアドレス変換 (NAT) 環境では、ファイアウォールにより、NNMi がノードの IP アドレス (プライベート IP アドレス) を使用して NAT ノードと通信することが妨げられます。これを解決するには、NAT アドレス (パブリック IP アドレス) を使用して NNMi と通信します。

NAT 環境では、ノードの管理アドレスが、ノードでホストされる IP アドレスと異なることがあります。NNMi が NAT 環境でノードを検出する場合は、NAT アドレスを検出シードとして NNMi に追加する必要があります。NNMi は、この NAT アドレスがノードの `ipAddressTable` に存在しなくても、それを SNMP 通信に使用します。

*NNMi 9.0x パッチ 2 を適用した後、ノードの SNMP アドレスを ICMP ポーリングするように、新しい NNMi 機能を設定できます。*そのように設定すると、分析の信頼性と正確性がより高まります。この機能を使用することにより、誤ったノード停止インシデントが回避され、根本原因分析がより正確に行われるようになります。

NAT 環境における管理アドレスの ICMP ポーリングの有効化

NAT環境で管理アドレスのICMPポーリングを有効にするには、以下の手順を実行します。

1 ［ICMP 管理アドレス ポーリング ］を有効にします。NNMi ヘルプの「デフォルトのモニタリング」を参照します。

2 以下のように、システムプロパティを設定します。

   a ディレクトリを次のように変更します。

      Windows: `%NNM_PROPS%`

      UNIX: `$NNM_PROPS`

   b 次のプロパティファイルを作成します: *mypropertyfile*.properties。*mypropertyfile* の代わりに任意のファイル名を使用します。ただし、.properties ファイル拡張子を使用する必要があります。

   c *mypropertyfile*.properties ファイルに、以下の行を追加します。

```
com.hp.ov.nnm.useSnmpAgentManagementAddressState = true
```

   d NNMi 管理サーバーを再起動します。

```
ovstop -c
ovstart -c
```

SNMP エージェントに対して **[アクション] -> [モニタリングの設定]** を実行した後に NNMi が表示する情報が表示されます。表示される情報に、NNMi が管理アドレスのポーリングを有効にしているかどうかが示されます。

NNMi に対する変更点

368 ページの「NAT 環境における管理アドレスの ICMP ポーリングの有効化」に示されている手順を実行すると、NNMi は以下のように変更されます。

- [エージェント ICMP 状態] フィールドが、以下のフォームに表示されます。
  - [ノード] フォーム
  - [SNMP エージェント] フォーム
  - [SNMP エージェント] テーブル ビュー
- NNMi は、管理アドレス ICMP 状態の表示場所を変更します。NNMi は、SNMP エージェント ステータスの判断方法も変更します。

表 33 に、エージェント ICMP および IP アドレス状態のポーリングアクションを示します。NNMi は、ICMP 管理アドレスポーリング設定および ICMP 障害ポーリング設定に応じて、これらのアクションを実行します。表 33 の影付きの先頭行はデフォルト設定を示します。

表 31

ICMP 管理アドレス ポーリング	ICMP 障害ポーリング	エージェント ICMP 状態	IP アドレス状態
有効	無効	ポーリング	ポーリングなし

表 31

ICMP 管理アドレス ポーリング	ICMP 障害ポーリング	エージェント ICMP 状態	IP アドレス状態
有効	有効	ポーリング	ポーリング
無効	無効	ポーリングなし	ポーリングなし
無効	有効	ポーリングなし	ポーリング

表 34に、SNMPエージェントとICMPの応答に合わせてAPAによって決定されるSNMPエージェントステータスに対する変更点を示します。

表 32

応答	応答	正常域
応答	無応答	警戒域
無応答	応答	危険域
無応答	無応答	危険域

管理アドレスの ICMP ポーリングを有効にすると、APA は、結果の生成とインシデントの生成時に、管理アドレス ICMP の応答と SNMP エージェントの応答を考慮するようになります。

大規模スイッチの VLAN インデックス付けの使用を抑制する

NNMi が管理対象ネットワークのスイッチ デバイス間でレイヤー 2 接続を認識する方法の 1 つは、`dot1dTpFdbTable` (FDB) をスイッチから取得することです。ただし Cisco スイッチの場合、NNMi は `VLAN-indexing` 方法を使用して FDB 全体を取得する必要があります。各デバイスで設定されている VLAN の数が多い場合、`VLAN-indexing` による FDB の取得の完了には数時間かかることがあります。

Cisco スイッチは、多くの場合、Cisco Discovery Protocol (CDP) を使用するように設定されています。CDP は、レイヤー 2 接続を認識するための優れた方法であるとみなされています。ネットワークのコアに配置されている大規模スイッチには、多くの VLAN が含まれていることがあります。このスイッチには一般的に、直接接続されているエンドノードがありません。管理するスイッチに直接接続されているエンド ノードがない場合は、この大規模スイッチで FDB の収集を抑制するとよいでしょう。NNMi は、CDP から収集したデータを使用してレイヤー 2 検出を完了します。この大規模スイッチは、`VLAN-indexing` の抑制の主な候補となります。多くのエンド ノードが接続している、ネットワークのエッジにある小規模スイッチ (アクセス スイッチと呼ばれる) では、`VLAN-indexing` を抑制しないでください。

`VLAN-indexing` を抑制するように NNMi を設定できます。これを実行するには、370 ページの「VLAN インデックス付けの使用を抑制する」で示すように、NNMi 管理者が大規模スイッチの管理アドレスまたはアドレス範囲を作成して `disco.NoVLANIndexing` ファイルに追加する必要があります。`ovjboss` サービスは起動時に `disco.NoVLANIndexing` ファイルを読み取ります。`ovjboss` サービスの起動後、NNMi 管理者が `disco.NoVLANIndexing` ファイルを変更した場合、その変更内容は、`ovjboss` サービスを次回起動するまで有効になりません。デフォルトでは、`disco.NoVLANIndexing`

ファイルは存在しません。disco.NoVLANIndexing が存在しない場合、この機能は無効になり、NNMi は VLAN-indexing を使用して、すべてのデバイスで FDB テーブル全体を収集しようとします。

VLAN インデックス付けの使用を抑制する

この vlan-indexing を無効にする必要がある場合は、以下の手順を実行します。

1 以下のファイルを作成します。
   - *Windows*: %NnmDataDir%¥shared¥nnm¥conf¥disco¥disco.NoVLANIndexing
   - *UNIX*: $NnmDataDir/shared/nnm/conf/disco/disco.NoVLANIndexing

     disco.NoVLANIndexing ファイルでは、大文字と小文字が区別されます。
2 vlan-indexing を無効にするすべてのデバイスの IP アドレスまたはアドレス範囲を disco.NoVLANIndexing ファイルに追加します。*disco.NoVLANIndexing* リファレンス ページ、または UNIX のマンページの指示に従ってください。
3 NNMi 管理サーバーを再起動します。
   a NNMi 管理サーバーで **ovstop** コマンドを実行します。
   b NNMi 管理サーバーで **ovstart** コマンドを実行します。

1 つまたは複数のノードの vlan-indexing を抑制すると、管理対象ネットワークのレイヤー 2 レイアウトの精度が多少落ちることがあります。HP はこの精度低下の責任を負いません。

ovjboss サービスは起動時に disco.NoVLANIndexing ファイルを読み取ります。NNMi の起動後に変更を行った場合は、この手順で示すように NNMi を再起動してください。

詳細については、*disco.Disco.NoVLANIndexing* リファレンス ページまたは UNIX のマンページを参照してください。

NAT 環境における管理アドレスの ICMP ポーリングの概要

ネットワーク アドレス変換 (NAT) 環境では、ファイアウォールにより、NNMi がノードの IP アドレス (プライベート IP アドレス) を使用して NAT ノードとやり取りすることがブロックされます。これを解決するには、NNMi で NAT アドレス (パブリック IP アドレス) を使用して NNMi とやり取りします。

NAT 環境では、ノードの管理アドレスが、ノードでホストされる IP アドレスと異なることがあります。NNMi が NAT 環境でノードを検出する場合は、NAT アドレスを検出シードとして NNMi に追加する必要があります。NNMi は、この NAT アドレスがノードの `ipAddressTable` に存在しなくても、それを SNMP 通信に使用します。

NNMi はこの機能を提供することで、誤ったノード停止中インシデントの生成を回避し、根本原因分析をより正確にします。

NAT 環境の管理アドレスの ICMP ポーリング

NNMi では、NAT 環境に存在するノードも含めてすべてのノードの ICMP 管理アドレスポーリングが自動的に有効になります。NNMi は NAT 環境で以下のように機能します。

- [管理アドレスの状態] フィールドが以下のフォームに表示されます。
  - [ノード] フォーム
  - [SNMP エージェント] フォーム
  - [SNMP エージェント] テーブル ビュー
- NNMi は、管理アドレス ICMP 状態の表示場所を変更します。NNMi は、SNMP エージェント ステータスの判断方法も変更します。

表 33 に、管理アドレス ICMP および IP アドレスの状態ポーリング アクションを示します。NNMi は ICMP 管理アドレス ポーリング設定および ICMP 障害ポーリング設定にこれを実行します。表 33 の影付きの先頭行はデフォルト設定を示します。

表 33　ICMP 設定および結果の状態ポーリング

ICMP 管理アドレス ポーリング	ICMP 障害ポーリング	管理 ICMP アドレス状態	IP アドレス状態
有効	無効	ポーリング	ポーリングなし
有効	有効	ポーリング	ポーリング
無効	無効	ポーリングなし	ポーリングなし
無効	有効	ポーリングなし	ポーリング

表 34 には、SNMP エージェントと ICMP の応答のために APA が判断する SNMP エージェント ステータス、および生成されるインシデントの変化を示します。管理アドレスの ICMP ポーリングにより、APA は、結論とインシデントの生成時に、管理アドレス ICMP 応答と SNMP エージェント応答を考慮します。

表 34　SNMP エージェント ステータスの判断および生成されるインシデント

SNMP エージェント応答	管理アドレス ICMP 応答	SNMP エージェントステータス	生成されるインシデント
応答	応答	正常域	なし
応答	無応答	警戒域	その他のネットワークの問題により、次の 2 つの可能性があります。 - なし - `AddressNotResponding`
無応答	応答	危険域	- `SNMPAgentNotResponding`
無応答	無応答	危険域	その他のネットワークの問題により、次の 2 つの可能性があります。 - なし - `NodeDown`

NNMi ロギング

NNMi ログ ファイル

HP Network Node Manager i Software (NNMi) のパフォーマンスを調べる、または NNMi のプロセスとサービスがどのように動作しているかを観察するには、プロセスとサービス アクティビティの履歴を表示するログ ファイルを確認できます。これらのファイルは、以下の場所にあります。

- *Windows*: `%NnmDataDir%¥log¥nnm¥`
- *UNIX*: `$NnmDataDir/log/nnm`

NNMi では、*name*`.%g.%u.log` という形式でログ ファイルが保存されます。

- *name* はログ ファイルのベース名であり、多くの NNMi 機能では `nnm` になります。
- `%g` はアーカイブ済みログ ファイルに関連します。ログ ファイル名の `%g` の部分が ゼロ (0) であるとき、NNMi は *name*`.0.%u.log` ファイルにアクティブに記録しています。*name*`.0.%u.log.lck` ファイルも確認してください。
- ログセッション中に親 ovjboss が失敗しない限り、%u は通常ゼロ (0) です。

ログ ファイルは、以下のいずれかの場合にアーカイブされる可能性があります。

- ovjboss プロセスが再起動される。
- ログ ファイルのサイズが設定した制限を超える。

ovjboss が再起動されるか、ログ ファイルのサイズが設定済み制限を超えると、最後のアクティブなログ ファイルはアーカイブされます。たとえばファイル `nnm.0.0.log` は、ファイル `nnm.1.0.log` としてアーカイブされます。次に NNMi は、新しい `nnm.0.0.log` ファイルにロギングを開始します。

NNMi では、以下のロギング レベルでメッセージがログに記録されます。

- SEVERE: NNMi の異常動作に関連するイベント。
- WARNING: 潜在的な問題を示すイベント、および SEVERE ロギング レベルに含まれるすべてのメッセージ。
- INFO: NNMi コンソール (またはそれと同等のもの) 書き込まれるメッセージ、および WARNING ロギング レベルに含まれるすべてのメッセージ。
- CONFIG: 静的な設定情報、および INFO ロギング レベルに含まれるすべてのメッセージ。

ログ ファイルのプロパティ

`logging.properties` ファイルの NNMi ログ ファイル ハンドラの `.limit` プロパティを調整し、サービスごとにログ ファイルのサイズを制御できます。`logging.properties` ファイルの NNMi ログ ファイル ハンドラの `.count` プロパティを調整し、アーカイブ済みファイルの数を制御することもできます。

`logging.properties` ファイルは以下の場所に保存されています。

- *Windows*: `%NnmDataDir%¥shared¥nnm¥conf¥ovjboss`
- *UNIX*: `$NnmDataDir/shared/nnm/conf/ovjboss`

ロギングの詳細については、*logging.properties* のリファレンス ページまたは UNIX のマンページを参照してください。

ロギング ファイルのプロパティの変更

以下のロギング パラメータを調整し、NNMi ログ ファイルの数とサイズを設定できます。

- `.count`
- `.limit`

たとえば、`nnm.%g.%u.log` ファイルを少なくして、サイズを大きくするには、以下の手順を実行します。

1. `logging.properties` ファイルをバックアップしてから、そのファイルを任意のテキスト エディタで開きます。
2. 以下の行を変更し、ログ ファイルの数を 10 に減らします。

   ```
   com.hp.ov.nms.admin.log.NnmMainFileHandler.count = 20
   ```

   以下のように変更します。

   ```
   com.hp.ov.nms.admin.log.NnmMainFileHandler.count = 10
   ```

3. 以下の行を変更し、検出プロセスのログ済み情報の量を増加します。

   ```
   com.hp.ov.nms.admin.log.NnmMainFileHandler.limit = 50000000
   ```

   以下のように変更します。

   ```
   com.hp.ov.nms.admin.log.NnmMainFileHandler.limit = 100000000
   ```

4 以下のコマンドを実行して ovjboss を再開します。

a **ovstop ovjboss**

b **ovstart ovjboss**

nnmrereadlogging.ovpl コマンドを NNMi サポート ディレクトリで実行することもできます。

- *Windows*: %NnmInstallDir%¥support
- *UNIX*: $NnmInstallDir/support

ファイル管理

ログ ファイルは大きくなり続けるため、%NnmDataDir%¥log¥nnm (Windows) または $NnmDataDir/log/nnm (UNIX) で定期的に監視してください。大きなアーカイブ ファイルは削除してください。

NNMi 管理サーバーの変更

他のシステムで HP Network Node Manager i Software (NNMi) 設定を複製できます。たとえば、テスト環境から生産環境に移動したり、NNMi 管理サーバーのハードウェアを変更したりできます。

NNMi 設定に影響を及ぼさずに、NNMi 管理サーバーの IP アドレスを変更できます。

この章には、以下のトピックがあります。

- NNMi 設定移動の準備のベストプラクティス
- NNMi 設定および組み込みデータベースの移動
- NNMi 設定の移動
- NNMi パブリック キー証明書のリストア
- スタンドアロン NNMi 管理サーバーの IP アドレスを変更する
- NNMi 管理サーバーのホスト名またはドメイン名の変更
- Oracle データベース インスタンス接続情報の変更
- NNMi が Oracle データベース インスタンスへの接続に使用するパスワードを変更する

NNMi 設定移動の準備のベストプラクティス

次のベストプラクティスは、NNMi 設定の異なるシステムへの移動に適用されます。

- ノード グループ設定が管理対象ノードの識別にホスト名を使っている場合、製品およびテストの NNMi 管理サーバーは同じ DNS サーバーを使う必要があります。製造システムとテスト システムが異なる DNS サーバーを使っている場合、管理対象ノードの解決済みの名前を変更すると、2 つの NNMi 管理サーバーの間でポーリング設定が異なる結果になることがあります。
- 設定エクスポートを 1 人の作成者に制限できます。 自分のグループまたは会社に一意の新しい作成者値を作成します。次のアイテムを作成または変更するときに、この作成者の値を指定します。
  - デバイス プロファイル
  - インシデントの設定
  - URL アクション
- スマート プラグイン (iSPIs) をインストールする場合は、NNMi との統合セクションの該当する章を参照してください。

NNMi 設定および組み込みデータベースの移動

NNMi の設定と組み込みデータベースを、たとえばテスト システムから本番システムなどへ移動するには、ソース (テスト) システム上のすべての NNMi データをバックアップしてから、バックアップをターゲット (本稼働) システムにリストアします。バックアップの実行後 NNMi データベースに対する変更が何も行われないようにするため、すべての NNMi プロセスを停止し、オフライン バックアップを作成してください。たとえば、以下のようにします。

```
nnmbackup.ovpl -type offline -scope all ¥
-target nnmi_backups¥offline
```

353 ページの「異なるシステムでのリストア」にリストされた要件が新規システム上で満たされることを確認してから、以下の例のようなコマンドを実行します。

```
nnmrestore.ovpl -source nnmi_backups¥offline¥newest_backup
```

NNMi は同じ SSL 証明書を使用して、データベース (組み込みまたは外部) へのアクセス、および NNMi コンソールへの HTTPS アクセスをサポートします。データベースへアクセスするための証明書は、ソース システム上で NNMi プロセスを最初に開始したときに作成されました。この証明書はバックアップおよびリストア データに含まれています。この証明書がないと、NNMi はターゲット システムからデータベースにアクセスできません。

ただし、NNMi コンソールへの HTTPS アクセスの場合は、SSL 証明書をターゲット システムに生成する必要があります。jboss の現在の実装が証明書のマージをサポートしていないため、NNMi は別のシステムからのデータをリストアして設定されたシステム上での NNMi コンソールへの HTTPS アクセスはサポートしていません。ターゲット システムが NNMi コンソールへの HTTPS アクセスをサポートする必要がある場合は、379 ページの「NNMi 設定の移動」の手順を実行してから、ターゲット システム上で新たにデータ収集を開始します。

NNMi 設定の移動

nnmconfigexport.ovpl コマンドを使用して、NNMi 設定を XML ファイルに出力します。次に、nnmconfigimport.ovpl コマンドを使って、XML ファイルから新しいシステムの NNMi にこの設定をインポートします。

nnmconfigimport.ovpl スクリプトを使用してファイルをインポートする前に、nnmconfigexport.ovpl スクリプトでエクスポートしたファイルを編集しないでください。

これらのコマンドの詳細については、該当するリファレンス ページ、または UNIX のマンページを参照してください。

nnmconfigexport.ovpl コマンドでは SNMPv3 資格情報は保持されません。詳細については、*nnmconfigexport.ovpl* リファレンス ページ、または UNIX のマンページを参照してください。

NNMi 設定のみを移動できます。HP は、ある NNMi 管理サーバーから異なる NNMi 管理サーバーへのトポロジまたはインシデント データの移動をサポートしません。また、HP は、NNM iSPI Performance for Metrics 用に収集されたパフォーマンス データのような iSPI データの移動をサポートしません。

NNMi パブリック キー証明書のリストア

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関与、または高可用性 (HA) クラスタのメンバーの場合は、サポート担当者に問い合わせてください。

nnm.keystore ファイルには NNMi が暗号化に使用するパブリック キー証明書が格納されます。NNMi のインストール プロセスで nnm.keystore ファイルが作成され、このファイルの証明書が NNMi データベースの nms_sec_key レコード (Postgres または Oracle) にリンクされます。

NNMi が後でアンインストールされるが、再インストールする前に NNMi の Oracle ユーザーおよびデータベースが削除されていない場合 (Oracle ユーザーのカスケード削除)、nms_sec_key エントリは新規に作成される nnm.keystore ファイルに対して有効ではありません。

NNMi パブリック キー証明書をリストアするには、以下のタスクを実行します。

- タスク 1: KeyManager サービスのステータスを決定する
- タスク 2: 現在の nnm.keystore ファイルをバックアップする
- タスク 3: 元の nnm.keystore ファイルを検索する
- タスク 4: 可能な場合、元の nnm.keystore ファイルをリストアする

タスク 1: KeyManager サービスのステータスを決定する

1. 以下のコマンドを実行します。

   ```
   ovstatus -v ovjboss
   ```

2. コマンド出力で、KeyManager サービスが実行中でないことを確認します。これは、通常、nnm.keystore ファイルが壊れている、またはないことを示します。

   ovstatus 出力で KeyManager サービスが開始されていることが示される場合は、サポート担当者に問い合わせてください。

タスク 2: 現在の nnm.keystore ファイルをバックアップする

1 NNMi トラストストアが格納されているディレクトリに変更します。

- *Windows*: `%NnmDataDir%¥shared¥nnm¥certificates`
- *UNIX*: `$NnmDataDir/shared/nnm/certificates`

2 バックアップ用に、以下のファイルのコピーを保存します。

- `nnm.keystore`
- `nnm.truststore`

タスク 3: 元の nnm.keystore ファイルを検索する

1 NNMi データベースのセキュリティ キーのフィンガープリントを決定します。

- 組み込み Postgres データベースの場合は、以下を入力します。
  - *Windows*:
    %NnmInstallDir%¥nonOV¥Postgres¥bin¥psql -U postgres ¥
    -d nnm -c "*<database_command>*"
  - *UNIX*:
    $NnmInstallDir/nonOV/Postgres/bin/psql -U postgres ¥
    -d nnm -c "*<database_command>*"

  <database_command> を以下の SQL コマンド文字列に置き換えます。

  select fingerprint from nms_sec_key;

- Oracle データベースの場合は、Oracle データベース管理者に *<database_command>* (この手順のはじめに組み込みデータベースに説明) を適切な Oracle 管理ツールで実行するよう依頼します。

コマンド結果は単一データベース行にする必要があります。正しい nnm.keystore ファイルには、このフィンガープリントも含まれます。

2 テストするバックアップ nnm.keystore ファイルを確認します。

このファイルは、元のインストール ディレクトリの NNMi 管理サーバーのバックアップ内に置くことができます。

3 バックアップ nnm.keystore ファイルのフィンガープリントをテストします。

a NNMi 証明書が含まれるディレクトリを変更します。
  - *Windows*: `%NnmDataDir%¥shared¥nnm¥certificates`
  - *UNIX*: `$NnmDataDir/shared/nnm/certificates`

b キー ストアの内容を確認します。
  - *Windows*:
    %NnmInstallDir%¥nonOV¥jdk¥b¥bin¥keytool -list ¥
    -keystore nnm.keystore
  - *UNIX*:
    $NnmInstallDir/nonOV/jdk/b/bin/keytool -list ¥
    -keystore nnm.keystore

  キー ストアのパスワードの入力を求められたら、**nnmkeypass** と入力します。

キー ストアの出力形式は以下のとおりです。

```
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entry
selfsigned, Oct 28, 2008, keyEntry,
Certificate fingerprint (MD5):
29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
```

c この nnm.keystore ファイルの MD5 フィンガープリントの値と NNMi データベース (このタスクの 手順 1) のフィンガープリントを比較します。

— フィンガープリントが完全一致する場合は、この NNMi データベースの正しい nnm.keystore ファイルを検索したことになります。タスク 4: 可能な場合、元の nnm.keystore ファイルをリストアする を継続します。

— フィンガープリントが完全一致しない場合は、タスク 3: 元の nnm.keystore ファイルを検索する を繰り返します。

上記の手順で元の nnm.keystore ファイルを検索できない場合は、サポート担当者に連絡してください。タスク 4: 可能な場合、元の nnm.keystore ファイルをリストアする は続行しないでください。

タスク 4: 可能な場合、元の nnm.keystore ファイルをリストアする

正しい nnm.keystore ファイルを検索できた場合は、以下の手順に従ってそのファイルをリストアします。

1 ovjboss プロセスを停止します。

```
ovstop ovjboss
```

2 既存のファイルの上部にある nnm.keystore ファイルを以下の場所にコピーします。

- *Windows*: `%NnmDataDir%¥shared¥nnm¥certificates`
- *UNIX*: `$NnmDataDir/shared/nnm/certificates`

3 ovjboss プロセスを起動します。

```
ovstart ovjboss
```

4 以下のコマンドを実行します。

```
ovstatus -v ovjboss
```

5 コマンド出力で、KeyManager サービスが起動されていることを確認します。

NNMi が正しく動作していることを確認したら、nnm.keystore ファイルのバックアップ コピーを タスク 2: 現在の nnm.keystore ファイルをバックアップする から削除できます。

スタンドアロン NNMi 管理サーバーの IP アドレスを変更する

NNMi 管理サーバーの IP アドレスを変更するには、以下の手順に従います。

1 **http://www.webware.hp.com** にアクセスします。

2 **[ライセンスの管理]** をクリックします。

3 ログインしてから手順に従って新規ライセンスを取得し、削除プロセスを完了します。

4 NNMi 管理サーバーを新しい IP アドレスで設定します。

5 NNMi 管理サーバーの新規 IP アドレスを認識するように DNS サーバーを設定します。

6 NNMi 管理サーバーを再起動します。

7 コマンドプロンプトで、以下のコマンドを入力します。

```
nnmlicense.ovpl NNM -g
```

8 **[Autopass: ライセンス管理]** ダイアログ ボックスで、**[ライセンス キーの削除]** をクリックします。

9 削除するライセンス キーを選択します。

10 **[ライセンスを恒久的に削除]** を選択します。

11 **[削除]** をクリックしてから、ダイアログボックスを閉じます。

12 手順 3 で取得した新しいライセンス キーを `license.txt` という名前のテキスト ファイルにコピーします。

13 コマンドプロンプトで、以下のコマンドを入力します。

```
nnmlicense.ovpl NNM -f license.txt
```

ライセンスの考慮事項

NNMi ライセンス キーの取得とインストールの詳細については、115 ページの「NNMi ライセンスの取得」を参照してください。

NNMi 管理サーバーのホスト名またはドメイン名の変更

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関与、または高可用性 (HA) クラスタのメンバーの場合は、サポート担当者に問い合わせてください。

NNMi 管理サーバーのホスト名、ドメイン名、またはその両方を変更するには、以下のタスクを実行します。

- タスク 1: システムの準備
- タスク 2: 新規 NNMi パブリック キー証明書の作成
- タスク 3: NNMi 管理サーバーの完全修飾ドメイン名を変更する
- タスク 4: 新しい証明書で HTTPS 設定を更新する
- タスク 5: システムの再起動、更新、およびリフレッシュ
- タスク 6: NNMi のバックアップ

タスク 1: システムの準備

1 標準手順に従って、NNMi バックアップを完了します。

NNMi 管理サーバー名を変更する前に、このバックアップに明確なラベルを付けます。

2 システム名を変更します。

必要に応じて、システムを再起動します。ovjboss プロセスを完全に起動できない場合があります。

3 NNMi の IP アドレスも変更している場合は、382 ページの「スタンドアロン NNMi 管理サーバーの IP アドレスを変更する」の手順を完了します。

4 ovjboss を停止します。

```
ovstop ovjboss
```

5 NNMi 証明書が含まれるディレクトリを変更します。

- *Windows*: `%NnmDataDir%¥shared¥nnm¥certificates`
- *UNIX*: `$NnmDataDir/shared/nnm/certificates`

6 バックアップ用に、以下のファイルのコピーを保存します。

- `nnm.keystore`
- `nnm.truststore`

タスク 2: 新規 NNMi パブリック キー証明書の作成

この NNMi 管理サーバーの新規証明書を nnm.keystore ファイルに作成します。次回 ovjboss プロセスが正常に起動すると、NNMi によって新規証明書を使用するデータベースへのアクセスが更新されます。

1 NNMi 証明書が含まれるディレクトリを変更します。

- *Windows*: `%NnmDataDir%¥shared¥nnm¥certificates`
- *UNIX*: `$NnmDataDir/shared/nnm/certificates`

certificates ディレクトリから、この手順のコマンドすべてを実行します。

2 以下のコマンドを実行し、キーストアに新規パブリック / プライベート キー ペア (証明書) を生成します。

- *Windows*:
```
%NnmInstallDir%¥nonOV¥jdk¥b¥bin¥keytool -genkey ¥
-alias "<unique_alias>" -keyalg rsa
-dname "cn=<hostname>, dc=<domain_name_by_parts>" ¥
-keypass "nnmkeypass" -validity 36500 ¥
-keystore nnm.keystore -storepass "nnmkeypass"
```
- *UNIX*:
```
$NnmInstallDir/nonOV/jdk/b/bin/keytool -genkey ¥
-alias "<unique_alias>" -keyalg rsa
-dname "cn=<hostname>, dc=<domain_name_by_parts>" ¥
-keypass "nnmkeypass" -validity 36500 ¥
-keystore nnm.keystore -storepass "nnmkeypass"
```

<alias> を NNMi 管理サーバーの新規ホスト名などの一意値 (例 : newnnmi) に置き換えます。

<hostname> を NNMi 管理サーバーの新規完全修飾ドメイン名 (例 : newnnmi.servers.example.com) に置き換えます。

dc=*<domain_name_by_parts>* を NNMi 管理サーバーがある新規ドメインの各コンポーネントに置き換えます。たとえば、NNMi 管理サーバー newnnmi.servers.example.com の場合は、以下を指定します。
dc=servers, dc=example, dc=com

keytool コマンドの詳細については、**java.sun.com** で「鍵および証明書管理ツール」を検索してください。

タスク 3: NNMi 管理サーバーの完全修飾ドメイン名を変更する

NNMi で NNMi 管理サーバーの新規完全修飾ドメイン名を使用するように設定するには、nnmsetofficialfqdn.ovpl コマンドを使用します。たとえば、以下のようにします。

```
nnmsetofficialfqdn.ovpl newnnmi.servers.example.com
```

詳細については、*nnmsetofficialfqdn.ovpl* リファレンス ページ、または UNIX のマンページを参照してください。

タスク 4: 新しい証明書で HTTPS 設定を更新する

以下のファイルを編集して Tomcat サーバーを設定します。

```
$jboss.home.dir/server/nms/deploy/jboss-web.deployer/server.xml
```

`$jboss.home.dir` のデフォルト値は次のとおりです。

- *Windows*: `%NnmInstallDir%¥nonOV¥jboss¥nms`
- *UNIX*: `$NnmInstallDir/nonOV/jboss/nms`

NNMi Web サーバーで HTTPS プロトコルを使用する場合は、以下の手順に従って HTTPS 設定を更新します。

1. 任意のテキスト エディタで `server.xml` ファイルを開きます。
2. コメント解除された HTTPS コネクタでは、タスク 2: 新規 NNMi パブリック キー証明書の作成 の新規証明書に使用した別名値に一致するように `keyAlias` パラメータの値を変更します。
3. `server.xml` ファイルを保存します。

`server.xml` ファイルの詳細および HTTPS コネクタ ブロックの例については、86 ページの「server.xml ファイルの更新」を参照してください。

タスク 5: システムの再起動、更新、およびリフレッシュ

1. ovjboss を起動します。

   `ovstart ovjboss`

2. NNMi 管理サーバーの新規完全修飾ドメイン名を使用するように、NNMi 管理サーバーと専用サーバー上で実行中の任意の NNM iSPI 間の接続を更新します。
3. NNMi 管理サーバーの新規完全修飾ドメイン名を使用するように、NNMi 管理サーバーと任意の統合アプリケーション間の接続を更新します。

   必要に応じて、新規 NNMi 証明書を信頼するように統合アプリケーションのシングル サインオン設定を更新します。
4. NNMi データベースに暗号化データ (SNMPv3 パスフレーズなど) が含まれる場合、このデータは旧セキュリティ キーで暗号化されています。そのデータは新規セキュリティ キーで解読できません。これらの設定項目の削除および再作成については、サポート担当者に連絡してください。

タスク 6: NNMi のバックアップ

標準手順に従って、NNMi バックアップを完了します。

NNMi 管理サーバーの名前を変更する前に作成されたバックアップから NNMi をリストアすると、nnm.keystore ファイルが上書きされるため、NNMi データベースにアクセスできなくなります。旧バックアップから NNMi データをリストアする必要がある場合は、サポート担当者に連絡してください。

Oracle データベース インスタンス接続情報の変更

NNMi が一度に接続できる Oracle データベース インスタンスは 1 つです。この接続を設定できます。

以下のような場合に Oracle データベース インスタンス接続情報を変更します。

- Oracle データベースのサーバー名を変更する必要がある。
- データベースへ接続するポートが別のプロセスと競合している、または企業ポリシーでデフォルト以外のポートを使用する必要がある。
- データベース インスタンス名を変更する必要がある (たとえば、企業ポリシーに準拠するため)。
- Oracle データベース サーバーのハードウェアを変更する必要がある。

NNMi で使用する Oracle データベース インスタンスを変更するには、以下のタスクを実行します。

- タスク 1: Oracle データベース インスタンスの更新
- タスク 2: NNMi 設定の更新

タスク 1: Oracle データベース インスタンスの更新

1. ovjboss を停止します。

   ovstop ovjboss

2. データベースを移動、Oracle データベース サーバー名を変更、またはその他の必要な変更を行って Oracle データベースを準備します。
3. ターゲットの Oracle データベース インスタンスが、以下の前提条件を満たしていることを確認します。
   - データベース インスタンスが存在している。
   - データベース インスタンスに正しい NNMi データが入力されている。

     Oracle ツールを使用して、NNMi データを作業用データベース インスタンスからターゲットのデータベース インスタンスにコピーします。
   - データベース インスタンスを実行中である。

タスク 2: NNMi 設定の更新

1. データベース接続設定ファイルのバックアップ
   a. ディレクトリを次のように変更します。
      — *Windows*: `%NnmInstallDir%¥nonOV¥jboss¥nms¥server¥nms¥`
      — *UNIX*: `$NnmInstallDir/nonOV/jboss/nms/server/nms/`
   b. `nms` ディレクトリ内に、`deploy.save` というディレクトリを作成します。
   c. `nms-ds.xml` ファイルを `deploy` ディレクトリから `deploy.save` ディレクトリにコピーします。

   最初に、`ovjboss` プロセスでは `deploy` ディレクトリ階層内のすべてのファイルが読み取られます。そのため、`deploy.save` ディレクトリの場合と同様、`deploy` ディレクトリ階層外の場所に展開されたファイルのバックアップ コピーを保存します。

2. データベース接続設定ファイルの編集
   a. `deploy` ディレクトリに移動します。

b 任意のテキスト エディタで、nms-ds.xml ファイルを開きます。

c connection-url エントリを検索します。

たとえば、以下のようにします。

```
<connection-url>jdbc:oracle:thin:@ohost:1521:nnmidb1</connection-url>
```

このエントリの最後の 3 つのパラメータが重要です。これらのパラメータの形式は oracle_hostname:database_port:database_instance_name です。

d connection-url エントリの 4 番目、5 番目、または 6 番目のパラメータの 1 つ以上を変更します。

たとえば、以下のようにします。

— 異なる Oracle データベース サーバーを指すには、ohost を別のホスト名に変更します。

— 別のポートの Oracle データベース サーバーに接続するには、1521 を別のポート番号に変更します。

— 別の Oracle データベース インスタンスに接続するには、nnmidb1 を別のデータベース インスタンス名に変更します。(このデータベース インスタンスはすでに存在している必要があります。)

e nms-ds.xml ファイルを保存します。

3 ovjboss を起動します。

```
ovstart ovjboss
```

NNMi が Oracle データベース インスタンスへの接続に使用するパスワードを変更する

NNMi データベース インスタンスへの接続に異なるパスワードを使用するように Oracle 設定を変更するには、以下の手順に従って NNMi 設定を更新します。

1 NNMi をシャットダウンします。

```
ovstop
```

2 nnmchangedbpw.ovpl コマンドを実行し、プロンプトに従います。

3 NNMi を起動します。

```
ovstart
```

詳細については、*nnmchangedbpw.ovpl* リファレンス ページ、または UNIX のマンページを参照してください。

Xen 仮想化環境での NNMi の実行

Xen は Linux 用のオープン ソースの仮想化環境です。Xen には、Windows や Linux などのオペレーティング システムを実行する仮想マシンを作成できる低レベルのハイパーバイザが用意されています。 また、スナップショットなどの VMWare と同様の他の機能も提供されます。

NNMi をインストールする前に Xen がすでに存在する場合、NNMi のインストールプロセスで Xen 仮想インタフェースに関する問題が自動的に解決されます。

この章には、以下のトピックがあります。

- Xen をインストールした後の NNMi 管理サーバーの動作に関する問題

Xen をインストールした後の NNMi 管理サーバーの動作に関する問題

NNMi 9.10 をサーバーにインストールして、運用環境で NNMi が正常に動作しているとします。この NNMi 管理サーバーに Xen をインストールすると、Xen によって NNMi 管理サーバーのネットワーク ルーティング テーブルが変更され、ループバック アドレスへのパケットを含むすべてのパケットが Xen 仮想インタフェースを経由するようになります。NNMi 管理サーバーで **`ifconfig -a`** コマンドを実行すると、Xen の仮想アドレスが `virbr0` として表示されます。 いくつかの NNMi プロセスでは NNMi 管理サーバーのループバック アドレスを使用して通信する必要があるため、NNMi 管理サーバーに Xen をインストールすると NNMi が正常に動作しなくなる可能性があります。NNMi 管理サーバーのループバック アドレスの代わりに `virbr0` 仮想インタフェースが応答するようになるため、NNMi 内で通信の問題が発生します。

Xen 内で実行している仮想マシンで NNMi を実行しないでください。この設定はサポートされていません。

この問題を解決するには、以下を実行します。

1. **`kill`** コマンドを使用してすべての NNMi プロセスを停止します。

   `kill` コマンドを使用する必要があります。`virbr0` 仮想インタフェースの問題により、**`ovstop`** コマンドを使用して NNMi のプロセス マネージャ (`ovspmd`) と通信することができなくなっています。

2 **ifconfig virbr0** コマンドを実行して、virbr0 インタフェースの IP アドレスを表示します。この手順の残りの部分では、表示されるこの IP アドレスを *IP_Address* として表記します。

3 ファイル $NNM_SHARED_CONF/ovspmd.auth を編集します。

4 このテキストの最後に、手順 2 の IP アドレスとプラス記号 (+) を含む行を追加します。*IP_Address* + のようになります。

5 NNMi を組み込みデータベースとともに使用する場合、以下の手順を実行します。

   a 次のファイルを編集します： $NNM_DATA/shared/nnm/databases/Postgres/pg_hba.conf。

   b 手順 2 の IP アドレスを含む host all all IP_Address/32 trust という行を追加します。

6 **ovstart -c** コマンドを使用して NNMi プロセスを開始します。NNMi 管理サーバーが通常どおり動作します。

NNMi 9.0x からのアップグレード

NNM 6.x/7.x から NNMi 9.10 へのアップグレードの詳細については、『NNMi アップグレード リファレンス』を参照してください。

表 35 に示した情報に従って、NNMi をアップグレードできます。最適な結果を得るには、NNMi 9.10 にアップグレードする前に NNMi 9.0x パッチ 3 以降にアップグレードします。表 35 の情報は、NNMi 管理サーバーに NNMi 9.0x 以降がインストールされていることを想定して記載されています。

表 35　サポート対象の NNMi アップグレード

NNMi バージョン	NNMi 9.10 へのアップグレード
NNMi 9.0x	対応
NNMi 9.0x パッチ 1	対応
NNMi 9.0x パッチ 2 (NNMi 9.01)	対応
NNMi 9.0x パッチ 3 以降	対応

NNMi アプリケーション フェイルオーバー設定で実行している旧バージョンの NNMi 9.0x をアップグレードする場合、一時的なアプリケーション フェイルオーバーの設定解除、NNMi 9.10 への NNMi 管理サーバーのアップグレード、アプリケーション フェイルオーバーの再設定という順番のアップグレード パスがサポートされています。詳細については、「283 ページの「アプリケーション フェイルオーバーおよび NNMi 9.10 へのアップグレード」」を参照してください。

高可用性 (HA) で実行している旧バージョンの NNMi 9.0x をアップグレードする場合は、327 ページの「HA 下の NNMi を NNMi 9.0x から NNMi 9.10 にアップグレードする」を参照してください。

グローバルネットワーク管理環境で設定されている NNMi 管理サーバーをアップグレードする場合は、249 ページの「NNMi 9.0x から NNMi 9.10 へのアップグレード」を参照してください。

Linux NNMi 管理サーバーを NNMi 9.0x から NNMi 9.10 にアップグレードする場合、NNMi 9.10 をインストールする前に HP パブリック キーを Linux RPM データベースにインポートする必要があります。 これを行うには、ブラウザで以下の場所を指定してその指示に従います。

```
https://h20392.www2.hp.com/portal/swdepot/
displayProductInfo.do?productNumber=HPLinuxCodeSigning
```

いくつかの想定されるアップグレード例があります。この項では以下の章について説明します。

- NNMi 管理サーバーを適切にアップグレードする - 以下のアップグレード 例について説明します。
  - 同じハードウェアおよびオペレーティングシステムで、NNMi 9.0xからNNMi 9.10にアップグレードします。
- 別の NNMi 管理サーバーにアップグレードする - 以下のアップグレード 例について説明します。
  - 同じバージョンのオペレーティングシステムで、NNMi 9.0x から NNMi 9.10 にアップグレードします。
- Windows 2003 から Windows 2008 への NNMi の移行。NNMi 9.10 は Windows 2003 をサポートしていません。NNMi 9.10 にアップグレードする前に、オペレーティング システムを Windows 2008 に変更する必要があります。
- NNMi Oracle データの移行。 NNMi 管理サーバーが使用する Oracle データを Oracle データベースのインスタンスから別のインスタンスに移動する時に実行する手順を説明します。
- 追加アップグレード情報。NNMi 9.10 がそれまでのバージョンの NNMi と違ういくつかのエリアを説明します。

NNMi 管理サーバーを適切にアップグレードする

この章では、既存の NNMi 管理サーバーを NNMi 9.10 にアップグレードするプロセスを説明します。

この章の内容は以下のとおりです。

- 既存の NNMi 管理サーバー を NNMi 9.10 にアップグレード

既存の NNMi 管理サーバー を NNMi 9.10 にアップグレード

NNMi インストール ガイド と 403 ページの「追加アップグレード情報」の NNMi 9.10 「*インストール前チェックリスト*」章を読んでから、始めてください。NNMi インストール ガイド が大幅に変更されています。たとえば、組み込みデータベースではなく Oracle データベース インスタンスを使用する場合は、FLASHBACK ANY TABLE 権限を設定する必要があります。この設定により、NNMi で移行中に復元ポイントを作成できるためです。

まず、アップグレードする NNMi ソフトウェアの『HP Network Node Manager i Software システムとデバイス対応マトリックス』を読んでから、手順を続行してください。このドキュメントは、http://h20230.www2.hp.com/selfsolve/manuals で入手できます。この Web サイトにアクセスするには、HP Passport のユーザー ID が必要です。

以下の手順では、NNMi 管理サーバーから NNMi 9.10 へのアップグレード方法を説明します。以下の手順では、NNMi 9.0x が NNMi 管理サーバーで実行中であることを前提としています。

1. `nnmbackup.ovpl` スクリプトを使用して、NNMi 管理サーバーをバックアップします。移行が失敗することは稀ですが、万一に備えてバックアップを行います。このバックアップを使用するのは移行が失敗した場合のみです。詳細については、*nnmbackup.ovpl* リファレンス ページ、または UNIX のマンページを参照してください。
2. *Oracle データベース専用*: NNMi 管理サーバーで Oracle データベースを使用する場合は、Oracle データベース管理者に NNMi データのバックアップを依頼してください。NNMi で移行中に復元ポイントを作成できるように、前述のように、Oracle データベース管理者に FLASHBACK ANY TABLE 権限の設定を依頼してください。

3 *Oracle データベース専用*: `nnmconfigexport.ovpl` スクリプトを使用して、NNMi 管理サーバーからの設定情報をバックアップします。移行が失敗することは稀ですが、万一に備えてバックアップを行います。このバックアップを使用するのは移行が失敗した場合のみです。詳細については、*nmconfigexport.ovpl* または *nnmconfigimport.ovpl* のリファレンス ページ、または UNIX のマンページを参照してください。

`nnmconfigexport.ovpl` スクリプトを使用してファイルをインポートする前に、`nnmconfigimport.ovpl` スクリプトでエクスポートしたファイルを編集しないでください。

4 NNMi インストール ガイド の指示に従って、NNMi 9.10 を NNMi 管理サーバーにインストールします。

Oracle データベース専用 : Oracle データベース管理者が FLASHBACK ANY TABLE 権限を設定しないと、インストール完了後にその権限がないという警告が表示されます。この警告は無視できます。

5 NNMi 管理サーバーの情報が正しく移行されたことを確認します。

別の NNMi 管理サーバーにアップグレードする

この章では、既存の NNMi 管理サーバーの設定を維持しながら、新規システム上で NNMi 9.10 にアップグレードするプロセスを説明します。

この章の内容は以下のとおりです。

- 別の NNMi 管理サーバーへのアップグレード

別の NNMi 管理サーバーへのアップグレード

NNMi インストール ガイド と 403 ページの「追加アップグレード情報」の NNMi 9.10 「*インストール前チェックリスト*」章を読んでから、始めてください。NNMi インストール ガイド が大幅に変更されています。たとえば、組み込みデータベースではなく Oracle データベース インスタンスを使用する場合は、FLASHBACK ANY TABLE 権限を設定する必要があります。この設定により、NNMi で移行中に復元ポイントを作成できるためです。

以下の手順は、既存の NNMi 管理サーバーをターゲットの NNMi 管理サーバーにデータをコピーする方法を説明したものです。以下の手順では、NNMi 9.0x が既存の NNMi 管理サーバーで実行中であることを前提としています。

Oracle データベース サーバー を変更する場合は、NNMi 9.10 にアップグレードする前または後にそのプロセスを実行します。詳細については、401 ページの「NNMi Oracle データの移行」を参照してください。

1. 万一に備えて、既存 (ソース) の NNMi 9.0x 管理サーバーを `nnmbackup.ovpl` スクリプトを使用してバックアップしておきます。この NNMi 9.0x のバックアップにラベルを付けます。詳細については、NNMi 9.0x の *nnmbackup.ovpl* リファレンス ページ、または UNIX のマンページを参照してください。
2. 既存 (ソース) の NNMi 管理サーバーが Oracle データベースを使用している場合は、Oracle データベース管理者に NNMi 9.0x データのバックアップを依頼します。前述のように、移行中に NNMi で復元ポイントを作成できるように、Oracle データベースに FLASHBACK ANY TABLE 権限の設定を依頼してください。

3 『NNMi インストール ガイド』の手順に従って、ソース NNMi 管理サーバー上に NNMi 9.10 および最新の統合パッチ (ある場合) をインストールします。

Oracle データベース専用 : Oracle データベース管理者が FLASHBACK ANY TABLE 権限を設定しないと、インストール完了後にその権限がないという警告が表示されます。この警告は無視できます。

4 NNMi 9.10 がソース NNMi 管理サーバー上で正しく動作していることを確認します。

5 `nnmbackup.ovpl` スクリプトを使用して、NNMi 9.10 をソース NNMi 管理サーバー上にバックアップします。この NNMi 9.10 のバックアップにラベルを付けます。データをターゲットの NNMi 管理サーバーにコピーする必要があります。詳細については、NNMi 9.10 の *nnmbackup.ovpl* リファレンス ページ、または UNIX のマンページを参照してください。

6 『NNMi インストール ガイド』の手順に従って、ターゲット NNMi 管理サーバー上に NNMi 9.10 および最新の統合パッチ (ある場合) をインストールします。手順 5 からデータを移行するには、ターゲットの NNMi 管理サーバーが同じオペレーティング システム バージョンを実行中である必要があります。NNMi では、別のオペレーティング システム上で実行中の NNMi 管理サーバーへのデータ移行はサポートされていません。

7 `nnmrestore.ovpl` スクリプトを使用して、NNMi のデータベース情報をターゲットサーバーにコピーします。詳細については、*nnmrestore.ovpl* リファレンス ページ、または UNIX のマンページを参照してください。

8 新規ライセンスを取得し、ターゲットの NNMi 管理サーバーにインストールします。

詳細については、115 ページの「NNMi ライセンスの取得」を参照してください。

9 ターゲットの NNMi 管理サーバー情報が既存の NNMi 管理サーバーから正常に移行されたことを確認します。

Windows 2003 から Windows 2008 への NNMi の移行

NNMi 9.10 は Windows 2003 をサポートしていません。NNMi 9.10 に移行する前に、オペレーティング システムを Windows 2008 に変更する必要があります。

Windows 2003 サーバーで NNMi 9.0x パッチ 3 以降が実行されている場合は、この章の情報に従って、オペレーティング システムを Windows 2008 に変更する必要があります。

この章の内容は以下のとおりです。

Windows 2003 から Windows 2008 への NNMi の変更

Windows 2003 から Windows 2008 への NNMi の変更

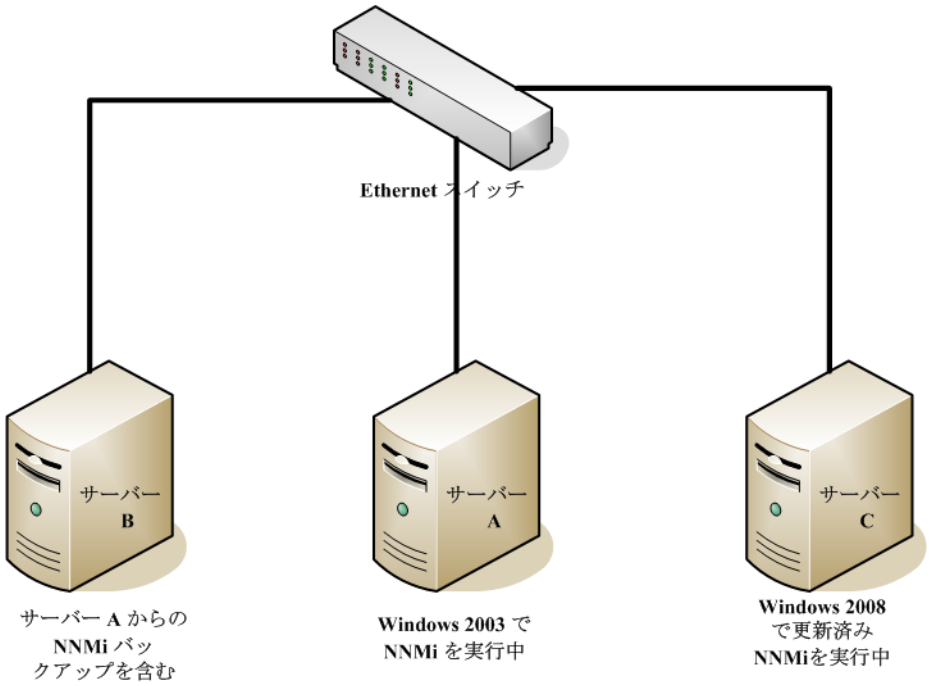
以下の手順を実行するには、Windows 2003 サーバーで NNMi 9.0x パッチ 3 以降が実行されている必要があります。NNMi のバージョン番号を調べるには、**[ヘルプ] -> [HP Network Node Manager i Software について]** ウィンドウで現在のパッチ レベルを書き留めます。バージョンが 9.01.003 以降であることを確認します。それ以前のバージョンの場合は、次に進まないでください。次に進む前に、NNMi 9.0x パッチ 3 以降をインストールする必要があります。

NNMi 9.0x パッチ 3 以降が実行されている NNMi 管理サーバーを Windows 2003 から Windows 2008 に変更するには、以下の手順を実行します。

1 この手順では、以下の 3 つのサーバーを使用します。

- `Server A` は、Windows 2003 を実行している現在の NNMi 管理サーバーです。
- `Server B` は、NNMi のバックアップ ファイルを保持します。
- `Server C` は、Windows 2008 を実行することになる新しい NNMi 管理サーバーです。この NNMi 管理サーバーは、現在の `Server A` と同じハードウェアにすることができます。

  新しい NNMi 管理サーバーの `hosts` ファイルに、エントリ **`127.0.0.1 localhost`** があることを確認してください。



2 Server A で、**nnmbackup.ovpl -type online -scope all -target** temporary_location コマンドを実行して NNMi のフル バックアップを完了します。

使用するコマンド オプションの詳細については、347 ページの「NNMi のバックアップおよびリストア ツール」と、*nnmbackup.ovpl* リファレンス ページ、または UNIX のマンページを参照してください。

3 Server A で、手順 2 で作成したバックアップを Server B にコピーします。

4 Server C で、Windows 2008 をインストールします。

Server C を使用する代わりに、Server A のディスクを再フォーマットして Windows 2008 をインストールすることもできます。その場合は、以下の手順に示す Server C を Server A と読み替えてください。

5 Server C で、NNMi 9.0x パッチ 3 以降をインストールします。手順 2 でバックアップを実行したときの NNMi Server A のパッチと同じレベルのパッチをインストールする必要があります。

6 Server C で NNMi をインストールするときに、インストール スクリプトによって Server B の設定とは異なるポートが割り当てられることがあります。このことが原因で、Server C で設定をリストアするときにポートの競合が発生する可能性があります。これを解決するには、以下を実行します。

a Server C で、%$NNM_CONF%¥nnm¥props¥ ディレクトリに移動します。

b Server C で、nms-local.properties ファイルを一時保存場所の nms-local.properties.save in にコピーします。

c Server B で、NNMi のバックアップを Server C にコピーします。

d Server C で、**nnmrestore.ovpl -force -source *temporary_location*** コマンドを実行して NNMi をフル リストアします。

使用するコマンド オプションの詳細については、347 ページの「NNMi のバックアップおよびリストア ツール」と、*nnmrestore.ovpl* リファレンス ページ、または UNIX のマンページを参照してください。

手順 2 で作成したバックアップに一致するコマンド オプションを使用してください。

e Server C で、一時保存場所にある nms-local.properties.save ファイルと、%NNM_CONF%¥nnm¥props¥ディレクトリにある nms-local.properties ファイルを比較します。

上記のディレクトリの nms-local.properties を変更してポートの競合を解決します。Server C で NNMi をインストールするときに選択した jboss.http.port (NNMi の Web サーバー ポート) および jboss.https.port (NNMi の HTTPS Web サーバー ポート) の値を保持してください。

f ovjboss を再起動します。

```
ovstop ovjboss
ovstart ovjboss
```

7 NNMi は、ライセンス キーをサーバーの IP アドレスと関連付けます。Server C の IP アドレスと Server A の IP アドレスが異なる場合は、新しい NNMi ライセンス キーを入手してインストールしてください。382 ページの「スタンドアロン NNMi 管理サーバーの IP アドレスを変更する」を参照してください。

8 Server C で、NNMi 9.10 をインストールします。

NNMi Oracle データの移行

NNMi の Oracle データを Oracle 11G に移動する計画の場合。この章では、この作業を完了する手順を説明します。

NNMi Oracle データの以降

以下のいずれかの設定で NNMi を実行しているとします。

- 最新のパッチを適用済みの NNMi 9.0x が Oracle 10G データベースに接続されており、NNMi 9.10 にアップグレードする必要がある。
- 最新のパッチを適用済みの NNMi 9.0x が Oracle 11G データベースに接続されており、NNMi 9.10 にアップグレードする必要がある。

実施する必要のある Oracle データベース インスタンスの移行には、以下の要件が含まれている場合があります。

- NNMi 9.10 で実行されている既存の Oracle インスタンスでは、Oracle 10G または 11G を実行できる。
- NNMi 9.10 で実行されている新しい Oracle インスタンスでは、Oracle 11G を実行している必要がある。
- 新しい Oracle インスタンスは元のサーバーまたは別のサーバーとホスト名上に存在する。

NNMi Oracle データの移行を完了するには、以下の手順を実行します。

1. root または管理者として **`ovstop -c`**. コマンドを実行して NNMi を停止します。
2. Oracle ツールを使用して、既存の Oracle サーバーから新しいサーバーに NNMi データを移動またはコピーします。詳細は、Oracle のドキュメントを参照してください。

   この Oracle データ移行は、同じサーバーでの Oracle 10 から Oracle 11 へのインプレース アップグレードを行えます。Oracle は、Oracle 10 データを Oracle 11 フォーマットに変換するデータベース移行ツールを提供しています。

3. *新しい Oracle サーバーに以前の Oracle サーバーとは異なるホスト名を使用している場合にのみこの手順を実行します。* NNMi 管理サーバーで、以下の手順を実行し、NNMi が新しい Oracle サーバーにポイントするように再設定します。

a 以下に示すデータベース設定ファイルを編集します。

jboss が Oracle 11G データベースに正しく接続するには、以下の手順を正確に実行する必要があります。

— *Windows*: `%NNM_JBOSS%¥server¥nms¥deploy¥nms-ds.xml`

— *UNIX*: `$NNM_JBOSS/server/nms/deploy/nms-ds.xml`

b 新しいサーバーの情報を反映するように、以下の属性を変更します。

旧 :
<connection-url>jdbc:oracle:thin:@*EXISTING_FQDN*:*EXISTING_ORACLE_PORT*:*EXISTING_SID* </connection-url>

新 :
<connection-url>jdbc:oracle:thin:@NEW_*FQDN*:*NEW_PORT*:*NEW_SID*</connection-url>

4 以下の操作の 1 つを完了してください。

NNMi 9.0x から NNMi 9.10 にアップグレードする場合は、『HP Network Node Manager i ソフトウェア インストール ガイド』のインストール手順に従って、今すぐ移行を実行します。

すでに NNMi 9.10 を使用している場合は、以下の手順に従って NNMi を再起動し、Oracle データベースの移動 / 移行を完了します。

a NNMi 管理サーバーで **`ovstart -c`** コマンドを実行し、NNMi を再起動します。

b NNMi 管理サーバー で **`ovstatus -v`** コマンドを実行し、すべてのサービスが開始しており、正しく実行していることを確認します。

追加アップグレード情報

この章では、NNMi 9.10 とそれ以前の NNMi バージョン間の変更点について説明します。この章には、以下のトピックがあります。

- 設定面の相違点
- MIB
- 機能面の相違点

設定面の相違点

- NNMi コンソール内でのユーザー アクセスを制限するため、ユーザー グループにより NNMi ロールを置き換えています。ユーザー アカウントは、複数のユーザー グループにマッピングできます。
  - NNMi コンソールにサインインするには、各ユーザー アカウントを NNMi 提供のユーザー グループの少なくとも 1 つにマッピングする必要があります。これらのグループは、以前のリリースでの NNMi ロールと同等の機能を果たします。
  - マルチテナント環境では、各ユーザー アカウントを、トポロジ オブジェクトのサブセットへのアクセスを提供する 1 つ以上のカスタム ユーザー グループにマッピングできます。

  詳細については、193 ページの「NNMi セキュリティおよびマルチテナント」を参照してください。
- ディレクトリ サービスからユーザー情報を取得する NNMi 統合では、ユーザーごとに複数のグループ名を取得できるようになっています。
  - 設定オプション 2 (ディレクトリ サービス内のユーザー名とパスワードのみ) の場合、既存のディレクトリ サービスとの統合は `ldap.properties` 設定ファイルに修正を加えなくても機能し続けます。
  - 設定オプション 3 (ディレクトリ サービス内のすべてのユーザー情報) の場合は、以下の情報が適用されます。
    - 単一テナント環境 (すべての NNMi コンソールユーザーがすべてのトポロジ オブジェクトにアクセスできる) の場合、既存のディレクトリ サービスとの統合は `ldap.properties` 設定ファイルに修正を加えなくても機能し続けます。

新しい NNMi ユーザー グループをディレクトリ サービスに追加する場合は、ディレクトリ サービスからユーザー情報を取得できるようにするため、ldap.properties 設定ファイルを新しいモデルに更新する必要があります。

– マルチテナント環境では、ディレクトリ サービスからユーザー情報を取得できるようにするため、ldap.properties 設定ファイルを新しいモデルに更新してください。

– ldap.properties 設定ファイルの更新の詳細については、174ページの「ディレクトリ サービスのアクセス設定を変更し、NNMi のセキュリティ モデルをサポートする」を参照してください。

— NNMi 9.10 では、以下の ldap.properties 設定ファイルのパラメータを廃止しています。これらのパラメータは、将来的なリリースではサポートされなくなります。

– roleAttributeID

– roleAttributeIsDN

– roleNameAttributeID

- NNMi 9.10 をアップグレードした後、以下のセキュリティ設定およびマルチテナント設定が適用されます。

  — すべてのノードは、デフォルトテナントとデフォルトセキュリティグループに割り当てられます。

  — すべてのユーザーは、NNMi トポロジ内のすべてのノードと、すべてのインシデントにアクセスできます。

  このデフォルト設定は、NNMi 9.0x で使用できるオブジェクトアクセスと一致します。オブジェクトアクセスのカスタマイズの詳細については、193 ページの「NNMi セキュリティおよびマルチテナント」を参照してください。

- HP NNMi 幽 P NA 統合を NNMi 9.0x 管理サーバーで設定した場合、その設定は NNMi 9.10 へのアップグレード プロセスによって無効にされます。詳細については、450 ページの「NNMi 9.0x からアップグレードされた統合設定」を参照してください。

- NNMi 9.10 へのアップグレード後、NNMi は NNMi コンソールでサインインまたはサインアウトする各ユーザーのログ エントリを生成しなくなります。この設定は、logging.properties ファイルを編集することで変更できます。詳細については、363 ページの「」を参照してください。
  NNMi 9.10 へのアップグレードが完了したら、NNMi 9.0x で使用する logging.properties ファイルのコピーを以下の場所で探します。

  – *Windows*:
  %NNM_DATA%¥shared¥nnm¥conf¥ovjboss¥logging.properties.old

  – *UNIX*:
  $NNM_DATA/shared/nnm/conf/ovjboss/logging.properties.old

アプリケーション フェイルオーバー

NNMi 9.0x では、アプリケーション フェイルオーバー機能で UDP または TCP のいずれかのソリューションをサポートしていました。NNMi 9.10 では、TCP ソリューションのみをサポートします。NNMi 9.0x で UDP アプリケーション フェイルオーバー ソリューションを使用していた場合に NNMi 9.10 にアップグレードすると、アップグレード スクリプトは、アプリケーション フェイルオーバー設定を TCP ソリューションに変換します。クラスタ内のすべてのノードのホスト名を nms-cluster.properties ファイルの com.hp.ov.nms.cluster.member.hostnames パラメータに追加する必要があります。詳細については、270 ページの「アプリケーション フェイルオーバー構成の NNMi の設定」を参照してください。

アプリケーション フェイルオーバーが正しく機能するには、アクティブ サーバーとスタンバイ サーバーは相互のネットワークに制限のないことが必要です。NNMi 9.10 では一部のポートが変更されているため、該当する場合はファイアウォール設定を変更する必要があります。詳細については、605 ページの「NNMi 9.10 およびウェルノウン ポート」を参照してください。

MIB

標準準拠でないか、または他の MIB ファイルに依存している以前のバージョンの NNMi に追加の MIB をロードした場合は、正常に移行できない可能性があります。MIB が正常に移行しない場合、トラップ設定は機能し続けますが、その MIB を移行前と同じように参照することはできなくなります。

一部の MIB が移行しなかったことが疑われる場合は、以下のディレクトリで、MIB ファイル、障害の詳細、および MIB ファイルと関連付けられた名前が付けられたログ ファイル含む `failed` サブディレクトリがないかどうか確認してください。

- *Windows*: `%NNM_DATA%¥tmp¥nnm9xMibMigrate`
- *UNIX*: `$NNM_DATA/tmp/nnm9xMibMigrate`

上記のディレクトリに格納されているファイルを使用し、MIB が移行しなかった理由を見極めてから、MIB を再ロードしてください。

機能面の相違点

NNMi 9.10 に含まれる新機能についての情報を確認するには、『NNMi リリース ノート』の「*このバージョンでの更新点*」のセクションを参照してください。

NNMi との統合

この項では以下の章について説明します。

- CiscoWorks LAN Management Solution
- Clarus Systems ClarusIPC Plus+
- HP Asset Manager
- HP Business Service Management トポロジ
- HP Universal CMDB
- HP Business Availability Center My BSM
- HP Network Automation
- HP ProCurve Manager Plus
- HP RAMS MPLS WAN
- HP SiteScope
- HP Systems Insight Manager
- nGenius Performance Manager
- NNMi ノースバウンド インタフェース
- HP BSM Operations Management
- HP Operations Manager
- HP NNMi Integration Module for Netcool Software
- xMatters (以前の AlarmPoint)

CiscoWorks LAN Management Solution

Cisco Systems CiscoWorks LAN Management Solution (CiscoWorks LMS) は、Cisco ネットワークの設定、管理、監視、およびトラブルシューティングを行うための管理ツールの統合スイートです。

この章には、以下のトピックがあります。

- HP NNMi-CiscoWorks LMS 統合
- HP NNMi-CiscoWorks LMS 統合の有効化
- HP NNMi-CiscoWorks LMS 統合の使用法
- HP NNMi-CiscoWorks LMS 統合設定の変更
- HP NNMi-CiscoWorks LMS 統合の無効化
- HP NNMi-CiscoWorks LMS 統合のトラブルシューティング
- [HP NNMi-CiscoWorks LMS の統合設定] フォームのリファレンス

HP NNMi-CiscoWorks LMS 統合

HP NNMi-CiscoWorks LMS 統合では、NNMi コンソールから CiscoWorks ツールにアクセスするためのアクションを使用できます。

値

HP NNMi-CiscoWorks LMS 統合は、CiscoWorks LMS 情報を NNMi に追加し、NNMi ユーザーが Cisco デバイスの潜在的なネットワーク問題を検出および調査できるようにします。

統合製品

この章の情報は、以下の製品に当てはまります。

- CiscoWorks LMS

  サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10

NNMi と CiscoWorks LMS は、別々のコンピュータにインストールする必要があります。NNMi 管理サーバーと CiscoWorks LMS サーバー コンピュータのオペレーティング システムは、同じでも異なっていても構いません。

NNMi で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、『NNMi システムおよびデバイスのサポート マトリックス』を参照してください。

CiscoWorks LMS で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、ご使用のバージョンのマニュアルを参照してください。たとえば、以下のようにします。

- CiscoWorks LMS バージョン 3.1:

  http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/3.1/install/guide/prereq.html

- CiscoWorks LMS バージョン 3.2:

  http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/3.2/install/guide1/prereq.html

ドキュメント

この章では、CiscoWorks LMS と通信するように NNMi を設定する方法、および NNMi コンソールから統合を使用する方法について説明します。

HP NNMi-CiscoWorks LMS 統合の有効化

NNMi 管理サーバーで、以下の手順に従って NNMi と CiscoWorks LMS 間の接続を設定します。

1. NNMi コンソールで、**[HP NNMi-CiscoWorks LMS の統合設定]** フォーム (**[統合モジュールの設定] > [CiscoWorks LMS]**) を開きます。
2. **[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。
3. 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は、413 ページの「NNMi 管理サーバー接続」を参照してください。
4. CiscoWorks LMS 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は、414 ページの「CiscoWorks LMS サーバー接続」を参照してください。

5 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。

6 CiscoWorks LMS 管理対象デバイスのインシデント定義をロードします。

a ディレクトリを次のように変更します。

— *Windows*: `%NnmInstallDir%¥newconfig¥HPOvNmsEvent`

— *UNIX*: `$NnmInstallDir/newconfig/HPOvNmsEvent`

b 以下のコマンドを入力して、CiscoWorks LMS インシデント定義をインポートします。

```
nnmconfigimport.ovpl -f nnm-cisco-incidentConfig.xml ¥
-u <username> -p <password>
```

7 オプションおよび推奨事項。CiscoWorks LMS 管理対象デバイスが生成するトラップの MIB 定義ファイルをロードします。

a デバイス メディアまたは Cisco Web サイトから、適切な MIB ファイルを入手します。

tools.cisco.com/Support/SNMP/do/SearchOID.do?local=en&step=1

b MIB ファイルを格納するディレクトリに変更します。

c nnmloadmib.ovpl コマンドを使用して、管理対象環境の適切な MIB ファイルをロードします。たとえば、以下のようにします。

```
nnmloadmib.ovpl -load cpqhost.mib -u <username> -p <password>
```

d 以下のコマンドを入力して、MIB が正常にロードされたことを確認します。

```
nnmloadmib.ovpl -list -u <username> -p <password>
```

HP NNMi-CiscoWorks LMS 統合の使用法

HP NNMi-CiscoWorks LMS 統合では、NNMi コンソールから CiscoWorks LMS へのリンクを使用できます。この統合では、製品間のシングル サインオン機能は提供されません。CiscoWorks LMS のページを表示するには、CiscoWorks LMS のユーザー資格証明を入力する必要があります。

HP NNMi-CiscoWorks LMS 統合を有効にすると、以下のアクションが NNMi コンソールに追加されます。

- **CiscoWorks Device Center** - 選択したノードのコンテキストで CiscoWorks Device Center を開きます。
- **CiscoWorks CiscoView** - 選択したノードのコンテキストで CiscoWorks CiscoView を開きます。

HP NNMi-CiscoWorks LMS 統合設定の変更

1 NNMi コンソールで、**[HP NNMi-CiscoWorks LMS の統合設定]** フォーム (**[統合モジュールの設定] > [CiscoWorks LMS]**) を開きます。

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は、413 ページの「[HP NNMi-CiscoWorks LMS の統合設定] フォームのリファレンス」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。`ovjboss` を再起動する必要はありません。

HP NNMi-CiscoWorks LMS 統合の無効化

1 NNMi コンソールで、**[HP NNMi-CiscoWorks LMS の統合設定]** フォーム (**[統合モジュールの設定] > [CiscoWorks LMS]**) を開きます。

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。これで、統合アクションを使用できなくなります。

変更はただちに有効になります。`ovjboss` を再起動する必要はありません。

HP NNMi-CiscoWorks LMS 統合のトラブルシューティング

CiscoWorks LMS アクションが機能しない

[HP NNMi-CiscoWorks LMS の統合設定] フォームの値が正しいことを確認しても NNMi コンソールから CiscoWorks LMS ページを開くことができない場合は、以下の手順を実行します。

1 Web ブラウザのキャッシュをクリアします。

2 Web ブラウザから、すべての保存フォームまたはパスワード データをクリアします。

3 Web ブラウザ ウィンドウを完全に閉じてから、もう一度開きます。

4 **[HP NNMi-CiscoWorks LMS の統合設定]** フォームに値を再入力します。

5 CiscoWorks LMS が実行されていることを確認します。

トラップの MIB キャッシュ メッセージで OID を検出できない

CiscoWorks LMS 管理対象デバイスが生成するトラップの MIB 定義ファイルが NNMi にロードされない場合は、以下のテキストのようなエラー メッセージが表示されます。

<Cia .1.3.6.1.4.1.11.5.7.5.2.1.1.1.7.0 with value 1 was not found within the mib cache>

このようなエラーを解決するには、411 ページの手順 7 の説明に従って MIB をロードします。

[HP NNMi-CiscoWorks LMS の統合設定] フォームのリファレンス

[HP NNMi-CiscoWorks LMS の統合設定] フォームには、NNMi と CiscoWorks LMS 間の通信を設定するためのパラメータが含まれています。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。

[HP NNMi-CiscoWorks LMS の統合設定] フォームには、Administrator ロールの NNMi ユーザーのみがアクセスできます。

[HP NNMi-CiscoWorks LMS の統合設定] フォームでは、以下の一般領域に関する情報を収集します。

- NNMi 管理サーバー接続
- CiscoWorks LMS サーバー接続

統合設定に変更を適用するには、**[HP NNMi-CiscoWorks LMS 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 36 に、NNMi 管理サーバーへの接続パラメータをリストします。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 36　NNMi 管理サーバー情報

フィールド	説明
NNMi SSL 有効化	接続プロトコル指定。 • 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。これがデフォルト設定です。 • 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。
NNMi ホスト	NNMi 管理サーバーの完全修飾ドメイン名。このフィールドには、NNMi コンソールへのアクセスに使用するホスト名があらかじめ入力されています。この値が、NNMi 管理サーバー上で **`nnmofficialfqdn.ovpl -t`** コマンド実行によって返された名前であることを確認します。
NNMi ポート	NNMi コンソール に接続するためのポート。このフィールドには、次のファイルで指定されているように、NNMi コンソール との通信のために jboss アプリケーション サーバーが使用するポートがあらかじめ記入されています。 • *Windows*: `%NnmDataDir%¥conf¥nnm¥props¥nms-local.properties` • *UNIX*: `$NnmDataDir/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。

表 36　NNMi 管理サーバー情報 (続く)

フィールド	説明
NNMi ユーザー	NNMi コンソール 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。

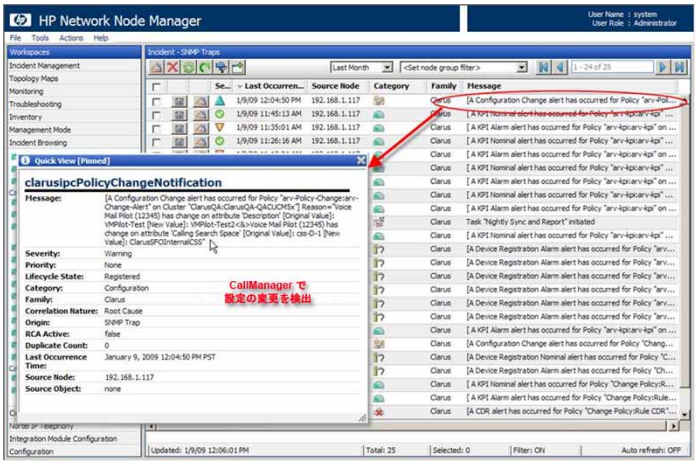
CiscoWorks LMS サーバー接続

表 37 に、CiscoWorks LMS サーバーに接続して、CiscoWorks LMS ページを開くためのパラメータを示します。CiscoWorks LMS 管理者と協力して、この設定項目に適切な値を決定してください。

表 37　CiscoWorks LMS 管理サーバー情報

CiscoWorks LMS サーバー パラメータ	説明
CiscoWorks LMS SSL 有効化	CiscoWorks LMS に接続するための接続プロトコル指定。 • HTTPS を使用するように CiscoWorks LMS を設定する場合は、**[CiscoWorks LMS SSL の有効化]** チェックボックスをオンにします。これがデフォルト設定です。 • HTTP を使用するように CiscoWorks LMS を設定する場合は、**[CiscoWorks LMS SSL の有効化]** チェックボックスをオフにします。
CiscoWorks LMS ホスト	CiscoWorks LMS サーバーの完全修飾ドメイン名。
CiscoWorks LMS ポート	CiscoWorks LMS の Web サービスに接続するときのポート。 デフォルトの CiscoWorks LMS 設定を使用する場合は、ポート `1741` (CiscoWorks LMS へ非 SSL 接続する場合) またはポート `443` (CiscoWorks LMS へ SSL 接続する場合) を使用してください。

Clarus Systems ClarusIPC Plus+



Clarus Systems ClarusIPC Plus+ は、新規導入時やアップグレード時、および通常の運用中に、Cisco Unified Communications Manager IP のテレフォニ システムに関する音声サービス テスト、IP フォン機能のリモート診断、コールの詳細レコード (CDR) に基づく警告および追跡、設定の報告を行います。

Clarus Systems は、ClarusIPC Plus+ と HP Network Node Manager i Software (NNMi) の統合を提供します。HP は、ClarusIPC Plus+ と NNM iSPI for IP Telephony の統合を提供します。これらの統合は相互排他的です。

この章では、以下の使用可能な統合について説明します。

- HP NNMi-Clarus Systems ClarusIPC Plus+ 統合
- HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合

HP NNMi-Clarus Systems ClarusIPC Plus+ 統合

この項では以下の内容について説明します。

- 416 ページの「HP NNMi-Clarus Systems ClarusIPC Plus+ 統合について」
- 416 ページの「HP NNMi-Clarus Systems ClarusIPC Plus+ 統合の有効化」
- 417 ページの「HP NNMi-Clarus Systems ClarusIPC Plus+ 統合の使用法」
- 417 ページの「HP NNMi-Clarus Systems ClarusIPC Plus+ 統合の無効化」
- 417 ページの「HP NNMi-Clarus Systems ClarusIPC Plus+ 統合のトラブルシューティング」

HP NNMi-Clarus Systems ClarusIPC Plus+ 統合について

Clarus Systems では、HP NNMi-Clarus Systems ClarusIPC Plus+ 統合を提供しサポートしています。この統合では、ClarusIPC Plus+ は IP テレフォニ サービスのテスト結果に関する SNMP トラップ、セット CDR ポリシーに基づく警告、または Unified Communications Manager Configuration 変更ポリシーに基づく警告に関する SNMP トラップ NNMi に転送し、そこで IP テレフォニ設定とデバイスのステータスに関するインシデントを生成します。NNMi は、ネットワーク全体の統合ビューを提供します。

この統合は、NNMi コンソール内のこれらのインシデントから複数の ClarusIPC Plus+ ツールにアクセスするために用意されています。

値

HP NNMi-Clarus Systems ClarusIPC Plus+ 統合により NNMi コンソールから ClarusIPC Plus+ ツールにアクセスして、IP テレフォニ設定変更の追跡とレポーティングを行い、IP テレフォニ デバイス管理を一元管理します。

統合製品

この章の情報は、以下の製品に当てはまります。

- ClarusIPC Plus+

  サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10 (Windows オペレーティングシステムのみ)

ドキュメント

HP NNMi-Clarus Systems ClarusIPC Plus+ 統合については、統合インストール パッケージに付属している『ClarusIPC Plus+ HP NNMi Software 統合ガイド』で詳しく説明しています。

ClarusIPC Plus+ のドキュメント スイートには、ClarusIPC Plus+ の機能について詳しく説明された追加ドキュメントがあります。ドキュメント スイートは、以下の Clarus Systems サイトからダウンロードできます。

www.support.clarussystems.com

HP NNMi-Clarus Systems ClarusIPC Plus+ 統合の有効化

HP NNMi-Clarus Systems ClarusIPC Plus+ 統合インストール パッケージを入手するには、Clarus Systems のサポートにお問い合わせください。

統合の有効化については、統合インストール パッケージにある『ClarusIPC Plus+ HP NNMi Software 統合ガイド』を参照してください。

HP NNMi-Clarus Systems ClarusIPC Plus+ 統合の使用法

HP NNMi-Clarus Systems ClarusIPC Plus+ 統合を有効にすると、NNMi コンソールにいくつかの URL アクションが追加されます。URL アクションの詳細は、『ClarusIPC Plus+ HP NNMi Software 統合ガイド』を参照してください。

ClarusIPC Plus+ を使用するには、Web ブラウザ Microsoft Internet Explorer が必要です。Internet Explorer で NNMi コンソールを開いてから、ClarusIPC Plus+ のウィンドウを開く URL アクションを起動します。

HP NNMi-Clarus Systems ClarusIPC Plus+ 統合の無効化

HP NNMi-Clarus Systems ClarusIPC Plus+ 統合の無効化については、Clarus Systems のサポートにお問い合わせください。

HP NNMi-Clarus Systems ClarusIPC Plus+ 統合のトラブルシューティング

統合の最適化と拡張、および既知の問題については、『ClarusIPC Plus+ HP NNMi Software 統合ガイド』を参照してください。

HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合

この項では以下の内容について説明します。

- 418 ページの「HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合について」
- 419 ページの「HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合の有効化」
- 419 ページの「HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合の使用法」
- 419 ページの「HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合の無効化」
- 420 ページの「HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合のトラブルシューティング」

HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合について

HP は、HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合を提供しサポートしています。この統合により、オペレータは IP テレフォニのサービス テストと診断、Cisco Unified Communications Configuration の変更レポート、および CDR 監視 ポリシーに適した ClarusIPC Plus+ 機能にアクセスできます。ClarusIPC Plus+ は IP テレフォニ サービスのテスト結果に関する SNMP トラップ、セット CDR ポリシーに基づく警告、または、Unified Communications Manager Configuration 変更ポリシーに基づく警告に関する SNMP トラップを NNMi に転送し、そこで IP テレフォニ設定とデバイスのステータスに関するインシデントを生成します。NNM iSPI for IP Telephony には、以下の機能があります。

- ClarusIPC Plus+ 設定変更レポート、ポリシー、テスト計画、テスト結果を処理するためのワークスペースとメニュー
- 選択した IP フォンのコンテキストに応じた、IP フォンの ClarusIPC Plus+ リモート診断ツールの開始
- NNMi インシデント ビューで選択した警告インシデントのコンテキストに応じた、ClarusIPC Plus+ のテスト結果、テストの詳細、および CDR ポリシーの詳細の起動

この統合により、NNMi コンソールから、NNM iSPI for IP Telephony なしで統合している場合よりも多くの ClarusIPC Plus+ ツールにアクセスできます。

値

HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合により、NNM iSPI for IP Telephony には、高度な IP テレフォニ サービスのテストと診断、CDR 監視、設定変更の追跡とレポートが追加されます。

統合製品

このセクションの情報は、以下の製品に当てはまります。

- ClarusIPC Plus+

  サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10 (NNM iSPI ネットワーク エンジニアリング ツールセット ソフトウェア ライセンス付き)
- NNM iSPI for IP Telephony 9.10

ドキュメント

HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合については、iSPI に付属している『NNM iSPI for IP Telephony ヘルプ』で詳しく説明しています。

ヘルプ (PDF 形式) その他の NNM iSPI for IP Telephony ドキュメントは、次の URL で入手できます。

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

HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合の有効化

1 NNMi 管理サーバーを準備します。

   a (Clarus Systems が提供する) HP NNMi-Clarus Systems ClarusIPC Plus+ 統合が NNMi 管理サーバーにインストールされている場合、NNM iSPI for IP Telephony と ClarusIPC Plus+ の統合を有効にする前にアンインストールしてください。

      ClarusIPC Plus+ 統合パッケージのアンインストール方法については、Clarus Systems のサポートにお問い合わせください。

   b NNMi 管理サーバーで、以下をインストールします。

      — 最新の NNMi 統合パッチ (該当するものがある場合)

      — 最新の NNM iSPI for IP Telephony 統合パッチ (該当するものがある場合)

      パッチは、次の URL で入手できます。

      http://h20230.www2.hp.com/selfsolve/patches

2 NNMi 管理サーバーで、NNM iSPI for IP Telephony ヘルプ の説明に従って HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合を有効にします。

HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合の使用法

HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合を有効にすると、NNMi コンソールに、いくつかのワークスペース、インシデント タイプ、URL アクションが追加されます。URL アクションの詳細は、『NNM iSPI for IP Telephony ヘルプ』を参照してください。

ClarusIPC Plus+ を使用するには、Web ブラウザ Microsoft Internet Explorer が必要です。Internet Explorer で NNMi コンソールを開いてから、ClarusIPC Plus+ のウィンドウを開く URL アクションを起動します。

HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合の無効化

HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合の無効化については、「NNM iSPI for IP Telephony ヘルプ」を参照してください。

HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合のトラブルシューティング

統合の最適化と拡張、および既知の問題については、『NNM iSPI for IP Telephony ヘルプ』を参照してください。

ClarusIPC Plus+ の問題のトラブルシューティングに関するヘルプについては、Clarus Systems のサポートにお問い合わせください。

HP Asset Manager

HP Asset Manager は、IT 資産を含めた企業のインベントリの追跡と維持のための資産管理プラットフォームです。Asset Manager には、以下の機能があります。

- ソフトウェア ライセンス コンプライアンス、資格、およびコストの管理
- 物理 IT 資産および仮想 IT 資産の使用の検出、プロビジョン、管理、改善
- インベントリ、資産、およびサービス データの分散ソースの効率的利用
- 設備、スペース、冷却、電源の管理の自動化

Asset Manager のご購入については、HP 営業担当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 Asset Manager 統合
- HP NNMi-HP Asset Manager 統合の使用法

HP NNMi-HP Asset Manager 統合

HP Network Node Manager i Software が HP Asset Manager と統合されると、Asset Manager ポートフォリオには、NNMi データベースからデバイス情報を自動的に取り込むことができます。

値

HP NNMi-HP Asset Manager 統合には、以下の利点があります。

- 管理対象デバイスのネットワーク トラフィックを削減する。NNMi がデバイスを検出すると、Asset Manager が NNMi トポロジと同期をとります。
- Asset Manager に対して完全なネットワーク インベントリを提供する。このインベントリは、NNMi スパイラル検出により常に最新に保たれます。
- ネットワーク管理設定を簡素化する。ネットワーク検出設定は、NNMi にのみ保管されます。

統合製品

この章の情報は、以下の製品に当てはまります。

- Asset Manager (HP Connect-It 付き)

  サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10

NNMi と Asset Manager は、別々のコンピュータにインストールする必要があります。NNMi 管理サーバーと Asset Manager コンピュータ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。

ドキュメント

HP NNMi-HP Asset Manager 統合については、『HP Connect-It コネクタ ガイド』で詳しく説明されています。**http://h20230.www2.hp.com/selfsolve/manuals** の Connect-It 製品および Integration Connectors 製品のカテゴリから入手できます。

HP NNMi-HP Asset Manager 統合の使用法

HP NNMi-HP Asset Manager 統合を有効化するステップは、Asset Manager サーバー上で行います。

HP NNMi-HP Asset Manager 統合を有効にすると、Asset Manager ポートフォリオに NNMi ノード、インタフェース、および IP アドレス情報が取り込まれます。

HP NNMi-HP Asset Manager 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 Connect-It コネクタ ガイド』を参照してください。

HP Business Service Management トポロジ

HP Business Service Management (BSM) ソフトウェアは、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監視、インフラストラクチャのパフォーマンス監視、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 営業担当者にご相談ください。

この章には、以下のトピックがあります。

- HP NNMi-HP BSM トポロジ統合
- HP NNMi-HP BSM トポロジ統合の有効化
- HP NNMi-HP BSM トポロジ統合の使用法
- HP NNMi-HP BSM トポロジ統合の設定の変更
- HP NNMi-HP BSM トポロジ統合の無効化
- HP NNMi-HP BSM 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 トポロジ統合
- HP NNMi-HP BSM トポロジ統合設定フォームのリファレンス

HP NNMi-HP BSM トポロジ統合

HP NNMi-HP BSM トポロジ統合では、NNMi トポロジを使用して BSM Run-time Service Model (RTSM) にデータを入力します。BSM は、設定項目 (CI) として NNMi トポロジに各デバイスを保存します。BSM ユーザーおよび統合アプリケーションは、ネットワーク デバイス間の関係を確認できます。

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-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 CI に関連付けることができます。詳細については、526 ページの「設定項目の ID」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 BSM CI に関連付けることができます。詳細については、546 ページの「設定項目の ID」を参照してください。

値

HP NNMi-HP BSM トポロジ統合によって、NNMi はネットワーク 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。統合により、BSM とのその他の統合が可能になります。NNMi コンソールから BSM ユーザー インタフェースにアクセスすることはできません。

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

  サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10

NNMi と BSM は別々のコンピュータ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 サーバーのコンピュータ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、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

この章では、BSM 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。ドキュメント スイートは BSM 製品メディアに含まれています。

HP NNMi-HP BSM トポロジ統合の有効化

NNMi では、HP BSM トポロジおよび HP Universal CMDB (UCMDB) を同時に統合できません。この NNMi 管理サーバーで HP NNMi-HP UCMDB 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 BSM 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、HP NNMi-HP BSM 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 Data Flow Management Guide*』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

以下の手順に従って、NNMi 管理サーバーで、NNMi と BSM の間の接続を設定します。

1. *オプション*。インタフェースの RTSM 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 ユーザー インタフェースで **[CI タイプ マネージャ]** 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]**)。
   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 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
      ```

2. *オプション*。RTSM ではドメイン名システム (DNS) 名を使用し、同じノードの複数の CI を調整します。HP Operations Manager も RTSM と同期している場合は、DNS 名に従ってノードに名前を付けるように NNMi を設定します。
   a. NNMi コンソールで **[検出の設定]** フォームを開きます (**[設定] > [検出の設定]**)。
   b. **[ノード名解決]** で以下を実行します。
      — **[最初の選択]** を **[完全 DNS 名]** に設定。
      — **[2 番目の選択]** を **[短い DNS 名]** に設定。
3. NNMi コンソールで、**[HP NNMi-HP BSM 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 Topology]**)。
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は、429 ページの「NNMi 管理サーバー接続」を参照してください。
6. BSM ゲートウェイ 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は、430 ページの「BSM ゲートウェイ サーバー接続」を参照してください。
7. *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は、430 ページの「BSM トポロジ フィルタ」を参照してください。

8 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。

HP NNMi-HP BSM トポロジ統合の使用法

HP NNMi-HP BSM トポロジ統合により、BSM RTSM 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。430 ページの「BSM トポロジ フィルタ」に記載されているとおりにノードを制限できます。

- InfrastructureElement > NodeElement> HardwareBoard

  統合によって BSM 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。

- InfrastructureElement > NodeElement> Interface

  統合によってBSM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。

- InfrastructureElement > NodeElement> PhysicalPort

  統合によって BSM 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 > IpAddress

  統合が BSM に入力するノード CI に関連付けられたインタフェースの IP アドレス。

- InfrastructureElement > NetworkEntity > IpSubnet

  NNMi トポロジのすべてのサブネット。

- 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。

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 の検出と監視の設定を更新し、BSM 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 トポロジ統合は、一方向通信で NNMi 情報と更新を BSM RTSM 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 のエージングポリシーに依存します。

ほかの製品が BSM と統合すると、HP NNMi-HP BSM 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。ユーザーがこの統合を直接操作することはありません。

HP NNMi-HP BSM トポロジ統合の設定の変更

1 NNMi コンソールで、**[HP NNMi-HP BSM 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 Topology]**)。

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は、429 ページの「HP NNMi-HP BSM トポロジ統合設定フォームのリファレンス」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。ovjboss を再起動する必要はありません。

HP NNMi-HP BSM トポロジ統合の無効化

1 NNMi コンソールで、**[HP NNMi-HP BSM 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 Topology]**)。

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。ovjboss を再起動する必要はありません。

HP NNMi-HP BSM トポロジ統合のトラブルシューティング

この項では以下の内容について説明します。

- 427 ページの「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」
- 428 ページの「RTSM の管理対象ノードで CI が重複する」

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 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 ユーザー インタフェースでインタフェース名を表示するには、425 ページの手順 1 の説明に従ってインタフェース 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 コンピュータであり、NNMi 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。

RTSM で、各管理対象ノードの HPOM と NNMi のトポロジ情報を 1 つの CI にマージする場合は、425 ページの手順 2 の説明のとおりに DNS 名に従ってノードに名前を付けるように NNMi を設定します。RTSM では、ノードごとに古い CI が維持されます。

アプリケーション フェイルオーバーと HP NNMi-HP BSM 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 トポロジ統合では、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 BSM サーバーが再設定されます。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 サーバーのフェイルオーバーはサポートされません。

HP NNMi-HP BSM トポロジ統合設定フォームのリファレンス

[HP NNMi-HP BSM トポロジの統合設定] フォームには、NNMi と BSM の間の通信用パラメータが含まれています。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。

[HP NNMi-HP BSM トポロジの統合設定] フォームには、管理者ロールのある NNMi ユーザーのみがアクセスできます。

[HP NNMi-HP BSM トポロジの統合設定] フォームでは、以下の領域に関する情報が収集されます。

- 429 ページの「NNMi 管理サーバー接続」
- 430 ページの「BSM ゲートウェイ サーバー接続」
- 430 ページの「BSM トポロジ フィルタ」

統合設定に変更を適用するには、**[HP NNMi-HP BSM 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 38 に、NNMi 管理サーバーへの接続パラメータをリストします。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 38　NNMi 管理サーバー情報

フィールド	説明
NNMi SSL 有効化	接続プロトコル指定。 • 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。これがデフォルト設定です。 • 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。 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 ゲートウェイ サーバー接続

表 39 には、BSM ゲートウェイ サーバーに接続して BSM RTSM と通信するためのパラメータがリストされています。BSM 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。

表 39　BSM ゲートウェイ サーバー情報

BSM ゲートウェイ サーバー パラメータ	説明
BSM SSL 有効化	BSM に接続するための接続プロトコルの指定。 • BSM が HTTPS を使用するよう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。これがデフォルト設定です。 • BSM が HTTP を使用するよう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。
BSM ホスト	BSM ゲートウェイ サーバーの完全修飾ドメイン名。
BSM ポート	BSM に接続するためのポート。 デフォルトの BSM 設定を使用する場合は、ポート 80 を使用します (BSM への非 SSL 接続の場合)。
BSM ユーザー	BSM RTSM 管理者のユーザー名。
BSM パスワード	BSM RTSM 管理者のパスワード。 BSM 管理者は、以下の URL を使用して、BSM RTSM 管理者のパスワードを変更できます。 **http://<*BSM_hostname*>:21212/ucmdb-ui/applet/applet.jsp**

BSM トポロジ フィルタ

デフォルトでは、HP NNMi-HP BSM 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に関する情報が BSM に伝達されます。BSM 内の NNMi 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、このセクションで説明されるように、オプションのノード グループを 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 - NNMi で、すべての NNMi ノードが BSM トポロジ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 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 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 - NNMi で、監視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 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 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 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 に転送します。

— ノードがトポロジ フィルタ 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 40 は、BSM トポロジ フィルタを指定するためのオプション パラメータをリストし、これらのパラメータに入力する値を説明しています。

表 40　BSM トポロジ フィルタ情報

BSM トポロジ フィルタ パラメータ	説明
トポロジ フィルタ 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 に入力されます。 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。 トポロジ フィルタ ノード グループを指定しない場合、HP NNMi-HP BSM 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。
追加接続ノード グループ	BSM に挿入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 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 に入力されます。 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。 トポロジ フィルタ 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 トポロジ統合は、トポロジ フィルタ 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。 トポロジ フィルタ 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 トポロジ統合は、トポロジ フィルタ 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。 トポロジ フィルタ ノード グループを指定しない場合、HP NNMi-HP BSM 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。

HP Universal CMDB

HP Universal CMDB (UCMDB、ユニバーサル設定管理データベース) 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とアプリケーションの関係についての最新で正確な情報を自動的に維持します。UCMDB は以下のタスクに有益です。

- 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。

UCMDB の購入については、HP 販売員にお尋ねください。

この章には、以下のトピックがあります。

- HP NNMi-HP UCMDB 統合
- HP NNMi-HP UCMDB 統合の使用法

HP NNMi-HP UCMDB 統合

HP NNMi-HP UCMDB 統合では、UCMDB との間で NNMi トポロジ情報を共有します。UCMDB は、設定項目 (CI) として NNMi トポロジに各デバイスを保存します。UCMDB 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、UCMDB ユーザー インタフェースおよび NNMi コンソール から入手できます。

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。

- HP NNMi-HP BSM Operations Management 統合では、NNMi 管理デバイスに関するインシデントを UCMDB CI と関連付けることができます。詳細については、526 ページの「設定項目の ID」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 管理デバイスに関するインシデントを UCMDB CI と関連付けることができます。詳細については、546 ページの「設定項目の ID」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。

- UCMDB

サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10

NNMi と UCMDB は同じコンピュータ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 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 管理サーバーは Windows システムであり、UCMDB サーバーは 2 番目の Windows システムです。

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、UCMDB 製品メディアに収録されている『検出および統合コンテンツ ガイド』の「Network Node Manager i (NNMi) と HP Universal CMDB との統合」の章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。HP NNMi-HP BSM トポロジ統合をこの NNMi 管理サーバーで設定する場合は、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。

- 423 ページの「HP Business Service Management トポロジ」の説明に従って、HP NNMi-HP BSM 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 Data Flow Management Guide*』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

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、『検出および統合コンテンツ ガイド』の「Network Node Manager i (NNMi) と HP Universal CMDB との統合」の章を参照してください。

HP Business Availability Center My BSM

HP Business Availability Center (BAC) ソフトウェアは、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監視、インフラストラクチャのパフォーマンス監視、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。BAC には、My BSM ポータルが含まれており、これを使用して、レポートやリアルタイムの製品パフォーマンス情報を表示します。(BAC バージョン 8.00 以前は、ポータルは My BAC と呼ばれていました)。

この章には、以下のトピックがあります。

- HP NNMi-HP BAC My BSM 統合
- My BSM のデフォルト NNMi モジュール
- デモ ポートレットの設定
- カスタム NNMi ポートレットの作成
- HP NNMi-HP BAC My BSM 統合のシングル サインオンの設定
- HP NNMi-HP BAC My BSM 統合のトラブルシューティング
- HP NNMi-HP BAC My BSM 設定フォームのリファレンス

HP NNMi-HP BAC My BSM 統合

The HP NNMi-HP BAC My BSM 統合は、My BSM ポータルで NNMi を表示するためのイネーブルメントです。この統合には、NNMi と NNM iSPI for Performance ポートレットを My BSM ポータルに追加するテンプレートが提供されています。ポータルの簡単なデモとして、NNMi コンソールの設定ツールを使用して、ご利用の環境に合わせたテンプレートのカスタマイズを行えます。

My BSM 管理者は、My BSM 管理者の標準インタフェースを使用して、デフォルト ポートレットの設定とアクセス権をカスタマイズできます。また、そのインタフェースで、NNMi や NNMi Smart Plug-ins (NNM iSPI) のその他のビューのカスタム ポートレットを作成したり、複数の NNMi 管理サーバーのビューを 1 つのポータル ページに集約したりすることもできます。

値

HP NNMi-HP BAC My BSM 統合では、My BSM ポータルから取得する情報を拡張できます。

統合製品

この章の情報は、以下の製品に当てはまります。

- BAC

サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

BAC バージョン 9.x と統合するには、BAC コンポーネント ギャラリーを使用します。

- NNMi 9.10

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

この章では、NNMi コンソールを使用して、My BSM のデフォルト NNMi ポートレットを設定する方法を説明します。

My BAC の設定方法と管理方法は、BAC 7.x の製品メディアに含まれる『My BAC 使用ガイド』で説明しています。

My BSM の設定方法と管理方法は、BAC 8.x の製品メディアに含まれる『My BSM 使用ガイド』で説明しています。

My BSM のデフォルト NNMi モジュール

NNMi の NNMi コンソールでは、以下の My BSM モジュールを使用して設定を行います。

- NNMi デモ モジュールは、`NOC_Demo_Portal.xml` テンプレート ファイルに定義されています。このモジュールには、表 41 に示される一部の主要ネットワーク ステータス情報が含まれます。
- NNMi および NNM iSPI for Performance デモ モジュールは、`NOC_Demo_Portal_iSPIPerf.xml` テンプレート ファイルに定義されています。このモジュールは、NNMi デモ モジュールのネットワーク ステータス情報にいくつかの NNM iSPI for Performance レポートを追加します。437 ページの表 42 にこのモジュールの説明が記載されています。

表 41　NNMi デモ モジュールのコンテンツ

ページ	ポートレット	ポートレットの説明
概要マップ	主要操作マップ	特定のノード グループの NNMi トポロジ マップです。
ネットワーク ステータス / デバイス ヘルス	ノード グループのステータス	NNMi コンソールの特定のノード グループに使用する **[アクション] > [ステータスの詳細]** メニュー コマンドの結果に相当します。
	ネットワーク ステータス	NNMi コンソールの **[ノード グループ]** インベントリ ビューに相当します。

表 42　NNMi および NNM iSPI for Performance デモ モジュールのコンテンツ

ページ	ポートレット	ポートレットの説明
概要マップ	主要操作マップ	特定のノード グループの NNMi トポロジ マップです。
ネットワーク ステータス / デバイス ヘルス	ノード グループのステータス	NNMi コンソールの特定のノード グループに使用する **[アクション] > [ステータスの詳細]** メニュー コマンドの結果に相当します。
	ネットワーク ステータス	NNMi コンソールの **[ノード グループ]** インベントリ ビューに相当します。
	Top-N メモリ使用率	上位 10 個のノードをメモリ使用率別に表示するライブ NNM iSPI for Performance コンポーネント状況レポートです。
	Top-N CPU 使用率	上位 10 個のノードを CPU 使用率別に表示するライブ NNM iSPI for Performance コンポーネント状況レポートです。
NNM iSPI for Performance の例外	コンポーネントの例外別 Top-N デバイス	CPU 使用率の例外別とメモリ使用率の例外別に上位 5 個のノードを表示するライブ NNM iSPI for Performance コンポーネント状況ダッシュボードです。

デモ ポートレットの設定

このセクションでは、My BSM デモ モジュールの初期設定を説明します。My BSM 管理者は、ポートレットのコンテンツとポートレットへのユーザー アクセスを完全にカスタマイズできます。

1 NNMi 管理サーバーで、モジュール設定 XML ファイルを作成します。

   a NNMi コンソールで、**[HP NNMi-HP BAC My BSM の設定]** フォームを開きます (**[統合モジュールの設定] > [HP BAC My BSM]**)。

   b カスタマイズする名前付き XML ファイルを 1 つ選択します。

      — 環境に NNM iSPI for Performance がインストールされていない場合は、`NOC_Demo_Portal.xml` ファイルを選択します。

      — 環境に NNM iSPI for Performance がインストールされている場合は、`NOC_Demo_Portal_iSPIPerf.xml` ファイルを選択します。

   c **[ロードする]** をクリックします。

   d **[HP NNMi-HP BAC My BSM の設定]** フォームの各ページで、入力されているテキストを必要に応じて編集し、**[次]** をクリックします。これらのフィールドの詳細は、444 ページの「HP NNMi-HP BAC My BSM 設定フォームのリファレンス」を参照してください。

   e **[HP NNMi-HP BAC My BSM の設定]** フォームのすべてのページを編集したら、**[終了]** をクリックして XML ファイルをコンピュータに保存します。

   f **[HP NNMi-HP BAC My BSM の設定]** フォームを閉じます。

2 モジュール設定を BAC にインポートします。

   a BAC の **[管理者]** タブで、**[My BSM]** (または **[My BAC]**) の下にある **[ポートレットとモジュールをインポート]** をクリックします。

   b **[My BSM オブジェクトをインポート]** ページ (または **[My BAC オブジェクトをインポート]** ページ) で **[参照]** をクリックし、NNMi コンソールから保存した XML ファイルを選択します。

   c **[同一のポートレット定義を置き換える]** チェックボックスをオンにします。

   d **[同一のモジュールを置き換える]** チェックボックスをオンにします。

   e **[インポート]** をクリックします。

      [インポートのステータス] ウィンドウに、操作の結果が表示されます。インポートに失敗した場合は、チェックボックスが選択されていることを確認し、インポートを再試行します。

3 My BSM または My BAC でモジュールを表示します。

   - 各ポートレットに期待する情報が表示されていることを確認します。
   - My BSM または My BAC 管理者ツールを使用して、新しいポートレットにアクセスできるユーザーの定義、ページの再編成、ポートレットの定義の編集などを行います。

カスタム NNMi ポートレットの作成

以下は、NNMi または iSPI 情報を表示する新しいポートレットを最も簡単に作成する方法です。

1 My BSM 管理者インタフェースで、既存の NNMi ポートレットの定義をコピーします。

2 新しいポートレットの定義に記載の URL をポータルに表示する情報にポイントするように変更します。

ポートレットの定義を編集するときは、デモ ポートレットで使用されている HTML コードの構造に従って行います。HTML コードの構造の説明については、440 ページの「ポートレットの定義 HTML リファレンス」を参照してください。

ポートレット URL の特定

NNMi コンソール ウィンドウの URL

NNMi コンソール ウィンドウを直接開く URL を作成する方法については、NNMi コンソール の **[ヘルプ] > [NNMi ドキュメントライブラリ] > 「NNMi を別の場所で URL と統合」**を参照してください。

NNM iSPI for Performance レポートの URL

NNM iSPI for Performance レポートを起動する URL を特定する手順は、レポートを表示する Web ブラウザによって異なります。

レポートにアクセスする URL は Web ブラウザの種類に関わらず、同一のものが使用されます。

Mozilla Firefox の場合、以下の手順に従って、NNM iSPI for Performance レポートを起動する URL を特定します。

1 NNM iSPI for Performance レポートを実行します。

2 *オプション。* レポートの上部にある **[オプションを表示]** をクリックし、レポートのビューをカスタマイズします。

3 レポートの上部にある **[URL を表示]** をクリックします。

レポートの URL がレポートのバナーとカスタマイズのリンクの下に表示されます。その URL をコピーして、ポートレットの定義に使用できます。

4 *オプション。* **[URL を隠す]** をクリックして、ビューからレポートの URL を非表示にします。

Microsoft Internet Explorer では、以下の手順に従って、NNM iSPI for Performance レポートを起動する URL を特定します。

1 NNM iSPI for Performance レポートを実行します。

2 *オプション。* レポートの上部にある **[オプションを表示]** をクリックし、レポートのビューをカスタマイズします。

3 レポートの上部にある **[ブックマークを追加]** をクリックします。

4 **[お気に入りに追加]** ウィンドウで **[追加]** をクリックします。

5 お気に入りのリストで、手順 4 で作成したお気に入りを右クリックし、**[プロパティ]** をクリックします。

[URL] フィールドにレポートの URL が表示されます。その URL をコピーして、ポートレットの定義に使用できます。

ポートレットの定義 HTML リファレンス

BAC では、HTMLPortlet タイプに以下のルールが適用されます。

- 標準的な二重引用符 (") ではなく、単一引用符 (') を使用します。
- iframe の開始タグ (<iframe>) には対となる iframe 終了タグが必要です (</iframe>)。一部の Web ブラウザは、空のエレメント <iframe/> タグを正しく解析しません。
- iframe の定義で、以下のいずれかの値を id に指定します。

id の値	説明
nnmi-portlet	NNMi URL を表示する iframe の ID です。この ID によって一貫した設定で人間が読み取ることができます。
nnmi-auth	NNM iSPI for Performance へのシングル サインオンを管理する iframe の ID です。この ID の値は、NNM iSPI for Performance ポートレットをロードする JavaScript 関数によって解釈されます。
ispiperf-portlet	NNM iSPI for Performance レポートの URL を表示する iframe の ID です。この ID の値は、NNM iSPI for Performance ポートレットをロードする JavaScript 関数によって解釈されます。

NNMi ポートレットの HTML 構造

NNMi の URL を表示する BAC ポートレットには、表示する NNMi の URL を識別する iframe エレメントが 1 つあります。以下は、その構造です。

```
<html>
<head></head>
<body>
<iframe id='nnmi-portlet' src='<NNMi_URL>'></iframe>
</body>
</html>
```

<NNMi_URL> を NNMi コンソール ウィンドウを開く URL に置き換えます。

たとえば、以下のコードは、Routers ノード グループのステータスを表示するポートレットを定義しています。この例の高さと幅の値は、このポートレットに推奨される値です。必要に応じてこれらの値を変更できます。

```
<html>
<head></head>
<body>
<iframe id='nnmi-portlet'
  src='http://nnmi.example.com:8004/nnm/launch
    ?cmd=runTool
    &tool=nodegroupstatus
    &nodegroup=Routers
    &menus=false'
  width='100%'
  height='425px'>
</iframe>
</body>
</html>
```

NNM iSPI for Performance ポートレットの HTML 構造

NNM iSPI for Performance レポートの URL を表示する BAC ポートレットには、以下のエレメントが含まれます。

- ポートレットのヘッダーに記述される、`loadIspiPerf()` JavaScript 関数の宣言。この宣言によって、表示する NNM iSPI for Performance レポートが定義されます。
- NNMi から NNM iSPI for Performance へのシングル サインオンを処理する 1 つの iframe エレメント。
- ポートレットのヘッダーの `loadIspiPerf()` 関数宣言で指定された NNM iSPI for Performance レポートを表示する 2 つ目の iframe エレメント。

以下は、NNM iSPI for Performance レポートの URL を表示する BAC ポートレットの構造です。

```
<html>
<head>
<script id='ispiperf-load'>function loadIspiPerf()
{
  var ispiperf_url='<Report_URL>';
  document.getElementById('ispiperf-portlet').src =
    ispiperf_url;
}
</script>
</head>
<body onload='loadIspiPerf();'>
<iframe id='nnmi-auth'
  src='http:<NNMi_host>:<NNMi_port>/nnm/launch?cmd=isRunning'>
</iframe>
<iframe id='ispiperf-portlet'></iframe>
</body>
</html>
```

<Report_URL> を NNM iSPI for Performance レポートを開く URL に置き換えます。*<NNMi_host>* および *<NNMi_port>* をそれぞれ NNMi 管理サーバーの完全修飾ドメイン名と NNMi にアクセスするためのポート番号に置き換えます。

たとえば、以下のコードは、上位 N ノードのノード状況レポートを表示するポートレットを定義しています。この例の高さと幅の値は、このポートレットに推奨される値です。必要に応じてこれらの値を変更できます。

```
<html>
<head>
<script id='ispiperf-load'>function loadIspiPerf()
{
  var ispiperf_url=
    'http://nnmi.example.com:8004/ssoservlet/protected
    /reports
      ?reportURL=http://ispiperf.example.com:9300/PerfSpi
      /PerfSpi
        ?package=NodeHealth
          &report=Top%20N%20Live
          &element=All%20Nodes/Components&timeperiod=
          &dow=
          &hod=
          &metric=CPU%20Utilization%20(Avg%25)
          &namespaceID=ErsAuthenticationProvider
          &ssoDomain=example.com';
```

```
    document.getElementById('ispiperf-portlet').src =
      ispiperf_url;
  }
  </script>
  </head>
  <body onload='loadIspiPerf();'>
  <iframe id='nnmi-auth'
    src='http://nnmi.example.com:8004/nnm/launch
      ?cmd=isRunning'
    width='100%'
    height='1px'>
  </iframe>
  <iframe id='ispiperf-portlet'
    width='100%'
    height='750px'>
  </iframe>
  </body>
  </html>
```

HP NNMi-HP BAC My BSM 統合のシングル 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。BAC My BSM におけるシングル サインオンの設定方法については、143 ページの「NNMi と HP BSM または HP BAC 間のシングル サインオンの設定」を参照してください。

HP NNMi-HP BAC My BSM 統合のトラブルシューティング

NNMi ポートレットがサインイン ページとして表示される

シングル サインオンの設定を確認します。

1 My BSM にログオンするユーザー名で NNMi コンソール にサインインします。

   サインインに失敗した場合は、My BSM ユーザーのアカウントを設定するように NNMi 管理者に依頼してください。

2 442 ページの「HP NNMi-HP BAC My BSM 統合のシングル サインオンの設定」に記載されているとおり、BAC および NNMi が同一の初期化ストリングを使用していることを確認します。

443 ページの「シングル サインオンが正しく機能しない」も参照してください。

NNMi ポートレットが正しくロードしない

My BSM 管理者インタフェースで、ポートレット URL の NNMi 管理サーバーのホスト名とポート番号を確認してください。

NNM iSPI for Performance ポートレットが正しくロードしない

My BSM 管理者インタフェースで、ポートレット URL の NNM iSPI for Performance サーバーのホスト名、ポート番号、およびシングル サインオンのドメインを確認してください。

NNM iSPI for Performance ポートレットに AsynchWait_Requests エラーが表示される

BAC ポータル ページは NNM iSPI for Performance ポートレットをロードするとき、NNM iSPI for Performance Cognos データベースに情報を要求します。ページに複数の NNM iSPI for Performance ポートレットが含まれる場合、単一の Web ブラウザ セッションから Cognos データベースへの同時要求が行われ、その結果 `AsynchWait_Requests` エラーが発生する場合があります。ポータル ページを再ロードしてください。

シングル サインオンが正しく機能しない

すべての NNMi および NNM iSPI for Performance ポートレットがロードしません。以下に類似したメッセージにより、Web ブラウザが閉じる場合があります。

```
The page you requested cannot be displayed because the LW-SSO host
has logged out.
```

シングル サインオン統合を使用するすべてのアプリケーション サーバーが、最大 15 分の差異の範囲で同じ GMT 時間に設定されていることを確認してください。

ポートレットの定義を保存すると、My BSM で HTML 検証エラーが発生する

My BSM で新しいポートレットを保存する前に、BAC 設定ファイルで設定を行う必要があります。

`<HP Business Availability Center ルート ディレクトリ >¥HPBAC¥conf¥dashboard.properties` ファイルを編集し、以下の行を追加してください。

```
Block-URL-Injections=false
```

HP NNMi-HP BAC My BSM 設定フォームのリファレンス

表 43 は、**[HP NNMi-HP BAC My BSM の設定]** フォームのページに含まれるフィールドを示します。NNM iSPI for Performance 管理者と相談し、NNM iSPI for Performance フィールドに使用する正しい値を指定してください。テキスト フィールドに使用できる文字に制限はありません。NNMi は、設定された値を検証しません。My BSM ポータルで新しいポートレットを確認してください。

表 43　モジュールの設定情報

フィールド	説明
名前	ポータル モジュールの名前。このテキストを使用して、My BSM ポータル内を移動します。
説明	ポータル モジュールを説明するテキスト。このテキストは、My BSM 管理者インタフェースに表示されます。
ページ タイトル	ポータル ページの名前。このテキストを使用して、ポータル内を移動します。
ポートレット タイトル	ポータルに表示されるポートレットの名前。
ポートレットのタイプ	My BSM 設定に必要なフィールド。現在、これは読み取りのみのフィールドです。
NNMi マシン	NNMi 管理サーバーにアクセスするための URL。このフィールドには、現在の NNMi コンソールセッション用に NNMi 管理サーバーに接続するためのホスト名とポート番号が事前に入力されています。 • デフォルトの NNMi 管理サーバーにアクセスするポートレットの場合、デフォルトの設定をそのまま使用します。 • 別の NNMi 管理サーバーにアクセスするポートレットの場合、正しい URL を手動で入力します。
NNMi ノードグループ	現在の NNMi コンソール セッションの NNMi 管理サーバーにあるノード グループのリスト。 • ポートレットがデフォルトの NNMi 管理サーバーにアクセスする場合、このリストからノード グループを選択します。 • ポートレットが別の NNMi 管理サーバーにアクセスする場合、正しいノード グループの名前を手動で入力します。
iSPI for Performance マシン	NNM iSPI for Performance サーバーにアクセスするための URL。これは、事前入力済みのフィールドで、現在の NNM iSPI for Performance セッションで NNMi コンソール サーバーに接続するホスト名とポート番号です。 • デフォルトの NNM iSPI for Performance サーバーにアクセスするポートレットの場合、デフォルトの設定をそのまま使用します。 • 別の NNM iSPI for Performance サーバーにアクセスするポートレットの場合、正しい URL を手動で入力します。

表 43　モジュールの設定情報 (続く)

フィールド	説明
SSO ドメイン	NNM iSPI for Performance へのシングル サインオンのドメイン。
[iSPI for Performance ポートレットを無効にする] チェックボックス	**[iSPI for Performance ポートレットを無効にします]** チェックボックスは、NNM iSPI for Performance にアクセスするポートレットを定義する設定フォームのページにあります。 ページを表示したときにこのチェックボックスがオンである場合、この NNMi 管理サーバーに NNM iSPI for Performance は設定されていません。そのため、NNM iSPI for Performance に関連するフィールドは設定解除されます。 このチェックボックスをオフにしてフィールドを有効にし、NNM iSPI for Performance にアクセスするための情報を手動で入力します。

HP Network Automation

HP Network Automation Software (NA) は、グローバルに分散されたマルチベンダ ネットワークでの設定やソフトウェア変更を、プロセスの自動化によって追跡、規制、および自動化します。

NA の購入に関する詳細については、HP 営業担当にお尋ねください。

この章には、以下のトピックがあります。

- HP NNMi-HP NA 統合
- HP NNMi-HP NA 統合の有効化
- HP NNMi-HP NA 統合の使用法
- HP NNMi-HP NA 統合の変更
- HP NNMi-HP NA 統合の無効化
- HP NNMi-HP NA 統合のトラブルシューティング
- HP NNMi-HP NA 統合設定フォームのリファレンス
- HP NNMi-HP NA 統合設定フォームのリファレンス
- NA の NNMi 統合設定リファレンス

HP NNMi-HP NA 統合

HP NNMi-HP NA 統合は、NA 設定変更の検出機能と NNMi ネットワーク監視機能を合わせ、障害が発生した場合にユーザーにより多くの情報を提供します。

NNMi と Cisco Network Compliance Manager (NCM) の統合は、HP NNMi-HP NA 統合と同じ方法で動作します。この章の内容は、HP NNMi-Cisco NCM 統合にも該当します。

統合によって、以下の機能が提供されます。

- 所有コストを下げて、プロビジョニング済みデバイスの管理範囲を適切にするため、NNMi と NA トポロジを同期する。
- 特定の NNMi インシデントが発生したとき、NA デバイス診断を自動的に実行する。
- NA がデバイス設定更新を適用しているときにデバイスがサービス停止中になっている間、NNMi で不要なアラームを防止する。
- 管理対象デバイスにアクセスするための情報で NNMi 設定を更新する。

また、既存の NNMi コンソールを使用せずに、NA に接続して、NA 管理デバイスの情報や設定変更イベントの情報を表示することができます。NA では、ユーザーが必要な資格情報を持っている場合に NA 機能を実行できます。

HP NNMi-HP NA 統合では、NNMi コンソールに、NA に接続を開いたり NA が管理するデバイスの設定情報を表示するためのメニュー項目が追加されます。これらのツールを使用して以下を実行できます。

- ベンダー、モデル、モジュール、オペレーティング システムのバージョン、最近の診断結果など、デバイスの詳細情報を表示する
- デバイスの設定変更と設定履歴を表示する
- 設定 (通常、最も最近、または最後の以前の設定) を比較し、変更内容、変更理由、および変更適用者を表示する
- デバイスの適合情報を表示する
- NNMi ノードから NA Diagnostics とコマンド スクリプトを実行する
- 不整合な速度設定または二重設定の接続を検出する

これらの機能は、NA で設定されていないネットワーク デバイスまたは変更の検出が無効にされている NA デバイスでは利用できません。

値

HP NNMi-HP NA 統合では、すでに NNMi と NA を実行している環境で、以下の機能や利点が提供されます。

- アラーム統合 - NNMi 統合は、NNMi コンソールに NA 設定変更情報を示し、設定変更がネットワークの障害によるものであるかどうかを迅速に識別できるようにします。NNMi 内から、NA 機能にすばやくアクセスし、特定の設定変更やデバイス情報の表示、変更適用者の識別、ネットワーク操作を復旧するために以前の設定へのロールバックを行えます。多くのネットワーク使用停止は、デバイスの設定エラーに由来するものであるため、この機能によって問題の特定とネットワーク ダウンタイムの解決における対応時間が改善されます。
- NNMi から NA 設定履歴へのアクセス - NNMi コンソールでは、デバイス レベルのメニューから設定変更を確認するための NA 機能にアクセスできます。この機能は、NA データベースのデバイスについて、設定変更を隣り合わせに表示するため、変更内容を簡単に確認できます。また、設定の履歴を表示することもできます。
- 操作の効率性 - ネットワーク オペレータは、1 つの画面で 2 つのデータ ソースの情報を監視し、調査することができます。

統合製品

この章の情報は、以下の製品に当てはまります。

- NA

サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10

NNM iSPI NET ライセンスは、この統合には必要なくなりました。

統合は、1 つの NNMi 管理サーバーと接続している 1 つの NA サーバーに制限されます。NNMi と NA は、同じネットワーク セグメント (NA 領域とも呼ばれる) に存在する必要があります。

NNMi および NA は、同一のコンピュータまたは異なるコンピュータにインストールできます。

NNMi および NA が同一のコンピュータ上で正しく実行するには、NA をインストールする前に NNMi をインストールする必要があります。

以下のいずれかの設定で、2 つの製品を異なるコンピュータにインストールできます。

- 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、NA サーバーを Windows システムにインストールできます。
- 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、NA サーバーを別の Windows システムにインストールできます。

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

この章では、統合の設定方法と使用方法について説明します。

HP NNMi-HP NA 統合の有効化

HP NNMi-HP NA 統合を有効にすると、NNMi 管理サーバーは、管理対象環境の限定的なトポロジ マスターとして設定されます。NNMi では 1 つのノード グループを作成し、NA インベントリと同期するノードを含めます。453 ページの「NNMi と NA の間のトポロジ同期」で説明したように、統合により、このノード グループの内容は NA Default Site パーティションと同期されます。

このセクションでは、以下の手順について説明します。

- 450 ページの「NNMi 9.0x からアップグレードされた統合設定」
- 451 ページの「新規統合設定」

NNMi 9.0x からアップグレードされた統合設定

NNMi バージョン 9.10 以前は、NA が NNMi コネクタ ツールを提供し、NNMi と NA の間の通信を確立していました。現在は NNMi がこの機能を提供します。NA が提供する NNMi コネクタは使用されなくなります。

HP NNMi-HP NA 統合を NNMi 9.0x 管理サーバーで設定した場合、NNMi 9.10 にアップグレードすると、統合は無効になります (設定値は残ります)。アップグレードした NNMi 管理サーバーから統合を有効にするとき、NA データベースのオブジェクトには NNMi UUID がまだ含まれており、現在の NNMi トポロジと同期されます。

統合により、NNMi コンソールと NA ユーザー インタフェースの間でシングル サインオンが提供されます。

NNMi 9.10 管理サーバーで HP NNMi-HP NA 統合を有効にするには、以下の手順を実行します。

1. NNMi システムおよびデバイスのサポート マトリックスの「統合」セクションにリストされているサポート対象バージョンに NA がアップグレードされていることを確認します。
2. NNMi 管理サーバーから NNMi コネクタをアンインストールします。
   - *Windows* の場合 : [コントロール パネル] を開き、**[プログラムの追加と削除]** をクリックして、**[HP NA - HP Network Node Manager コネクタ]** を削除します。
   - *Linux or Solaris* の場合 : 以下のコマンドを実行します。

     $NAINSTALLDIR/UninstallConnector/Uninstall¥ NA

     $NAINSTALLDIR のデフォルト値は、/opt/NA です。
3. システムから、残りの integration.jar ファイルを削除します。
   a. NA ManagementEngine サービスを停止します。
      — *Windows* の場合 : **[サービス]** コントロールパネル (**[スタート] > [設定] > [コントロール パネル] > [管理ツール] > [サービス]**) を開きます。サービスのリストから、**[TrueControl ManagementEngine]** を右クリックし、**[停止]** をクリックします。
      — *Linux or Solaris* の場合 : 以下のコマンドを実行します。

      /etc/init.d/truecontrol stop

   b. 以下の場所から、integration.jar ファイルを手動で削除します。
      — *Windows*: %NAINSTALLDIR%¥server¥ext¥jboss¥server¥default¥integration.jar
      — *Linux or Solaris*: $NAINSTALLDIR/server/ext/jboss/server/default/integration.jar
   c. NA ManagementEngine サービスを再起動します。
      — *Windows* の場合 : **[サービス]** コントロールパネル (**[スタート] > [コントロール パネル] > [管理ツール] > [サービス]**) を開きます。サービスのリストで、**[TrueControl ManagementEngine]** を右クリックし、**[開始]** をクリックします。
      — *Linux or Solaris* の場合 : 以下のコマンドを実行します。

      /etc/init.d/truecontrol restart
4. *オプション*。145 ページの「NNMi と HP NA 間のシングル サインオンの設定」の説明に従い、NNMi と NA の間でシングル サインオンを設定します。

5 NNMi コンソールで NNMi から NA への接続を以下のように設定します。

   a **[HP NNMi-HP NA 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 NA]**)。

   b **[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。

   [HP NNMi-HP NA の統合設定] フォームには NNMi 9.0x 設定の値が含まれています。このフォームの新しいフィールドは、デフォルト値に設定されています。

   c 新しい統合設定フィールド (**[トポロジ フィルタ ノード グループ]**、**[トポロジ同期間隔]**、**[NA のデバイス ドライバの検出]**) に値を入力します。

   これらのフィールドの詳細は、466 ページの「統合動作」を参照してください。

   d 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。NA 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 メッセージのテキストを参考に NA サーバーに接続するための値を調整してください。

6 NNMi コンソールの **[アクション]** メニューで NA メニュー項目を使用できない場合、NNMi コンソールからログアウトして、もう一度ログインしてください。

新規統合設定

HP NNMi-HP NA 統合を有効にするには、以下の手順を実行します。

1 *オプション*。145 ページの「NNMi と HP NA 間のシングル サインオンの設定」の説明に従い、NNMi と NA の間でシングル サインオンを設定します。

2 *オプション*。同期したトポロジのデバイスのドライバが統合によって検出されるようにする場合は、NNMi トポロジのノードに SNMP 設定を指定します。NA ユーザーインタフェースで以下の手順を実行します。

   a **[デバイスのパスワード ルール]** ページを開きます (**[デバイス] > [デバイス ツール] > [デバイスのパスワード ルール]**)。

   b 1 つ以上のパスワード ルールを作成し、NNMi トポロジのノードとやり取りする方法を指定します。

3 NNMi コンソールで NNMi から NA への接続を以下のように設定します。

   a **[HP NNMi-HP NA 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 NA]**)。

   b **[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。

   c 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は、465 ページの「NNMi 管理サーバー接続」を参照してください。

   d NA 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は、465 ページの「NA サーバー接続」を参照してください。

e 残りのフィールドに値を入力します。

これらのフィールドの詳細は、466 ページの「統合動作」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。NA 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 メッセージのテキストを参考に NA サーバーに接続するための値を調整してください。

4 *オプション*。NA ユーザー インタフェースにおいて、統合によって提供される NA 機能のデフォルト設定を以下のように変更します。

a **[管理設定 - 第三者統合]** ページを開きます (**[管理者] > [管理設定] > [第三者統合]**)。

b **[第三者統合]** で **[使用可能]** が選択されていることを確認します。

c 以下いずれかのフィールドで、選択内容を変更します。

— **タスク後にホストを再検出**

— **サービス停止中イベント**

— **デバイス タスクが失敗した場合**

— **タスク完了後にデバイス適合チェックに失敗した場合**

— **SNMP コミュニティ文字列を伝播**

これらのフィールドの詳細は、467 ページの「NA の NNMi 統合設定リファレンス」を参照してください。

d ページの下にある **[保存]** をクリックします。

5 *オプション*。統合により、不整合な速度設定や全二重設定の接続を検出するには、NA トポロジに NNMi デバイスのインタフェース用の MAC アドレスを入力します。NA ユーザー インタフェースで以下の手順を実行します。

a NNMi トポロジの各ノードについて、NNMUuid プロパティが NA インベントリの対応するデバイスに設定されていることを確認します。

統合トポロジ同期プロセスにより、NNMUuid プロパティが設定されます。このプロパティは、NA のデバイス ページの **[デバイスの詳細]** セクションにリストされています。

b **[デバイスのパスワード ルール]** ページ (**[デバイス] > [デバイス ツール] > [デバイスのパスワード ルール]**) で、1 つ以上のパスワード ルールを作成して、NNMi トポロジのノードとやり取りする方法を指定します。

451 ページの手順 2 でパスワード ルールを作成した場合は、再作成する必要はありません。

c **[新規タスク - ドライバの検出]** ページ (**[デバイス] > [デバイスのタスク] > [ドライバの検出]**) で、NNMi トポロジからインポートされたデバイスのドライバを検出します。

ドライバを検出するように統合を設定した場合は、統合によってこの手順はすでに完了しています。

d NNMi トポロジからインポートされたデバイスのスナップショットを作成します (**[デバイス] > [デバイスのタスク] > [スナップショットの作成]**)。

ドライバを検出するように統合を設定した場合は、統合によってこの手順はすでに完了しています。

e NNMi トポロジからインポートされたデバイスに対し、**NA トポロジ データの収集** 診断を実行します (**[デバイス] > [デバイスのタスク]> [Diagnostics を実行]**)。

f NNMi トポロジと同期された各デバイスに、各インタフェース用の MAC アドレスがあることを確認します。

デバイスのページで、**[表示] > [デバイスの詳細] > [MAC アドレス]** をクリックして、そのデバイスの MAC アドレスを表示します。

6 NNMi コンソールの **[アクション]** メニューで NA メニュー項目を使用できない場合、NNMi コンソールからログアウトして、もう一度ログインしてください。

HP NNMi-HP NA 統合の使用法

HP NNMi-HP NA 統合は、NNMi と NA の両方に機能を追加します。この項では以下の内容について説明します。

- 453 ページの「NNMi と NA の間のトポロジ同期」
- 455 ページの「統合が提供する NNMi 機能」
- 458 ページの「統合により提供される NA 機能」

NNMi と NA の間のトポロジ同期

HP NNMi-HP NA 統合では、NA Default Site パーティションのデバイスで、指定した NNMi 同期ノード グループのノードのトポロジが動的に同期されます。統合により、ホスト名と IP アドレスが必要に応じて比較され、NNMi ノードと NA デバイスが照合されます。統合により、同期されたそれぞれの NNMi ノードに NA ID が追加され、同期されたそれぞれの NA デバイスに NNMi UUID が追加されます。

[HP NNMi-HP NA の統合設定] フォームの **[トポロジ フィルタ ノード グループ]** パラメータでは、NNMi 同期ノード グループを指定します。

この同期は以下のように行われます。

- **[HP NNMi-HP NA の統合設定]** フォームで統合を初めて有効にすると、統合によって、NNMi 統合ノード グループと NA Default Site パーティションの間で完全なトポロジ同期が実行されます。
  - 同期ノード グループの NNMi ノードが NA に存在しない場合は、統合によってこれらのノードが NA Default Site パーティションに追加されます。
  - 同期ノード グループの NNMi ノードが NA にすでに存在するが NA Default Site パーティションに存在しない場合は、統合によってこれらのデバイスが NA Default Site パーティションに移動されます。
  - NA Default Site パーティションのデバイスが NNMi 同期ノード グループに存在しない場合は、統合によってこれらのデバイス用に検出ヒントが NNMi に送信されます。NNMi の自動検出ルール設定によって、これらのノードを検出するかどうかが決まります。NNMi のノードグループ設定によって、NA からヒントを受けたデバイスがどのノードグループに含まれるかが決まります。

    NA Default Site パーティションには、NNMi 同期ノード グループに存在しないノードを含めることができます。同期の完了後、NNMi 同期ノード グループのすべてのノードは、NA Default Site パーティションに置かれます。

- 最初の同期後、統合によってトポロジ同期は以下のように維持されます。
  - 新しいノードが NNMi 同期ノード グループに追加されると、統合によって、NA Default Site パーティションにこのデバイスが作成されます。
  - 新しいデバイスが NA Default Site パーティションに追加されると、統合によって検出ヒントが NNMi に送信されます。
  - 同期されたノードが NNMi から削除されると、統合によって NA の対応するデバイスが管理対象外になります。NA で管理対象外になったデバイスのデバイス履歴は、まだ使用可能です。
  - 同期デバイスが NA から削除されると、統合によって NNMi トポロジから対応するノードが削除されます。

    同期ノードが NNMi 同期ノード グループから別のノード グループに移動しても、NA インベントリはすぐには影響されません。ただし、このノードが後で NNMi から削除されると、統合によって NA の対応するデバイスが管理対象外になります。同じように、このノードが後で NA から削除されると、統合によって対応するノードが NNMi トポロジから削除されます。

  - 完全なトポロジ同期は、統合によって 2 つの製品間で定期的に実行されます。この定期的な同期は、統合が最初に有効になったときに行われる同期と同じように処理されますが、統合では、NNMi トポロジではなく、NA インベントリにあるデバイス用に、NNMi に追加の検出ヒントは送信されないという点が異なります。

    [HP NNMi-HP NA の統合設定] フォームの **[トポロジ同期間隔]** パラメータでは、定期トポロジ同期の頻度を指定します。

定期的同期の考慮事項

トポロジ同期の間隔を選択するときは、以下のガイドラインを考慮してください。

- トポロジ同期はフェイルセーフ メカニズムです。NNMi 管理サーバーと NA サーバーの間で接続の信頼性が高い場合、トポロジ同期の間隔は広くすることができます。
- 同期ノードが 500 以下の場合、推奨最低トポロジ同期間隔は 24 時間です。同期ノードが 500 個増えるたびに、さらに 24 時間 (以上) を追加することを考慮してください。

定期トポロジ同期は NNMi スパイラル検出で負荷分散され、NNMi 管理サーバーに負荷がかかり過ぎないようにペース配分されます。検出アクティビティが多い期間は、トポロジ同期は行われません。

HP Blade System Virtual Connect デバイスのサポート

HP Blade System Virtual Connect デバイスを統合して、1 つのプライマリデバイスと、1 つ以上のスタンバイデバイスおよびスレーブデバイスで構成される Virtual Connect ドメインを形成することができます。この統合は、ドメインプライマリサービス、またはスタンドアロンサービスとして機能する Virtual Connect デバイスのみに関する NA インベントリ情報に渡されます。

NA インベントリと同期する Virtual Connect デバイスを制限するには、以下の手順を実行します。

1 以下のいずれかの機能を使用する追加フィルタに基づいて、1 つ以上の NNMi ノードグループを作成します。
   - com.hp.nnm.capability.node.hpvcStandalone
   - com.hp.nnm.capability.node.hpvcPrimary
   - com.hp.nnm.capability.node.hpvcStandby
   - com.hp.nnm.capability.node.hpvcSlave
2 手順 1 で作成したすべてのノードグループに対して、親ノードグループを 1 つ作成します。

   この親ノードグループに、NA インベントリと同期する必要のあるほかのデバイスも入れます。
3 その親ノードグループの名前を使用して、**[HP NNMi-HP NA 統合設定]** フォームの **[トポロジフィルタノードグループ]** パラメータを更新します。詳細については、466 ページの「統合動作」を参照してください。

統合が提供する NNMi 機能

HP NNMi-HP NA 統合では、以下の機能のために、NNMi から NA への通信が提供されます。

- 455 ページの「NNMi コンソールからの NA ビューの起動」
- 456 ページの「NA Diagnostics コマンド スクリプトをインシデント アクションとして設定」
- 457 ページの「NA にアクセスするインシデント アクションの結果の表示」
- 457 ページの「不整合な状態のレイヤー 2 接続の特定」

NNMi コンソールからの NA ビューの起動

HP NNMi-HP NA 統合は、NNMi コンソールから NA へのリンクを提供します。

HP NNMi-HP NA 統合を有効にすると、NNMi コンソールの **[アクション]** メニューに以下の項目が追加されます。

- **[HP NA の結果を表示]** - NNMi インシデントのデバイスにスケジュールされた NA タスクのリストを表示します。タスクを選択してタスクの結果を表示します。詳細については、457 ページの「NA にアクセスするインシデント アクションの結果の表示」を参照してください。
- **[HP NA Diagnostics を再実行]** - NNMi インシデントのデバイスに設定された NA アクションを実行します。詳細については、457 ページの「NA にアクセスするインシデント アクションの結果の表示」を参照してください。
- **[不整合の接続を表示]** - 速度または全二重設定に差があるすべてのレイヤー 2 接続のテーブルを表示します。詳細については、457 ページの「不整合な状態のレイヤー 2 接続の特定」を参照してください。
- **[HP NA デバイス情報を表示]** - NNMi で選択されたデバイスについて、現在の NA の **[デバイスの詳細]** ページを開きます。

- **[HP NA デバイス設定の表示]** - NNMi で選択されたデバイスについて、NA の **[現在の設定]** ページを開きます。

  デバイスのリアルタイム変更の検出が無効になっている場合、最後のデバイス ポーリング周期で NA が取得した設定が表示されます。その取得に続いて設定変更が行われた場合、**[現在の設定]** ページの情報は、実際の現在の設定でない場合があります。

- **[HP NA デバイス設定の差を表示]** - NNMi で選択されたデバイスについて、NA の **[デバイス設定を比較]** ページを開きます。
- **[HP NA デバイス設定の履歴を表示]** - NNMi で選択されたデバイスについて、**[NA デバイス設定の履歴]** ページを開きます。
- **[HP NA ポリシー適合レポートを表示]** - NNMi で選択されたデバイスについて、NA の **[ポリシー、ルール、および適合の検索結果]** ページを開きます。
- **[HP NA デバイスへの Telnet]** - NNMi で選択されたデバイスに接続する **[Telnet]** ウィンドウを開きます。
- **[HP NA デバイスへの SSH]** - NNMi で選択されたデバイスに接続する **[SSH]** ウィンドウを開きます。
- **[HP NA を起動]** - NA ユーザー インタフェースを開きます。
- **[HP NA コマンド スクリプトを起動]** - NA の **[新規タスク - コマンド スクリプトを実行]** ページを開きます。このページは、NNMi コンソールで選択されたノードまたはインシデントについて事前入力されます。
- **[HP NA Diagnostics を起動]** - NA の **[新規タスク - Diagnostics 実行]** ページを開きます。このページは、NNMi コンソールで選択されたノードまたはインシデントについて事前入力されます。

NA 機能の使用方法については、『HP Network Automation ユーザー ガイド』を参照してください。

NA Diagnostics コマンド スクリプトをインシデント アクションとして設定

HP NNMi-HP NA 統合を有効にすると、関連するインシデント タイプが発生するたびに、NA Diagnostics にアクセスするインシデント アクションを含めるように、すぐに使用できる NNMi インシデントのいくつかが変更されます。表 44 には、変更されたインシデントがリストされています。

表 44　NA Diagnostics で設定された NNMi インシデント

NNMi インシデント	NA Diagnostic
OSPFNbrStateChange	隣接ノードを表示
OSPFVirtIfStateChange	隣接ノードを表示
OSPFIfStateChange	隣接ノードを表示 インタフェースを表示
InterfaceDown	インタフェースを表示
CiscoChassisChangeNotification	モジュールを表示

別の NNMi インシデントに NA にアクセスするアクションを追加し、デフォルトのインシデント アクションを変更できます。インシデントの **[アクション]** タブで、`ScriptOrExecutable` の **[コマンド タイプ]** を使用して新しいライフサイクルの以降アクションを追加します。**[コマンド]** ボックスに、適切な引数を使用して、`naruncmdscript.ovpl` または `narundiagnostic.ovpl` を入力します。例については、表 44 にリストされたインシデントのアクション設定を参照してください。

NA にアクセスするインシデント アクションの結果の表示

NA アクションで設定された、あるタイプのインシデントが届くと、NNMi は、設定されたアクションを開始し、診断またはコマンド スクリプトのタスク ID をそのインシデントの属性として保存します。タスク ID の存在によって、**[アクション]** メニューの **[HP NA Diagnostic 結果を表示]** と **[HP NA Diagnostics を再実行]** 項目が利用できるようになります。

インシデントが発生したときのアクションの結果を表示するには、NNMi インシデント ビューでインシデントを選択し、**[アクション] > [HP NA Diagnostic の結果を表示]** を選択します。

設定されたアクションの現在の結果を表示するには、NNMi インシデント ビューでインシデントを選択し、**[アクション] > [HP NA Diagnostics を再実行]** を選択します。

タスクを複数回実行する場合、NNMi は、**[インシデント]** フォームの **[カスタム属性]** タブに最近のタスク ID のリストを表示します。**[HP NA Diagnostic の結果の表示]** アクションは、異なるユーザーの結果を比較できるように、インシデントに実行されたすべてのタスクを表示します。

不整合な状態のレイヤー 2 接続の特定

HP NNMi-HP NA 統合が有効になっている場合、NNMi は、NNMi トポロジの各レイヤー 2 接続のいずれかのエンドにある 2 つのインタフェースの速度と全二重設定を NA に定期的にクエリします。さらに、NNMi は、NNMi トポロジに追加される新しい接続と、NNM iSPI Performance for Metrics が実行している場合は、不整合接続を示すパフォーマンスしきい値の例外を伴う接続の、インタフェースの速度と全二重設定を NA にクエリします。NNMi は、不整合検出アルゴリズムを使用して、その値によって不整合な接続となるかどうかを判断します。

NNMi は、NA インベントリにレイヤー 2 接続を形成するインタフェース用の MAC アドレスが含まれている場合にのみ、不整合分析を実行します。NA インタフェースのレコードに有効な MAC アドレスが含まれていない場合は、NA の**トポロジ データ収集**診断を実行して、MAC アドレス フィールドを更新します。詳細については、452 ページの手順 5 を参照してください。

[アクション] > [不整合の接続を表示] コマンドでは、図 26 で示すように、速度の不整合か全二重の不整合、またはその両方を含むと NNMi が考えるレイヤー 2 接続のテーブルが表示されます。

図 26　　不整合接続テーブルの例

疑わしい接続について、テーブルは、接続のいずれか一端にあるインタフェースの速度と全二重の値、およびデータの解釈をリストします。考えられる解釈は以下のとおりです。

- MATCH は、速度の値と全二重の値によって、正しく機能するレイヤー 2 接続を得られることを示します。
- POSSIBLE_MISMATCH は、速度の値か全二重の値、またはその両方の値が競合しており、接続不良またはパフォーマンスが低い接続となる可能性があることを示します。

- MISMATCH は、速度の値か全二重の値、またはその両方の値が競合しており、接続不良またはパフォーマンスが低い接続となる可能性が高いことを示します。

[HP NNMi-HP NA の統合設定] フォームの **[HP NA 接続チェック間隔]** パラメータは、接続クエリの頻度を指定します。

統合により提供される NA 機能

HP NNMi-HP NA 統合では、以下の機能のために、NA から NNMi への通信が提供されます。

- 458 ページの「デバイス設定変更通知の送信」
- 458 ページの「正確なデバイス情報の維持」
- 459 ページの「デバイス設定中のネットワーク管理の無効化」
- 460 ページの「デバイス コミュニティ文字列の変更の伝播」
- 460 ページの「NA イベント ルール」

デバイス設定変更通知の送信

デバイスが NA インベントリに追加されたり、NA インベントリのデバイスで設定が変更されたりしたとき、NA は SNMP トラップを NNMi に送信します。NNMi オペレータはこのトラップをインシデント ビューで確認でき、必要に応じてその変更を調査できます。

統合により、NASnmpTrapv1 と NASnmpTrapv2 の SNMP トラップ インシデント設定が NNMi に追加されます。

正確なデバイス情報の維持

特定のデバイス設定タスクの場合、タスクが完了すると、NA からのトリガにより NNMi がデバイスを再検出します。

NA の **[管理設定 - 第三者統合]** ページの **[タスク後にホストを再検出]** フィールドでは、NNMi がデバイスを再検出するトリガとなるデバイス設定タスクを指定します。デフォルトの選択は以下のとおりです。

- デバイス ソフトウェアの更新
- パスワードの配布
- デバイスの再起動
- ドライバの検出

以下のタスクのいずれかまたはすべてをさらに選択できます。

- コマンド スクリプトの実行
- 診断の実行
- ACL の削除
- Syslog の設定
- ICMP テストの実行
- スナップショットの作成
- スタートアップと実行の同期

- OS 分析

この機能を無効にするには、タスク リストからすべての選択をクリアします。

デバイス設定中のネットワーク管理の無効化

特定のデバイス設定タスクで、NA からのトリガにより NNMi が設定プロセス中にデバイスを無効ステータスに設定します。この管理状態では、NNMi によるデバイスの監視が抑制され、不要なインシデントが防止されます。デバイスを設定する前に、NA は、サービス停止中イベントを NNMi に送信します。デバイスの設定が完了したら、NA は、サービス状態イベントを NNMi に送信し、デバイスから 無効ステータスを削除して、通常状態のポーリングを再開します。

NA の **[管理設定 - 第三者統合]** ページの **[サービス停止イベント]** フィールドで、タスク実施中の NNMi がデバイスを無効ステータスに設定するトリガとなるデバイス設定タスクを指定します。デフォルトの選択は以下のとおりです。

- デバイス ソフトウェアの更新
- パスワードの配布
- デバイスの再起動

以下のタスクのいずれかまたはすべてをさらに選択できます。

- コマンド スクリプトの実行
- 診断の実行
- ACL の削除
- Syslog の設定
- ドライバの検出
- ICMP テストの実行
- スナップショットの作成
- スタートアップと実行の同期
- OS 分析

この機能を無効にするには、タスク リストからすべての選択をクリアします。

デバイス設定が正しく行われない場合、動作は統合設定に依存します。

- NA の **[管理設定 - 第三者統合]** ページにある **[デバイス タスクが失敗した場合]** 設定では、デバイス設定が正しく行われなかった場合に NNMi の 無効ステータスを削除するか維持するかを指定します。
- NA の **[管理設定 - 第三者統合]** ページにある **[タスク完了後にデバイス適合チェックに失敗した場合]** 設定では、デバイス設定が適合していない場合に、NNMi の 無効ステータスを削除するか維持するかを指定します。

これらの設定は、**[サービス停止イベント]** フィールドで選択されたすべてのデバイス タスクに適用されます。タスク別に復旧の動作を設定することはできません。

デバイス コミュニティ文字列の変更の伝播

SNMP コミュニティ文字列の伝播が有効である場合、統合は以下のように動作します。

- 同期したデバイスにアクセスするために NA が使用する SNMPv1 または SNMPv2c コミュニティ文字列を変更した場合、NA は、その変更を NNMi に通知し、NNMi は、そのデバイスとの通信設定を更新します。

  NNMi は、デバイスの新しいコミュニティ文字列をすぐに使用します。

  NA は、デバイスを管理するためのコミュニティ文字列が変更された場合にのみ、NNMi に更新内容を送信します。NA がデバイスに新しいコミュニティ文字列を配布するとき、NNMi は更新を受信しません。

- 新しいデバイスが NA Default Site パーティションに追加された場合、NA は、デバイスの管理に使用する SNMPv1 および SNMP v2c のコミュニティ文字列を NNMi に通知します。

統合により、SNMPv3 ユーザーが NA から NNMi に伝播されることはありません。

NA の **[管理設定 - 第三者統合]** ページにある **[SNMP コミュニティ文字列を伝播]** 設定では、NA の SNMP コミュニティ文字列を NNMi に転送するかどうかを指定します。デフォルトでは、コミュニティ文字列の伝播は行われません。

NA イベント ルール

NA イベント ルールでは、NA が NNMi 管理サーバーとやり取りする方法を定義します。

NA のこのイベント ルールを変更したり削除したりしないでください。

統合により、NA では以下のイベント ルールが定義されます。

- SNMP トラップによる NA/NNMi 統合

  新しいデバイスが NA インベントリに追加されるか、デバイス設定が変更されると、この NA イベントによって SNMP トラップが NNMi に送信されます。詳細については、458 ページの「デバイス設定変更通知の送信」を参照してください。

- デバイス追加の NA/NNMi トポロジ同期

  NA インベントリの Default Site パーティションに新しいデバイスが追加されると、この NA イベントにより、デバイス ヒントが NNMi に送信されます。詳細については、453 ページの「NNMi と NA の間のトポロジ同期」を参照してください。

- デバイス削除の NA/NNMi トポロジ同期

  NA インベントリからデバイスが削除されると、この NA イベントにより、NNMi トポロジからこのデバイスを削除する要求が送信されます。詳細については、453 ページの「NNMi と NA の間のトポロジ同期」を参照してください。

- NA/NNMi 統合再検出ホスト

  NA インベントリのデバイスの設定が変更されると、この NA イベントにより、このデバイスの最新の NNMi ステータスが要求されます。詳細については、458 ページの「正確なデバイス情報の維持」を参照してください。

- NA/NNMi 統合サービス停止中

  タスクが開始されると、この NA イベントにより、このデバイスは NNMi で「サービス停止中」状態に設定されます。タスクの完了後、このイベントにより、このデバイスは NNMi で「サービス」状態に戻されます。詳細については、459 ページの「デバイス設定中のネットワーク管理の無効化」を参照してください。

- NA/NNMi 統合 SNMP コミュニティ文字列伝播

  NA インベントリのデバイスで [最後に使用したデバイス パスワードの変更] が変更されると、この NA イベントにより、NA がデバイスの管理に使用しているコミュニティ文字列が NNMi に送信されます。詳細については、460 ページの「デバイス コミュニティ文字列の変更の伝播」を参照してください。

HP NNMi-HP NA 統合の変更

1. NA ユーザー インタフェースで、**[管理設定 - 第三者統合]** ページを開きます (**[管理者] > [管理設定] > [第三者統合]**)。
   a. 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は、以下のリファレンスを参照してください。
      — 458 ページの「正確なデバイス情報の維持」
      — 459 ページの「デバイス設定中のネットワーク管理の無効化」
      — 460 ページの「デバイス コミュニティ文字列の変更の伝播」
   b. ページの下にある **[保存]** をクリックします。
2. NNMi コンソールで、**[HP NNMi-HP NA 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 NA]**)。
   a. 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は、464 ページの「HP NNMi-HP NA 統合設定フォームのリファレンス」を参照してください。
   b. 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。ovjboss を再起動する必要はありません。

HP NNMi-HP NA 統合の無効化

1. NNMi コンソールで、**[HP NNMi-HP NA 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 NA]**)。
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。これで、統合アクションを使用できなくなります。

➤ 変更はただちに有効になります。ovjboss を再起動する必要はありません。

HP NNMi-HP NA 統合のトラブルシューティング

この項では以下の内容について説明します。

- 462 ページの「統合をテストする」
- 464 ページの「NA デバイスが NNMi トポロジから欠落している」

統合をテストする

過去に統合が正常に動作していた場合は、構成の何か (NNMi または NA のユーザー パスワードなど) が最近変更された可能性があります。この手順全体を段階的に実行する前に、464 ページの「HP NNMi-HP NA 統合設定フォームのリファレンス」に説明されているように統合設定を更新してください。

1. NNMi コンソールで、**[HP NNMi-HP NA 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 NA]**)。

   このフォームのフィールドの詳細は、464 ページの「HP NNMi-HP NA 統合設定フォームのリファレンス」を参照してください。

2. 統合のステータスを確認するには、**[HP NNMi-HP NA の統合設定]** フォームで、フォームの下にある **[送信]** をクリックします (設定の変更は行いません)。

   正常に動作すると、この手順によって NNMi と NA の間で完全なトポロジ同期が開始されます。

   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。

   メッセージに NA サーバーへの接続の問題が示されている場合、NNMi と NA は通信できていません。この手順の 手順 3 を継続します。

3. NA 資格情報の正確性とアクセス レベルを確認するには、**[HP NNMi-HP NA の統合設定]** フォームの **[NA ユーザー]** の資格情報を使用して、NA ユーザー インタフェースにログオンします。

   NA ユーザー インタフェースにログオンできない場合、NA 管理者にログオン資格情報を問い合わせてください。

4. NA サーバーへの接続が正しく設定されていることを確認するには、NNMi 管理サーバーの Web ブラウザで、以下の URL を入力します。

   http://<*naserver*>:<*naport*>/soap

   以下のように、変数が **[HP NNMi-HP NA の統合設定]** フォームの値に関係する場合 :

   - **[NA SSL が有効になっています]** チェック ボックスは、NA サーバーへの接続が `http` プロトコルを使用するように、オフになっている必要があります。
   - *`<naserver>`* は **[NA ホスト]** の値です。
   - *`<naport>`* は **[NA ポート]** の値です。

NA Web サーバーが指定されたサーバーとポートで実行している場合、NA サーバーは以下のようなメッセージで応答します。

```
NAS SOAP API: Only handles HTTP POST requests
```

- 期待されるメッセージが表示されたら、手順 5 に進みます。
- エラー メッセージが表示されたら、NA サーバーへの接続は正しく設定されていません。NA 管理者に問い合わせ、NA Web サービスに接続するために使用している情報を確認します。期待されるメッセージが表示されるまで、NA への接続のトラブルシューティングを続けます。

5 NNMi への接続が正常に設定されていることを確認します。

この手順の 手順 1 で NNMi コンソール に接続するために、このステップで説明してある情報を使用した場合は、NNMi コンソール に再接続する必要はありません。手順 6 を継続します。

a NA サーバーの Web ブラウザで、以下の URL を入力します。

http://*<NNMiserver>*:*<port>*/nnm/

以下のように、変数が **[HP NNMi-HP NA の統合設定]** フォームの値に関係する場合 :

— `<NNMiserver>` は **[NNMi ホスト]** の値です。

— `<port>` は、**[NNMi ポート]** の値です。

b プロンプトが表示されたら、管理者ロールで NNMi ユーザーの資格認定を入力します。

NNMi コンソール が表示されるはずです。NNMi コンソールが表示されない場合は NNMi 管理者に連絡して、NNMi に接続するために使用している情報を確認してください。NNMi コンソール が表示されるまで、NNMi への接続のトラブルシューティングを継続します。

「Web サービス クライアント」ロールを持つユーザーとして NNMi コンソールにログオンすることはできません。

6 NNMi 管理者に連絡し、Web サービス クライアント ロールでの **[NNMi ユーザー]** の値、および対応する **[NNMi パスワード]** を確認します。

7 この手順の手順 4 と手順 5 で使用して正常に接続できた値で、**[HP NNMi-HP NA の統合設定]** フォームを更新します。また、手順 6 で使用した NNMi ユーザーとパスワードをこのフォームに再入力します。

詳細については、464 ページの「HP NNMi-HP NA 統合設定フォームのリファレンス」を参照してください。

8 フォームの下部にある **[送信]** をクリックします。

9 上記を実行してもステータス メッセージに NA サーバーへの接続の問題が示される場合は、以下の手順を実行します。

a Web ブラウザのキャッシュをクリアします。

b Web ブラウザから、すべての保存フォームまたはパスワード データをクリアします。

c Web ブラウザ ウィンドウを完全に閉じてから、もう一度開きます。

d この手順の手順 7 と手順 8 を繰り返します。

10 453 ページの「HP NNMi-HP NA 統合の使用法」にリストされたアクションの 1 つを起動して、設定をテストします。

NA デバイスが NNMi トポロジから欠落している

NA Default Site パーティションのデバイスが NNMi 同期ノードグループに表示されない場合、以下の手順を実行します。

1. NNMi ノードインベントリを調べて、そのデバイスがトポロジにはあるが、別のノードグループに入っていないかどうかを確認します。

   別のグループに入っている場合、NNMi 同期ノードグループの定義を更新して、そのデバイスが含まれるようにします。

2. NNMi IP アドレスのインベントリを調べて、NA で使用されている IP アドレスが NNMi にリストされているかどうかを確認します。

   IP アドレスが NNMi に含まれている場合、どのノードがその IP アドレスをホストしているかを確認します。このノードは、NA デバイスと同期されている必要があります。NNMi で、NA が検出ヒントとして送信した IP アドレスとは異なる管理アドレスがそのノードに使用されている可能性があります。

3. 必要に応じて、統合を再度有効化します。

   NA は、統合が有効になっている場合に、新しいデバイスが NA Default Site パーティションに追加されたときのみ、検出ヒントを送信します。ネットワークの停止中、または NNMi 同期ノードグループと自動検出ルールが正しく組み込まれる前にデバイスが NA に追加された場合、統合を再度有効化すると、NA は検出ヒントを再送信します。

アプリケーション フェイルオーバーと HP NNMi-HP NA 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 NA 統合では、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 NA サーバーが再設定されます。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、NA サーバーのフェイルオーバーがサポートされません。

HP NNMi-HP NA 統合設定フォームのリファレンス

NNMi コンソールの **[HP NNMi-HP NA の統合設定]** フォームには、NNMi から NA の通信を設定するためのパラメータが含まれています。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 ロールのある NNMi ユーザーのみが **[HP NNMi-HP NA の統合設定]** フォームにアクセスできます。

[HP NNMi-HP NA の統合設定] フォームは、以下の一般領域に関する情報を収集します。

- NNMi 管理サーバー接続
- NA サーバー接続
- 統合動作

統合設定に変更を適用するには、**[HP NNMi-HP NA 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 45 に、NA から NNMi 管理サーバーに接続するためのパラメータをリストします。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 45　NNMi コンソールの NNMi 管理サーバー情報

フィールド	説明
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。 注 : 統合により、以下のファイルの `jboss.http.port` の値が判断されて、NNMi コンソールに接続するためのポートが選択されます。 • *Windows*: `%NnmDataDir%¥conf¥nnm¥props¥nms-local.properties` • *UNIX*: `$NnmDataDir/conf/nnm/props/nms-local.properties`
NNMi ユーザー	NNMi コンソール に接続するためのユーザー名。このユーザーには NNMi Web Service Client ロールが必要です。 注 : このユーザー名のパスワードはクリアテキストで渡されます。 ベスト プラクティス : 「Web サービス クライアント」ロールを持つ `NNMiIntegration` ユーザー アカウントを作成して使用します。
NNMi パスワード	指定の NNMi ユーザーのパスワード。

NA サーバー接続

表 46 には、NA サーバー上の Web サービスに接続するためのパラメータがリストされています。NA 管理者と協力し、設定フォームのこのセクションに使用する適切な値を決定します。

表 46　NNMi コンソールの NA サーバー情報

HP NA サーバー パラメータ	説明
NA ホスト	NA サーバーの完全修飾ドメイン名または IP アドレス。

表 46　NNMi コンソールの NA サーバー情報（続く）

HP NA サーバー パラメータ	説明
NA ポート	NA Web サービスに接続するためのポート。 デフォルトの NA ポートは以下のとおりです。 • 80 - NNMi から別のコンピュータにある NA に接続する場合 • 8080 - NNMi と同じコンピュータにある NA に接続する場合 **ヒント :** NA URL には SSL ポートが表示されますが、統合の通信では動作しません。正しい SSL 以外のポートを入力してください。
NA ユーザー	NA 管理者ロールを持つ有効な NA ユーザー アカウント名。 **注 :** このユーザー名のパスワードはクリアテキストで渡されます。 ベスト プラクティス : `NAIntegration` ユーザー アカウントを作成して使用します。
NA パスワード	指定した NA ユーザーのパスワード。

統合動作

表 47 には、HP NNMi-HP NA 統合の動作を設定するための NNMi コンソールパラメータをリストします。

表 47　NNMi コンソールの統合動作情報

パラメータ	説明
トポロジ フィルタ ノード グループ	NA トポロジと同期するノードのセットを含む NNMi ノード グループ。統合により、このノード グループのすべてのノードに関する情報が NA Default Site パーティションに入力されます。 この NNMi 管理サーバーのノード グループのリストからノード グループを選択します。 ノード グループが指定されていない場合は、統合により、NNMi トポロジ全体が NA Default Site パーティションと同期されます。
トポロジ同期間隔 (時間)	453 ページの「NNMi と NA の間のトポロジ同期」の説明のように、NNMi が NA との完全トポロジ同期を実行する頻度。接続チェックのデフォルトの周期は 24 時間です。 定期トポロジ同期を無効にするには、この値を 0 に設定します。
NA のデバイス ドライバの検出	NA 設定の指定。 **[NA のデバイス ドライバの検出]** チェック ボックスがオンである場合、NA は NNMi とのトポロジ同期の結果として、NA に追加されたデバイスのデバイス ドライバを自動的に検出します。 デフォルト設定はオフです。この場合は、デバイス ドライバ検出を手動で開始できます。
NA 接続チェック間隔 (時間)	457 ページの「不整合な状態のレイヤー 2 接続の特定」の説明のように、NNMi が NNMi トポロジのすべてのレイヤー 2 接続のインタフェース データを NA で確認する頻度。接続チェックのデフォルトの周期は 24 時間です。 定期接続チェックを無効にするには、この値を 0 に設定します。

NA の NNMi 統合設定リファレンス

NA ユーザー インタフェースの **[管理設定 - 第三者統合]** ページの **[NNMi 統合]** セクションには、NA から NNMi への通信を設定するためのパラメータが含まれています。**[HP NNMi-HP NA の統合設定]** フォームで統合を有効にすると、**[管理設定 - 第三者統合]** ページのフィールドが設定されます。NNMi デバイス再検出トリガ、サービス停止中トリガ、SNMP コミュニティ文字列伝播の統合動作を変更するには、**[管理設定 - 第三者統合]** ページにアクセスします。

[管理設定 - 第三者統合] ページは、**[管理者] > [管理設定] > [第三者統合]** で表示できます。統合設定への変更を適用するには、このページの値を更新し、**[送信]** をクリックします。

Administrator ロールのある NA ユーザーのみが **[管理設定 - 第三者統合]** ページにアクセスできます。

統合通信

表 48 には、NA サーバーから NNMi Web サービスに接続するためのパラメータがリストされています。統合により、NNMi コンソールの **[HP NNMi-HP NA の統合設定]** フォームの情報でこのパラメータが設定されます。

表 48　NA ユーザー インタフェースの統合接続情報

フィールド	説明
NA ユーザー	**[HP NNMi-HP NA の統合設定]** フォームに指定されている NA ユーザー アカウント名。
NA パーティション	**[HP NNMi-HP NA の統合設定]** フォームに指定されている NA パーティション。
NNMi ホスト	**[HP NNMi-HP NA の統合設定]** フォームに指定されている NNMi 管理サーバー名。
NNMi HTTP ポート	統合によって決定した NNMi コンソール ポート。
NNMi User(NNMi ユーザー)	**[HP NNMi-HP NA の統合設定]** フォームに指定されている NNMi ユーザー名。
NNMi Password(NNMi パスワード)	**[HP NNMi-HP NA の統合設定]** フォームに指定されている NNMi ユーザー パスワード。

その他の統合動作

表 49 には、HP NNMi-HP NA 統合の動作を設定するための NA ユーザー インタフェース パラメータをリストします。

表 49　NA ユーザー インタフェースの統合動作情報

フィールド	説明
タスク後にホストを再検出	統合により、タスクの完了時に NNMi のデバイス検出が開始されるようにする NA タスク。デフォルトの選択は以下のとおりです。 • デバイス ソフトウェアの更新 • パスワードの配布 • デバイスの再起動 • ドライバの検出 詳細については、458 ページの「正確なデバイス情報の維持」を参照してください。
サービス停止中イベント	統合により、タスク発生中にデバイスが [無効] 状態に設定されるようにする NA タスク。デフォルトの選択は以下のとおりです。 • デバイス ソフトウェアの更新 • パスワードの配布 • デバイスの再起動 詳細については、459 ページの「デバイス設定中のネットワーク管理の無効化」を参照してください。
デバイス タスクが失敗した場合	サービス停止中イベントのデバイス タスク失敗復旧指定。デフォルト設定では、デバイスが NNMi のサービスに戻ります。 詳細については、459 ページの「デバイス設定中のネットワーク管理の無効化」を参照してください。
タスク完了後にデバイス適合チェックに失敗した場合	サービス停止中イベントのデバイス適合チェック失敗復旧指定。デフォルト設定では、デバイスが NNMi のサービスに戻ります。 詳細については、459 ページの「デバイス設定中のネットワーク管理の無効化」を参照してください。
SNMP コミュニティ文字列を伝播	コミュニティ文字列伝播指定。デフォルト設定は無効です。 詳細については、460 ページの「デバイス コミュニティ文字列の変更の伝播」を参照してください。

HP ProCurve Manager Plus

HP ProCurve Manager Plus (PCM Plus) は、HP ProCurve デバイスのマッピング、設定、および監視を実行するためのネットワーク管理プラットフォームです。PCM Plus は、以下の機能を備えています。

- ネットワーク全域でのケーブル接続 Ethernet とワイヤレス Ethernet の統合管理
- HP ProCurve デバイスの設定、更新、監視、およびトラブルシューティング
- ポリシーベースの複数デバイス管理
- 自動アラート応答によるプロアクティブ アラート
- 詳細なトラフィック監視機能

PCM Plus の購入に関する詳細については、HP 販売員にお尋ねください。

この章には、以下のトピックがあります。

- HP NNMi-HP ProCurve Manager Plus 統合
- HP NNMi-HP ProCurve Manager Plus 統合の使用法

HP NNMi-HP ProCurve Manager Plus 統合

PCM Plus 環境に HP Network Node Manager i Software (NNMi) を含めることにより、PCM Plus を使用して ProCurve デバイスを監視および管理するネットワーク管理者は、対象のデバイスについてさらに深い洞察を得ることができます。

HP NNMi-HP ProCurve Manager Plus 統合では、以下の機能を提供します。

- NNMi データベースの IPv4 ProCurve デバイス情報と PCM Plus の同期 (現時点において、PCM Plus は IPv6 ProCurve デバイスをサポートしていません)。
- SNMPv2 コミュニティ文字列および通信用の SNMPv3 ユーザーベース セキュリティ モデル (USM) 設定と、2 つのアプリケーションの間にある管理対象 ProCurve デバイスの同期。

値

HP NNMi-HP ProCurve Manager Plus 統合には、以下の利点があります。

- NNMi が NNMi と PCM Plus 両方の ProCurve デバイスを検出するため、ProCurve デバイスへのネットワーク トラフィックが減ります。
  - NNMi は、豊富な ProCurve デバイス情報を PCM Plus に転送します。
  - 簡素化された PCM Plus ネットワーク マップには、既知の ProCurve デバイスのみが含まれています。
- ProCurve デバイス イベント 処理を NNMi に統合します。
- ProCurve デバイスの可用性を最大限に高めるためにかかるコストを削減します。

統合製品

この章の情報は、以下の製品に当てはまります。

- PCM Plus

サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10

NNMi と PCM Plus は、別々のコンピュータにインストールする必要があります。NNMi 管理サーバーと PCM Plus コンピュータのオペレーティング システムは、同じでも異なっていても構いません。

PCM Plus リモート エージェントを NNMi 管理サーバーにインストールすることはできません。

PCM Plus バージョン 3.10 の 1 つのインストール済み環境を NNMi バージョン 8.1x (またはそれ以降)、あるいは NNM バージョン 7.x と統合することはできますが、同時に両方の製品と統合することはできません。

ドキュメント

HP NNMi-HP ProCurve Manager Plus 統合については、『HP ProCurve Manager ネットワーク管理者ガイド』の付録 A (**www.procurve.com/pcm-manuals**) で詳しく説明されています。

HP NNMi-HP ProCurve Manager Plus 統合の使用法

HP NNMi-HP ProCurve Manager Plus 統合を有効にする手順は、PCM Plus サーバー (設定) と NNMi 管理サーバー (PCM Plus トラップ定義のインストール) で実行されます。

HP NNMi-HP ProCurve Manager Plus 統合を有効にすると、PCM Plus が NNMi に転送するすべてのアプリケーション イベントについて、ICMEVT_PCMPLUS_EVENTS_ALL インシデント設定が NNMi に追加されます。このインシデントの SNMP オブジェクト ID は、.1.3.6.1.4.1.11.2.3.7.11.0.63000000 です。

HP NNMi-HP ProCurve Manager Plus 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の詳細については、『HP ProCurve Manager ネットワーク管理者ガイド』の付録 A を参照してください。

HP RAMS MPLS WAN

HP RAMS MPLS WAN 統合により、HP ルート分析管理システム (RAMS) は、WAN 接続の複数のサイトを持つ企業を、独自のネットワーク内でマルチプロトコル ラベル スイッチング (MLPS) を使用する ISP 経由でサポートできるようになりました。

HP RAMS のご購入については、HP 営業担当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 RAMS MPLS WAN 統合
- HP NNMi-HP RAMS MPLS WAN 統合の使用法

HP NNMi-HP RAMS MPLS WAN 統合

HP NNMi-HP RAMS MPLS WAN 統合では、NNMi コンソールから MPLS WAN 情報にアクセスする機能を提供します。

値

HP NNMi-HP RAMS MPLS WAN 統合により、さまざまなネットワーク クラウドを介した接続を表示する機能が追加されるため、NNMi ユーザーは WAN 接続の複数のサイトを検出して表示することができます。

統合製品

この章の情報は、以下の製品に当てはまります。

- RAM

  サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10 (NNMi Advanced ライセンス付き)

NNMi でサポートするハードウェア プラットフォームとオペレーティング システムについては、『NNMi システムおよびデバイスのサポート マトリックス』を参照してください。

ドキュメント

HP NNMi-HP RAMS MPLS WAN 統合については、MMNi ヘルプの「*経路分析管理システム (RAMS) と NNMi Advanced の使用*」で詳しく説明しています。

HP NNMi-HP RAMS MPLS WAN 統合の使用法

HP NNMi-HP RAMS MPLS WAN 統合を有効化するステップは、NNMi 管理サーバー上で行います。

HP NNMi-HP RAMS MPLS WAN 統合の有効化、使用法、無効化、トラブルシューティングについては、MMNi ヘルプの「*経路分析管理システム (RAMS) と NNMi Advanced の使用*」を参照してください。

HP SiteScope

HP SiteScope は、サーバー、オペレーティングシステム、ネットワークデバイス、ネットワークサービス、アプリケーション、およびアプリケーションコンポーネントなど、分散 IT インフラストラクチャの可用性およびパフォーマンスを追跡するエージェントレスの監視ソリューションです。SiteScope は、インフラストラクチャの運用状況を確認し、問題について通知し続け、深刻化する前にボトルネックを解決するためのリアルタイム情報を提供します。

SiteScope のご購入については、HP 営業担当にお尋ねください。

この章では、以下の統合について説明します。

- 475 ページの「HP NNMi-HP SiteScope イベント統合」
- 479 ページの「HP NNMi-HP SiteScope システム メトリックス統合」

NNM iSPI for IP Telephony-HP SiteScope 統合の詳細については、NNM iSPI for IP Telephony ヘルプの「*SiteScope との統合の設定*」を参照してください。

HP NNMi-HP SiteScope イベント統合

この項では以下の内容について説明します。

- 476 ページの「HP NNMi-HP SiteScope イベント統合について」
- 477 ページの「HP NNMi-HP SiteScope イベント統合の有効化」
- 477 ページの「HP NNMi-HP SiteScope イベント統合の使用法」
- 478 ページの「HP NNMi-HP SiteScope イベント統合の変更」
- 478 ページの「HP NNMi-HP SiteScope イベント統合の無効化」
- 478 ページの「HP NNMi-HP SiteScope イベント統合のトラブルシューティング」

HP NNMi-HP SiteScope イベント統合について

HP NNMi-HP SiteScope イベント統合により、SiteScope サーバーは、設定された SiteScope モニタアラート条件が満たされると、SNMP トラップを NNMi 管理サーバーに送信します。NNMi は、そのモニタアラートトラップを NNMi インシデントに変換します。これらのインシデントから、NNMi コンソールユーザーはそのモニタのコンテキストで SiteScope を起動できます。

値

NNMi で SiteScope インシデント設定を行うことにより、HP NNMi-HP SiteScope イベント統合では、SiteScope で監視するデバイスおよびアプリケーションのステータスに関する SNMP トラップの解釈プロセスが簡素化されます。

これらのトラップは、SiteScope で設定されたアラートに対してのみ生成されます。統合により、これらのトラップがインシデントとして NNMi コンソールに表示されます。SiteScope によってアラート条件がなくなった (正常になった) ことが示されると、NNMi はこれらのアラートインシデントを自動的に閉じます。

統合製品

このセクションの情報は、以下の製品に当てはまります。

- SiteScope

  サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10

NNMi および SiteScope は、同一のコンピュータまたは異なるコンピュータにインストールできます。

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。

サポートされる SiteScope モニタ

HP NNMi-HP SiteScope イベント統合では、SiteScope に設定されたとおりに、すべての SiteScope モニタタイプに関して SiteScope サーバーから送信された SNMP トラップを受信します。SiteScope アラート設定には、NNMi 管理サーバーをトラップターゲットとして組み込む必要があります。

SiteScope トラップ設定によって、トラップソースとして SiteScope サーバーと管理対象ホストのどちらが設定されるかが決まります。トラップソースが NNMi で管理されていない場合、**[インシデント設定]** フォームの **[未解決の SNMP トラップを破棄する]** チェックボックスの設定によって、NNMi でのトラップの処理方法が決まります。詳細については、NNMi ヘルプの「*未解決受信トラップの処理*」を参照してください。

ドキュメント

このセクションでは、この統合の設定方法と使用方法について説明します。

SiteScope モニタの設定方法、およびイベントデータが NNMi に送信されるように SiteScope を設定する方法については、SiteScope 製品メディアに収録されている『HP SiteScope SiteScope の使用法 ガイド』で説明されています。

HP NNMi-HP SiteScope イベント統合の有効化

HP NNMi-HP SiteScope イベント統合を有効にするには、SNMP トラップが NNMi に送信されるように、1 つ以上の SiteScope モニタを設定します。大まかな手順は、以下のとおりです。

NNMi インシデントタイプは、デフォルトで有効になっています。

1 SiteScope ユーザーインタフェースで、HP SiteScope イベントトラップが NNMi 管理サーバーに送信されるように SNMP 設定を作成します。

2 SiteScope ユーザーインタフェースで、SNMP トラップ設定をアラートアクションターゲットとして設定するアラートを作成します (このアラートで、可能性のあるモニタステータスごとにアラートアクションを作成します)。

詳細は、『HP SiteScope SiteScope の使用法 ガイド』の章「*Network Node Manager i (NNMi) の処理*」にある「イベントデータが NNMi に送信されるように SiteScope を設定する方法」を参照してください。

HP NNMi-HP SiteScope イベント統合の使用法

NNMi では、SiteScope モニタ アラート トラップとして 2 つのインシデント タイプを定義しています。

- SiteScopeAlertEvent1 は SNMPv1 形式のトラップを NNMi インシデントに変換します。
- SiteScopeAlertEvent2 は SNMPv2c 形式のトラップを NNMi インシデントに変換します。

これらのインシデント タイプの設定はまったく同じです。SiteScope SNMP トラップ設定によって、SiteScope が SNMPv1- と SNMPv2c- のどちらの形式のトラップを NNMi に送信するかが決定されます。

インシデント設定内で、インシデントの重大度は以下のように設定されます。

- デフォルトのインシデント ステータスは危険域で、SiteScope イベントの重大度であるエラー、NOTAVAILABLE、または NODATA にマップされます。
- インシデント強化では、SiteScope イベント重大度が注意域の場合に、インシデントステータスを注意域に設定します。
- インシデント強化では、SiteScope イベント重大度が正常の場合に、インシデント ステータスを正常域に設定します。

各 SiteScopeAlertEvent トラップには、そのモニタのコンテキストで SiteScope を起動するための URL が含まれています。この URL は、**[インシデント]** フォームの **[カスタム属性]** タブの .1.3.6.1.4.1.11.15.1.2.1.4 カスタム インシデント属性 (CIA) に含まれています。この URL は、統合ビューア ユーザーとして SiteScope にログオンするための暗号化された資格証明を渡します

SiteScopeAlertEvent インシデントごとに、NNMi は、トラップのペイロードに含まれているデータを比較することで、SiteScopeAlertEvent トラップで Pairwise 処理を実行します。各トラップにはイベント キー varbind (OID .1.3.6.1.4.1.11.15.1.3.1.7) が含まれています。トラップにイベント クローズ キー パターン varbind (OID .1.3.6.1.4.1.11.15.1.3.1.8) も含まれている場合、NNMi は、イベント クローズ キー パターン varbind の値を、既存のインシデントのイベント キー varbind と比較します。NNMi は、一致する既存のインシデントを閉じ、着信トラップに従ってそれらを相関付けます。NNMi は、解決済みの各インシデントに、cia.reasonClosed CIA と相関ノートを追加します。さらに、NNMi は、[正常域] ステータスの各 SiteScopeAlertEvent インシデントを自動的に閉じます。

SiteScope SNMP トラップは、システムおよびアプリケーション ファミリーで表示されます。

SiteScopeAlertEvent トラップの内容の詳細については、NNMi とともに配布される HP-SITESCOPE-MIB を参照してください。

HP NNMi-HP SiteScope イベント統合の変更

HP NNMi-HP SiteScope イベント統合を変更するには、以下のいずれかを実行します。

- NNMi コンソールで、SiteScopeAlertEvent1 および SiteScopeAlertEvent2 SNMP トラップのインシデント設定を編集します。
- SiteScope ユーザー インタフェースで、モニタ アラート設定を変更します。

HP NNMi-HP SiteScope イベント統合の無効化

HP NNMi-HP SiteScope イベント統合を無効にするには、以下のいずれか、または両方を実行します。

- NNMi コンソールで、SiteScopeAlertEvent1 および SiteScopeAlertEvent2 の **[SNMP トラップの設定]** フォームの **[有効にする]** チェックボックスをオフにします。
- SiteScope ユーザーインタフェースで、以下のいずれかを実行します。
  - モニタおよびグループをアラートアクションターゲットから削除する。
  - SiteScope モニタに関連付けられた SNMP トラップアラートを無効にするか、削除する。

HP NNMi-HP SiteScope イベント統合のトラブルシューティング

この項では以下の内容について説明します。

- 478 ページの「NNMi インシデントビューに SiteScopeAlertEvent インシデントが表示されない」
- 479 ページの「SiteScope が SiteScop インシデントの URL から正常に開かない」

NNMiインシデントビューにSiteScopeAlertEventインシデントが表示されない

NNMi インシデントビューに予期されるすべての SiteScopeAlertEvent 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 コンソールで、SiteScopeAlertEvent1 と SiteScopeAlertEvent2 のインシデント設定を調べます。
   - SiteScopeAlertEvent1 と SiteScopeAlertEvent2 のインシデントタイプが有効になっていることを確認します。
   - インタフェースまたはノードが設定されている場合は、予期される SiteScope トラップがそれらの設定によってブロックされていないことを確認します。
2. NNMi コンソールで、インシデント ビューのフィルタを調べます。

   現在のフィルタを SiteScopeAlertEvent1 と SiteScopeAlertEvent2 のインシデント設定と比較します。フィルタがそれらのインシデント タイプをブロックしていないことを確認します。
3. **[インシデント設定]** フォームの **[未解決の SNMP トラップを廃棄する]** チェック ボックスがオンになっている場合は、SiteScope モニタに関連付けられたノードが NNMi トポロジ内にあることを確認します。

   SiteScope トラップ設定によって、トラップソースとして SiteScope サーバーと管理対象ホストのどちらが設定されるかが決まります。
4. SiteScopeユーザーインタフェースで、HP SiteScopeイベントトラップに関するSNMPトラップ設定の内容を確認します。

5 SiteScope ユーザーインタフェースで、予期される各モニタアラートで SNMP トラップ設定がアラートアクションターゲットとして設定されていることを確認します。

6 SiteScope ユーザーインタフェースで、テストトラップを NNMi に送信します。

SiteScope が SiteScop インシデントの URL から正常に開かない

SiteScope が、**[インシデント]** フォームの **[カスタム属性]** タブに表示される .1.3.6.1.4.1.11.15.1.2.1.4 CIA の URL から正常に起動しない場合は、以下の手順を実行します。

1 SiteScope ユーザー インタフェースへのアクセスを確認します。

   a 新しいブラウザ ウィンドウで、SiteScope ユーザー インタフェースを直接開きます。

   SiteScope ユーザー インタフェースが正常に動作しない場合は、ブラウザの設定が『HP SiteScope リリース ノート』に記載されている要件を満たすことを確認します。

   b .1.3.6.1.4.1.11.15.1.2.1.4 CIA からブラウザのアドレス フィールドに URL をコピーします。ログオン資格証明を削除します。SiteScope のログオン ウィンドウで、SiteScope ログオン情報を入力します。

2 URL に含まれる SiteScope 統合ビューアのユーザー資格証明を確認します。.1.3.6.1.4.1.11.15.1.2.1.4 CIA からブラウザのアドレス フィールドに URL をコピーします。(ログオン資格証明を保持します)。

   このテストに失敗する場合は、SiteScope 管理者に統合ビューア ユーザーのステータスについて問い合わせてください。統合ビューアユーザーのパスワードを最近変更した場合、パスワードの変更前に存在した SiteScope への URL は使用できません。

HP NNMi-HP SiteScope システム メトリックス統合

この項では以下の内容について説明します。

- 479 ページの「HP NNMi-HP SiteScope システムメトリックス統合について」
- 481 ページの「HP NNMi-HP SiteScope システム メトリックス統合の有効化」
- 484 ページの「HP NNMi-HP SiteScope システム メトリックス統合の使用法」
- 487 ページの「HP NNMi-HP SiteScope システム メトリックス統合の変更」
- 487 ページの「HP NNMi-HP SiteScope システム メトリックス統合の無効化」
- 488 ページの「HP NNMi-HP SiteScope システム メトリックス統合のトラブルシューティング」
- 492 ページの「HP NNMi-HP SiteScope システム メトリックス統合設定フォームのリファレンス」

HP NNMi-HP SiteScope システムメトリックス統合について

HP NNMi-HP SiteScope システム メトリックスの統合では、SiteScope モニタによって収集したシステム メトリックス データが NNM iSPI Performance for Metrics Network Performance Server (NPS) に入力されます。この統合では、データを以下のように処理します。

1 SiteScope が、SiteScope データ統合設定のレポート間隔で、モニタ データを XML ファイルに収集し、収集したデータを NNMi に渡します。

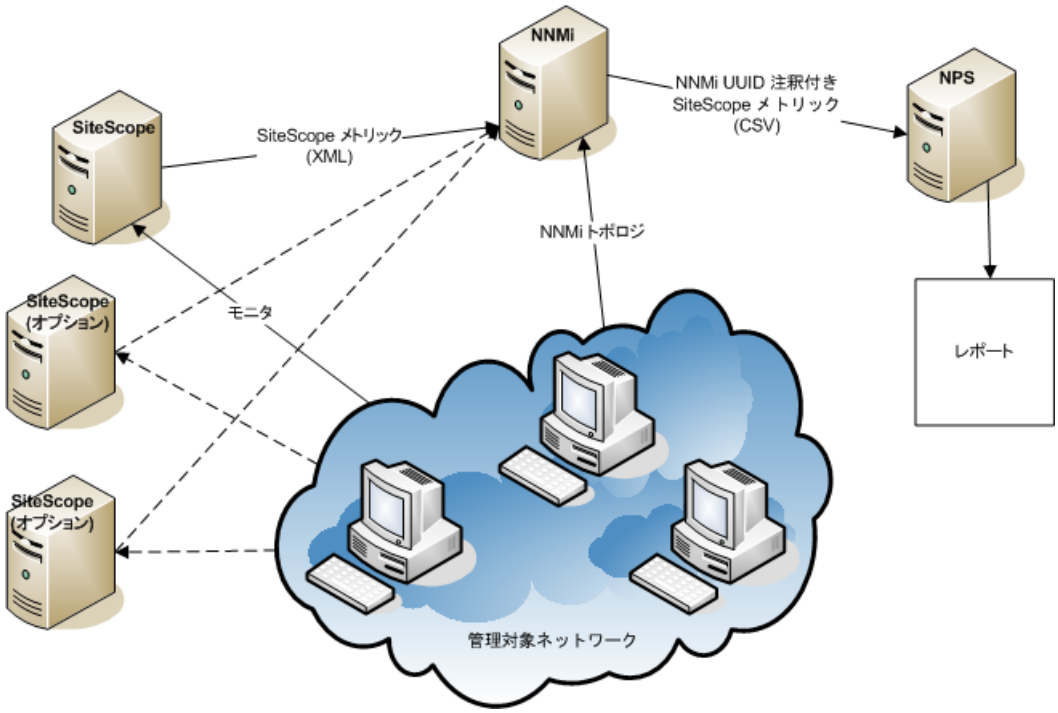
2 NNMi は、SiteScope データに NNMi ノードの UUID を追加します。

3 NNMiは､NPSが取得できるように設定された場所に追加されたデータを配置します。

4 NPS は、NPS 累積間隔で追加されたデータを取り込みます。

図 27にHP NNMi-HP SiteScopeシステムメトリックス統合のデータフローを示します。

図 27 HP NNMi-HP SiteScope システム メトリックス統合のデータ フロー



値

HP NNMi-HP SiteScope システム メトリックス統合により、SiteScope で収集したメトリックスのレポートを NPS で作成できます。

統合製品

このセクションの情報は、以下の製品に当てはまります。

- SiteScope

サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10
- NNM iSPI Performance for Metrics バージョン 9.10

この統合には、NNM iSPI Performance for Metrics ライセンスが必要です。

NNMi、NNM iSPI Performance for Metrics、および SiteScope は、同一のコンピュータまたは異なるコンピュータにインストールできます。

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。

サポートされる SiteScope モニタ

HP NNMi-HP SiteScope システム メトリックス統合では、以下のタイプの SiteScope モニタからのデータを認識します。

- CPU 使用率モニタ
- ディスク容量モニタ
- メモリ モニタ
- Microsoft Windows リソース モニタのプロセス監視対象オブジェクト
- UNIX リソース モニタのプロセス監視対象オブジェクト

監視対象ノードは、NNMi で管理する必要があります。この統合では、NNMi トポロジに存在しないノードと管理対象外のノードのデータを破棄します。

ドキュメント

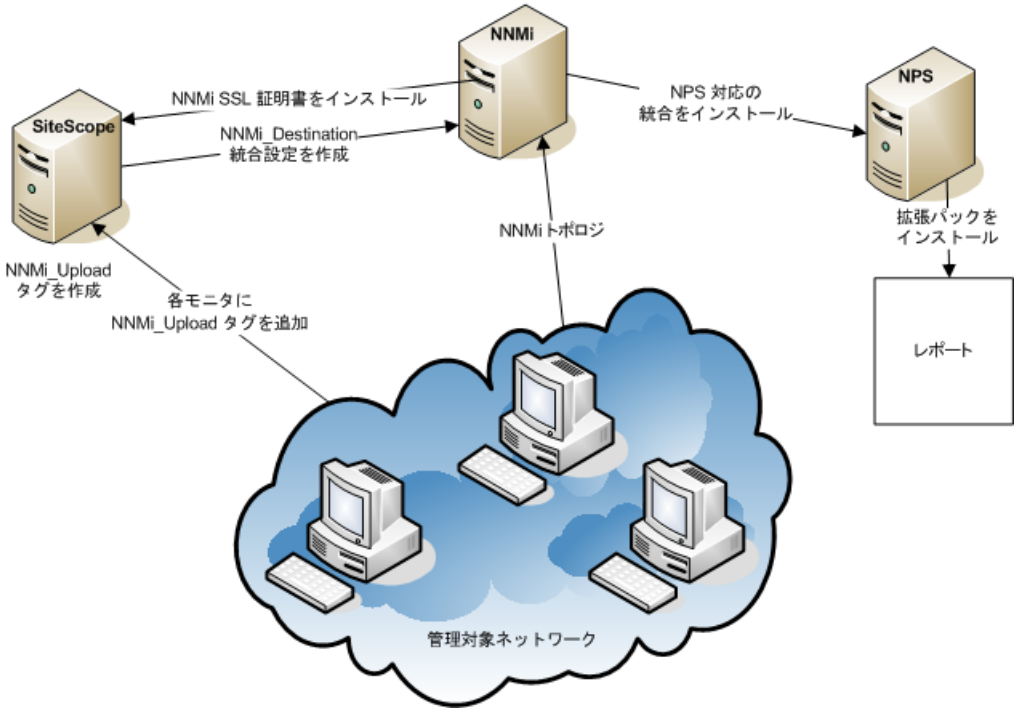
このセクションでは、SiteScope と通信するように NNMi を設定する方法と、SiteScope が収集したデータから作成可能な NPS レポートについて説明します。

SiteScope モニタの設定方法については、SiteScope 製品メディアに収録されている『HP SiteScope SiteScope の使用法 ガイド』で説明されています。

HP NNMi-HP SiteScope システム メトリックス統合の有効化

図 28に、HP NNMi-HP SiteScopeシステムメトリックス統合の設定ポイントを示します。

図 28　　HP NNMi-HP SiteScope システムメトリックス統合の設定ポイント



HP NNMi-HP SiteScope システムメトリックス統合を有効にするには、以下の手順を実行します。

1 NNMi コンソールで、SiteScope システム メトリックス統合パックを使用し、統合を有効にして NPS を設定します。

   a *オプション*。NNMi コンソールに接続するためにこの統合で使用する、Web Service Client ロールの NNMi ユーザーを作成します。

      または、この統合で Web Service Client ロールの既存ユーザーを使用できます。

   b **[HP NNMi-HP SiteScope System Metrics 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 SiteScope システム メトリックス]**)。

   c **[統合の有効化]** チェック ボックスをオンにします。

   d 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は、492 ページの「HP NNMi-HP SiteScope システム メトリックス統合設定フォームのリファレンス」を参照してください。

   e フォームの下部にある **[送信]** をクリックします。

      ウィンドウにステータス メッセージが表示されます。NNMi 資格証明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。

   f 結果ウィンドウから、データ統合 URL を一時的な場所にコピーします。この値は SiteScope を設定するときに使用します。

2 SiteScope ユーザー インタフェースで、NNMi と SSL 通信するように SiteScope サーバーを設定します。

   a **[設定]** ワークスペースで、**[証明書管理]** ページを開き、**[証明書のインポート]** をクリックします。

   b **[ソースの選択]** で、SiteScope に対して NNMi 管理サーバーを特定する情報を入力します。

      — **[ホスト]** が選択されていることを確認してから、NNMi 管理サーバーの完全修飾ドメイン名を入力します。

      — 必要に応じて、NNMi 管理サーバーの HTTPS ポートと一致するようにポート番号を変更します。

         詳細については、492 ページの「NNMi ポート」を参照してください。

   c **[ロード]** をクリックします。

      NNMi 証明書情報は、**[ロード済み証明書]** の下に表示されます。証明書のエイリアスを記録します。

   d NNMi 証明書を選択し、**[インポート]** をクリックします。

      NNMi 証明書の一覧は、**[証明書管理]** ページに表示されます。

3 SiteScope ユーザー インタフェースで、NNMi ターゲットを識別するのに使用する検索 / フィルタ タグを作成します。

   a **[設定]** ワークスペースで、**[検索 / フィルタ タグ]** ページを開き、**[新規タグ]** をクリックします。

   b タグ名 (たとえば、NNMi_upload) と少なくとも 1 つの値を入力します。

4 SiteScope ユーザー インタフェースで、SiteScope と NNMi の間の接続を設定します。

a **[設定]** ワークスペースで、**[統合設定]** ページを開き、**[新規統合]** をクリックして、**[データ統合]** をクリックします。

b **[一般設定]** で、名前 (たとえば、NNMi_receiver) とオプションの説明を入力します。

c **[データ統合の優先設定]** で、以下の設定を行います。

— **[レシーバの URL]** フィールドに、この手順の手順 1 の最後に保存した URL を貼り付けます (例 : `https://nnmi_server.example.com:443/sitescope-adapter/sitescopereceiver`)。

— **[GZIP 圧縮]** チェック ボックスをオンにします。

— **[追加データを含める]** と **[リダイレクトのエラー]** チェック ボックスをオフにします (これらはデフォルト設定です)。

— **[要求時に認証]** チェック ボックスをオンにします。(これはデフォルト設定です)。

— **[統合を無効化]** チェック ボックスをオフにします。(これはデフォルト設定です)。

その他のすべての設定については、デフォルトの設定を受け入れます。

d **[Web サーバーのセキュリティ設定]** の下で、手順 1 の統合設定フォームで指定した NNMi ユーザーのユーザー名とパスワードを入力します。

e **[レポート タグ]** の下で、手順 3 で作成した検索 / フィルタ タグ (たとえば、NNMi_upload) を選択します。

5 SiteScope ユーザー インタフェースで、NPS の SiteScope レポートに情報を提供するモニタを設定します。

a 必要に応じて、新規モニタを作成するか、サポートされるタイプの既存のモニタを特定します。

— CPU 使用率モニタ

— ディスク容量モニタ

— メモリ モニタ

— Microsoft Windows リソース モニタのプロセス監視対象オブジェクト

— UNIX リソース モニタのプロセス監視対象オブジェクト

b 手順 3 で作成した検索 / フィルタ タグ (たとえば、NNMi_upload) を、NNMi にデータを渡すモニタに追加します。

この統合では、NNMi トポロジ内の管理対象ノードのデータのみを処理できます。したがって、NNMi トポロジ内のノードのモニタにのみタグを適用します。

c 推奨。NNMi にデータを渡すモニタを 1 つのモニタ グループに集めます。

HP NNMi-HP SiteScope システム メトリックス統合の使用法

HP NNMi-HP SiteScope システム メトリックス統合により、NPS で以下の SiteScope モニタ レポートを作成できます。

- カレンダー
- チャート詳細
- ヒート チャート
- 管理対象インベントリ
- 最大変化
- ピーク期間
- しきい値スリーブ
- 上位 N
- 上位 N チャート

SiteScope システム メトリックス レポートにアクセスするには、以下の手順を実行します。

1. NNMi コンソールで、**[アクション] > [レポートーレポートメニュー]** をクリックします。
2. NPS の **[レポート]** ワークスペースで、**[SiteScope システム メトリックス] > [SiteScope] > [System_Metrics]** フォルダを開きます。

ベストプラクティス

以下のヒントを SiteScope システム メトリックス レポートに適用できます。

- 上位 N などの一部のレポートでは、SiteScope モニタの 1 つのタイプを対象にしたレポートのほうが、複数のモニタ タイプについてのレポートより容易に解釈できます。トポロジ フィルタで、[ComponentType] 属性として 1 つの値を選択します。
- [ノード名] 属性が設定されていない場合、レポートには、選択したタイプのすべてのモニタのデータが含められます。1 つ以上の特定のノードにレポート データを限定するには、それに応じて [ノード名] 属性を設定します。[ComponentType] 属性を設定すると、[ノード名] 選択リストには、選択したモニタ タイプを含むノードのみが表示されます。
- Windows リソース モニタについてのレポートの場合は、`Idle on` および `_Total on` データをフィルタで除去するのが効果的です。それには、トポロジ フィルタで、[ComponentName] 属性を `_Total on` および `Idle on` と異なる値に設定します。

表 50 に、統合によって追加されるグループ化オプションの一覧を示します。

表 50　使用可能なレポートグループ化オプション

オプション名	説明
Windows プロセス - プロセスの作成	測定対象プロセスを作成した親プロセスのプロセス ID (PID) を識別する整数値。
Windows プロセス - ID プロセス	測定対象プロセスのプロセス ID (PID) を識別する整数値。

表 50　使用可能なレポートグループ化オプション (続く)

オプション名	説明
UNIX プロセス - PID	測定対象プロセスのプロセス ID (PID) を識別する整数値。
UNIX プロセス - ユーザー	測定対象プロセスの UNIX ユーザー ID (uid) を識別する整数値。
修飾コンポーネント名	メトリックス名と、メトリックスを収集したノードを識別する文字列値。修飾コンポーネント名の形式は、`<metric_name>` on `<node_long_name>` (例 : `disk percent full on device.example.com`) です。 修飾コンポーネント名は、推奨されるグループ化オプションの選択肢です。

表 51 に、統合によって追加されるメトリックスの一覧を示します。各メトリックスについて、実際の値をレポートするように選択できます。メトリックスが多い場合は、しきい値情報もレポートできます。レポート値の解釈の詳細については、各オペレーティング システムのマニュアルを参照してください。

表 51　報告可能な SiteScope システム メトリックス

モニタ タイプ	使用可能なメトリックス
CPU 使用率 [1]	• CPU 使用率
ディスク容量	• 空きディスク MB • ディスク割合 (フル)
メモリ [2]	• メモリ ページ / 秒 • 仮想メモリ使用率 • 空き仮想メモリ MB • スワップ メモリ使用率 • 空きスワップ メモリ MB • 物理メモリ使用率 • 空き物理メモリ MB

表 51　報告可能な SiteScope システム メトリックス (続く)

モニタ タイプ	使用可能なメトリックス
Microsoft Windows のリソース	• Windows プロセス - 権限時間の割合 • Windows プロセス - プロセッサ時間の割合 • Windows プロセス - ユーザー時間の割合 • Windows プロセス - プロセス ID の作成 • Windows プロセス - 経過時間 • Windows プロセス - 処理数 • Windows プロセス - ID プロセス • Windows プロセス - IO データ (バイト / 秒) • Windows プロセス - IO データ操作 / 秒 • Windows プロセス - その他の IO データ (バイト / 秒) • Windows プロセス - その他の IO 操作 / 秒 • Windows プロセス - IO 読み取り (バイト / 秒) • Windows プロセス - IO 読み取り操作 / 秒 • Windows プロセス - IO 書き込み (バイト / 秒) • Windows プロセス - IO 書き込み操作 / 秒 • Windows プロセス - ページ障害 • Windows プロセス - ページ ファイル (バイト) • Windows プロセス - ピーク時のページ ファイル (バイト) • Windows プロセス - 非ページ プール (バイト) • Windows プロセス - ページ プール (バイト) • Windows プロセス - 優先度ベース • Windows プロセス - プライベート (バイト) • Windows プロセス - スレッド数 • Windows プロセス - 仮想 (バイト) • Windows プロセス - ピーク時の仮想 (バイト) • Windows プロセス - ワーキング セット • Windows プロセス - プライベート ワーキング セット • Windows プロセス - ピーク時のワーキング セット
UNIX のリソース [3]	• UNIX プロセス - CPU 割合 • UNIX プロセス - memsize • UNIX プロセス - number_running • UNIX プロセス - PID • UNIX プロセス - ユーザー

1 SiteScope では、HP-UX および AIX オペレーティング システムで収集した CPU 使用率データを、特定の CPU 単位ではなく、システムの 1 つの平均値として要約します。この統合では平均値を NPS に送信しないため、HP-UX および AIX オペレーティング システムでは CPU 使用率データを使用できません。

2 SiteScope は、すべてのオペレーティングシステムでこれらのメトリックスをすべて収集するわけではありません。

3 HP-UX オペレーティング システムの UNIX リソース モニタの場合、SiteScope は、CPU 割合、実行数、およびプロセス ID のみを収集します。HP-UX ノードのメモリ サイズとユーザー データは使用できません。

HP NNMi-HP SiteScope システム メトリックス統合の変更

HP NNMi-HP SiteScope システム メトリックス統合は、以下の方法で変更できます。

- NNMi から NPS への接続を変更する
- SiteScope から NNMi への接続を変更する

NNMi から NPS への接続を変更する

NPS への接続情報を変更するには、以下の手順を実行します。

1 NNMi コンソールで、**[HP NNMi-HP SiteScope System Metrics 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 SiteScope システム メトリックス]**)。

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は、492 ページの「HP NNMi-HP SiteScope システム メトリックス統合設定フォームのリファレンス」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。有効にすると、データ統合 URL が変更された場合に **[HP NNMi-HP SiteScope System Metrics の統合設定]** フォームに表示されるその URL が更新され、483 ページの手順 4 の説明のとおりに SiteScope データ統合設定が更新されます。

SiteScope から NNMi への接続を変更する

SiteScope データ レシーバの情報を変更するには、以下の手順を実行します。

1 SiteScope インタフェースで、SiteScope と NNMi の間の接続を定義するデータ統合を開きます (**[設定] > [統合設定]** の順に選択)。

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、SiteScope ヘルプを参照してください。

3 **[統合を無効化]** チェック ボックスがオフになっていることを確認して、フォームの下部にある **[OK]** 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 SiteScope システム メトリックス統合の無効化

HP NNMi-HP SiteScope システム メトリックス統合を完全に無効にするには、以下の両方の手順を実行します。

- NNMi から NPS への接続を無効にする
- SiteScope から NNMi への接続を無効にする

NNMi から NPS への接続を無効にする

NNMi による SiteScope のモニタ データの処理を停止するには、以下の手順を実行します。

1 NNMi コンソールで、**[HP NNMi-HP SiteScope System Metrics 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 SiteScope システム メトリックス]**)。

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。

   変更はただちに有効になります。

SiteScope から NNMi への接続を無効にする

SiteScope から NNMi 管理サーバーへのモニタ データの送信を停止するには、以下の手順を実行します。

1 SiteScope インタフェースで、SiteScope と NNMi の間の接続を定義するデータ統合を開きます (**[設定] > [統合設定]** の順に選択)。

2 **[統合を無効化]** チェック ボックスをオンにして、フォームの下部にある **[OK]** 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 SiteScope システム メトリックス統合のトラブルシューティング

XML 解析エラーや、NNMi トポロジ内に存在しないノードのモニタ データの情報を含む、SiteScope データの処理に関連したメッセージは、NNMi 管理サーバーの `nnm.0.0.log` (および古い) ファイルに記録されます。NNMi 管理サーバーで問題が発生した場合は、それらのログ ファイル、文字列 `com.hp.ov.nnm.sitescope.im` または `com.hp.ov.nms.im.sitescope` で始まるクラスの SEVERE メッセージや WARNING メッセージがないかどうか調べてください。詳細については、373 ページの「NNMi ロギング」を参照してください。

SiteScope ログ ファイルには、データ統合の問題に関するメッセージが収集されます。SiteScope ログ ファイルを調べて、以下の設定問題の 1 つ以上が原因で発生しやすいデータ送信エラーがないか探してください。

- 証明書エラー。NNMi 証明書が SiteScope に正しくロードされていません。
- ユーザー名とパスワードの認証エラー : NNMi コンソールの **[HP NNMi-HP SiteScope System Metrics の統合設定]** フォームで、**[NNMi ユーザー]**、**[NNMi パスワード]**、またはその両方の値が正しくありません。
- 統合モジュールの有効化エラー : NNMi コンソールの **[HP NNMi-HP SiteScope System Metrics の統合設定]** フォームで、**[統合の有効化]** チェック ボックスがオフになっています。

SiteScope ログ ファイルの詳細については、SiteScope のマニュアルを参照してください。

この項では以下の内容について説明します。

- 489 ページの「統合データ フローを確認する」
- 490 ページの「統合設定の NNMi 側を確認する」
- 491 ページの「ファイアウォールの背後の NAT 構成環境にノードのレポートデータが存在しない」

統合データ フローを確認する

SiteScope からの XML ファイル

システムメトリックス統合では、SiteScope データサンプルが `*.gz` ファイルとして NNMi 管理サーバーの以下のディレクトリに置かれます。

- *Windows*:
  `%NnmDataDir%¥shared¥perfspi¥datafiles¥metric¥working¥sitescope`
- *UNIX*:
  `$NnmDataDir/shared/perfspi/datafiles/metric/working/sitescope`

デフォルトで、システムメトリックス統合は新しいファイルをこのディレクトリに毎分配置し、NNMi は 5 分ごとにそれらのファイルを取り込みます。

SiteScope データ統合設定のレポート間隔により、SiteScope がシステムメトリックス統合にデータサンプルを送信する頻度が決まります。NNMi の使用率をユーザーが設定することはできません。

`sitescope` ディレクトリが 2 分より長い間空の状態になると、SiteScope はファイルを配信しなくなります。この場合は、以下を実行します。

1. SiteScope ユーザー インタフェースで、データ統合設定が有効であり、483 ページの手順 4 の説明に従って設定されていることを確認します。

   また、**[レポート間隔]** フィールドの値も確認します。

2. SiteScope ユーザー インタフェースで、少なくとも 1 つのモニタ設定に、データ統合設定に関連付けられた検索 / フィルタ タグがあることを確認します。

`sitescope` ディレクトリにファイルが累積されると、NNMi はファイルを取り込まなくなります。この場合は、NNMi コンソールで、HP NNMi-HP SiteScope システム メトリックス統合が正しく設定されていることを確認します。詳細については、490 ページの「統合設定の NNMi 側を確認する」を参照してください。

NNMi からの CSV ファイル

NNMi は、NNMi 管理サーバーの以下のディレクトリに、NPS が取り込む `SiteScopeMetrics_*.csv.gz` ファイルを配置します。

- *Windows*: `%NnmDataDir%¥shared¥perfspi¥datafiles¥metric¥final`
- *UNIX*: `$NnmDataDir/shared/perfspi/datafiles/metric/final`

NNMi は、およそ 5 分ごとに新しいファイルをこのディレクトリに配置し、NPS はこれらのファイルをおよそ 5 分ごとに取り込みます。

NNMi の配置率をユーザーが設定することはできません。NPS の累積率により、NPS がこのディレクトリのファイルを取り込む頻度が決まります。NPS 累積率は NNM iSPI Performance for Metrics によって設定されます。ユーザーが設定することはできません。

`final` ディレクトリが 10 分より長い間空の状態になると、NNMi はファイルを配信しなくなります。この場合は、NNMi コンソールで、HP NNMi-HP SiteScope システム メトリックス統合が正しく設定されていることを確認します。詳細については、490 ページの「統合設定の NNMi 側を確認する」を参照してください。

`final` ディレクトリにファイルが累積されると、NPS はファイルを取り込まなくなります。その場合は、NPS のトラブルシューティングのマニュアルを参照してください。

レポート ファイルが final ディレクトリを通過してから 2 時間以内に NPS ユーザーインタフェースで SiteScope レポートが使用可能にならない場合、この統合は正しく設定されていません。この場合は、SiteScope、NNMi ovjboss プロセス、および NPS を以下の順に再起動してください。

1 SiteScope を再起動します。

- *Windows*:
  - **[サービス]** コントロールパネル (**[スタート] > [コントロールパネル] > [管理ツール] > [サービス]**) を開きます。
  - サービスのリストで、**[SiteScope]** を右クリックし、**[開始]** をクリックします。
- *Linux または Solaris*:
  - SiteScope がインストールされているサーバーで、ターミナルウィンドウを開きます。
  - 以下の構文を使用して、start コマンドのシェルスクリプトを実行します。

    <installpath>/SiteScope/start

2 以下のコマンドを実行して ovjboss を再開します。

a **ovstop ovjboss**

b **ovstart ovjboss**

3 NPS を再起動します。

統合設定の NNMi 側を確認する

1 NNMi コンソールで、**[HP NNMi-HP SiteScope System Metrics 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 SiteScope システム メトリックス]**)。

このフォームのフィールドの詳細は、492 ページの「HP NNMi-HP SiteScope システム メトリックス統合設定フォームのリファレンス」を参照してください。

2 統合のステータスを確認するには、**[HP NNMi-HP SiteScope System Metrics の統合設定]** フォームで、フォームの下にある **[送信]** をクリックします (設定の変更は行いません)。

ウィンドウにステータス メッセージが表示されます。

3 NNMi への接続が正常に設定されていることを確認します。

この手順の 手順 1 で NNMi コンソール に接続するために、このステップで説明してある情報を使用した場合は、NNMi コンソール に再接続する必要はありません。手順 4 を継続します。

a Web ブラウザで、次の URL を入力します。

<protocol>://<NNMiserver>:<port>/nnm/

以下のように、変数が **[HP NNMi-HP SiteScope System Metrics の統合設定]** フォームの値に関係する場合 :

- **[NNMi SSL が有効になっています]** チェック ボックスがオンの場合、<protocol> は https です。
- **[NNMi SSL が有効になっています]** チェック ボックスがオフになっている場合、<protocol> は http です。
- <NNMiserver> は **[NNMi ホスト]** の値です。
- <port> は、**[NNMi ポート]** の値です。

b プロンプトが表示されたら、管理者ロールで NNMi ユーザーの資格認定を入力します。

NNMi コンソール が表示されるはずです。NNMi コンソール が表示されない場合は NNMi 管理者に連絡して、NNMi に接続するために使用している情報を確認してください。NNMi コンソール が表示されるまで、NNMi への接続のトラブルシューティングを継続します。

「Web サービス クライアント」ロールを持つユーザーとして NNMi コンソールにサインインすることはできません。

c NNMi 管理者に連絡して、Web サービスクライアントロールを持つ NNMi 統合ユーザーの **[NNMi ユーザー]** と **[NNMi パスワード]** の値を確認します。

パスワードは NNMi コンソール では非表示です。NNMi ユーザー名のパスワードが何か確信がない場合は、NNMi 管理者に問い合わせするか、またはパスワードをリセットします。

4 この手順の手順 3 で使用して正常に接続できた値で、**[HP NNMi-HP SiteScope System Metrics の統合設定]** フォームを更新します。

詳細については、492 ページの「HP NNMi-HP SiteScope システム メトリックス統合設定フォームのリファレンス」を参照してください。

5 フォームの下部にある **[送信]** をクリックします。

6 ステータス メッセージに問題があることがまだ表示される場合は、以下の手順を実行します。

a Web ブラウザのキャッシュをクリアします。

b Web ブラウザから、すべての保存フォームまたはパスワード データをクリアします。

c Web ブラウザ ウィンドウを完全に閉じてから、もう一度開きます。

d この手順の手順 4 と手順 5 を繰り返します。

7 489 ページの「統合データ フローを確認する」の説明に従って、SiteScope モニタ データの転送を監視して設定をテストします。

ファイアウォールの背後のNAT構成環境にノードのレポートデータが存在しない

ネットワーク アドレス変換 (NAT) 環境において、SiteScope サーバーが、ファイアウォールの背後に展開されている場合に、ファイアウォールの外部に重複する IP アドレスを持つノードのデータをレポートしても、NNMi は監視対象のノードを判別できません。この場合、この統合では、これらのノードの SiteScope データを NPS に提供しないため、NPS のレポートにこの情報は含まれません。

HP NNMi-HP SiteScope システム メトリックス統合設定フォームのリファレンス

[HP NNMi-HP SiteScope System Metrics の統合設定] フォームには、NNMi と SiteScope の間の通信を設定するパラメータが含まれています。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 SiteScope System Metrics の統合設定]** フォームにアクセスできます。

[HP NNMi-HP SiteScope System Metrics の統合設定] フォームでは、NNMi 管理サーバーを識別するための情報を収集します。

統合設定に変更を適用するには、**[HP NNMi-HP SiteScope System Metrics 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。

表 52 に、NNMi 管理サーバーへの接続パラメータをリストします。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 52　NNMi 管理サーバー情報

フィールド	説明
NNMi SSL 有効化	接続プロトコル指定。 • 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。
NNMi ホスト	NNMi 管理サーバーの完全修飾ドメイン名。このフィールドには、NNMi コンソール へのアクセスに使用するホスト名があらかじめ入力されています。この値が、NNMi 管理サーバー上で **`nnmofficialfqdn.ovpl -t`** コマンド実行によって返された名前であることを確認します。
NNMi ポート	NNMi コンソール に接続するためのポート。このフィールドには、次のファイルで指定されているように、NNMi コンソール との通信のために jboss アプリケーション サーバーが使用するポートがあらかじめ記入されています。 • *Windows*: `%NnmDataDir%¥conf¥nnm¥props¥nms-local.properties` • *UNIX*: `$NnmDataDir/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。
NNMi ユーザー	NNMi コンソール に接続するためのユーザー名。このユーザーには、Web Service Client ロールが必要です。
NNMi パスワード	指定の NNMi ユーザーのパスワード。

HP Systems Insight Manager

HP Systems Insight Manager (SIM) により、HP サーバーとストレージ デバイスのシステム管理を行うことができます。SIM の機能には、システムの検出と識別、単一イベント ビュー、インベントリ データ収集、および報告などがあります。

SIM は以下のタスクで役立ちます。

- サーバーとストレージ インフラストラクチャが関係する複雑な問題のトラブルシューティングを行います。
- サーバーおよびストレージ資産の情報をメンテナンスします。
- インフラストラクチャとアプリケーションの変更を行う前に、それらの変更による影響をモデル化します。
- 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。
- 専門分野の枠を越えてネットワーク管理担当者をトレーニングします。
- ネットワーク管理の焦点を、日常のメンテナンスから将来的な業務上のニーズにシフトさせます。

SIM の購入に関する詳細については、HP 販売員にお尋ねください。

この章には、以下のトピックがあります。

- HP NNMi-HP SIM 統合
- HP NNMi-HP SIM 統合の有効化
- HP NNMi-HP SIM 統合の使用法
- HP NNMi-HP SIM 統合設定の変更
- HP NNMi-HP SIM 統合の無効化
- HP NNMi-HP SIM 統合のトラブルシューティング
- [HP NNMi-HP SIM 統合設定] フォームのリファレンス

HP NNMi-HP SIM 統合

HP NNMi-HP SIM 統合では、NNMi コンソールから数種類の SIM ツールにアクセスするためのアクションを使用できます。

値

HP NNMi-HP SIM 統合では、ネットワーク デバイス情報を NNMi に追加して、NNMi ユーザーが HP ProLiant サーバーとストレージ デバイスの潜在的なネットワーク問題を検出および調査できるようにします。

統合製品

この章の情報は、以下の製品に当てはまります。

- SIM

  サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10

NNMi と SIM は、別々のコンピュータにインストールする必要があります。NNMi 管理サーバーと SIM サーバー コンピュータのオペレーティング システムは、同じでも異なっていても構いません。

NNMi で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、『NNMi システムおよびデバイスのサポート マトリックス』を参照してください。

SIM で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、以下の QuickSpecs のサイトを参照してください。

www.hp.com/go/sim

ドキュメント

この章では、SIM と通信するように NNMi を設定する方法、および NNMi コンソールから SIM 統合を使用する方法について説明します。

SIM のドキュメント スイートでは、SIM 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、以下の SIM 情報ライブラリのサイトからダウンロードできます。

www.hp.com/go/sim

HP NNMi-HP SIM 統合の有効化

NNMi 管理サーバーで、以下の手順に従って NNMi と SIM 間の接続を設定します。

1. NNMi コンソールで、**[HP NNMi-HP SIM 統合設定]** フォームを開きます (**[統合モジュールの設定] > [HP SIM]**)。
2. **[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。
3. 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は、498 ページの「NNMi 管理サーバー接続」を参照してください。
4. SIM 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は、499 ページの「SIM サーバー接続」を参照してください。
5. 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。
6. SIM 管理対象デバイスのインシデント定義をロードします。
   a. ディレクトリを次のように変更します。
      — *Windows*: `%NnmInstallDir%¥newconfig¥HPOvNmsEvent`
      — *UNIX*: `$NnmInstallDir/newconfig/HPOvNmsEvent`
   b. 以下のコマンドを入力して、SIM インシデント定義をインポートします。

      ```
      nnmconfigimport.ovpl -f nnm-sim-incidentConfig.xml ¥
      -u <username> -p <password>
      ```
7. オプションおよび推奨事項。SIM 管理対象デバイスが生成するトラップの MIB 定義ファイルをロードします。
   a. ディレクトリを次のように変更します。
      — *Windows*: `%NNM_SNMP_MIBS%¥Vendor¥Hewlett-Packard¥SystemsInsightManager`
      — *UNIX*: `$NNM_SNMP_MIBS/Vendor/Hewlett-Packard/SystemsInsightManager`
   b. nnmloadmib.ovpl コマンドを使用して、管理対象環境の適切な MIB ファイルをロードします。たとえば、以下のようにします。

      ```
      nnmloadmib.ovpl -load cpqhost.mib -u <username> -p <password>
      ```

      — HP ProLiant デバイスのトラップの場合は、`cpqhost.mib` ファイルをロードしてから、`SystemsInsightManager` ディレクトリにある残りの `cpq*.mib` ファイルをロードします。
      — HP Virtual Connect デバイスのトラップの場合は、`vc*.mib` ファイルと `fa-mib40.mib` ファイルを NNMi にロードします。
   c. 以下のコマンドを入力して、MIB が正常にロードされたことを確認します。

      ```
      nnmloadmib.ovpl -list -u <username> -p <password>
      ```

HP NNMi-HP SIM 統合の使用法

HP NNMi-HP SIM 統合には、NNMi コンソールからデバイス上の SIM エージェントへのリンク、または SIM への直接リンクが設定されています。この統合では、製品間のシングル サインオン機能は提供されません。SIM ページを表示するには、SIM ユーザー資格証明を入力する必要があります。

HP NNMi-HP SIM 統合を有効にすると、以下のアクションが NNMi コンソールに追加されます。

- **HP システム管理ホームページ** - NNMi コンソールで選択したノードの HP System Management デバイスのホームページを開きます。
- **HP Systems Insight Manager ホーム** - SIM ホーム ページを開きます。
- **HP Systems Insight Manager** - NNMi コンソールで選択したノードの SIM System ページを開きます。

HP NNMi-HP SIM 統合設定の変更

1. NNMi コンソールで、**[HP NNMi-HP SIM 統合設定]** フォームを開きます (**[統合モジュールの設定] > [HP SIM]**)。
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は、498 ページの「[HP NNMi-HP SIM 統合設定] フォームのリファレンス」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。ovjboss を再起動する必要はありません。

HP NNMi-HP SIM 統合の無効化

1. NNMi コンソールで、**[HP NNMi-HP SIM 統合設定]** フォームを開きます (**[統合モジュールの設定] > [HP SIM]**)。
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。これで、統合アクションを使用できなくなります。

変更はただちに有効になります。ovjboss を再起動する必要はありません。

HP NNMi-HP SIM 統合のトラブルシューティング

SIM アクションが機能しない

[HP NNMi-HP SIM 統合設定] フォームの値が正しいことを確認しても、NNMi コンソールから SIM ページを開くことができない場合は、以下の手順を実行します。

1 Web ブラウザのキャッシュをクリアします。

2 Web ブラウザから、すべての保存フォームまたはパスワード データをクリアします。

3 Web ブラウザ ウィンドウを完全に閉じてから、もう一度開きます。

4 **[HP NNMi-HP SIM 統合設定]** フォームに値を再入力します。

NNMi は SIM サーバーへの接続をサイレントに検証できないため、**[HP NNMi-HP SIM 統合設定]** フォームのステータス メッセージは NNMi 管理サーバーの接続情報にのみ適用されます。

5 Web ブラウザで SIM ホームページを開いて、SIM が実行されていることを確認します。

トラップの MIB キャッシュ メッセージで OID を検出できない

SIM 管理対象デバイスが生成するトラップの MIB 定義ファイルが NNMi にロードされない場合は、以下のテキストのようなエラー メッセージが表示されます。

<Cia .1.3.6.1.4.1.11.5.7.5.2.1.1.1.7.0 with value 1 was not found within the mib cache>

このようなエラーを解決するには、495 ページの手順 7 の説明に従って MIB をロードします。

[HP NNMi-HP SIM 統合設定] フォームのリファレンス

[HP NNMi-HP SIM 統合設定] フォームには、NNMi と SIM 間の通信を設定するためのパラメータが含まれています。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 SIM 統合設定]** フォームにアクセスできます。

[HP NNMi-HP SIM 統合設定] フォームは、以下の一般領域に関する情報を収集します。

- NNMi 管理サーバー接続
- SIM サーバー接続

統合設定に変更を適用するには、**[HP NNMi-HP SIM 統合設定]** フォームの値を更新して、**[送信]** をクリックします。

NNMi 管理サーバー接続

表 53 に、NNMi 管理サーバーへの接続パラメータをリストします。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 53　NNMi 管理サーバー情報

フィールド	説明
NNMi SSL 有効化	接続プロトコル指定。 • 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。これがデフォルト設定です。 • 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。
NNMi ホスト	NNMi 管理サーバーの完全修飾ドメイン名。このフィールドには、NNMi コンソールへのアクセスに使用するホスト名があらかじめ入力されています。この値が、NNMi 管理サーバー上で **`nnmofficialfqdn.ovpl -t`** コマンド実行によって返された名前であることを確認します。
NNMi ポート	NNMi コンソール に接続するためのポート。このフィールドには、次のファイルで指定されているように、NNMi コンソール との通信のために jboss アプリケーション サーバーが使用するポートがあらかじめ記入されています。 • *Windows*: `%NnmDataDir%¥conf¥nnm¥props¥nms-local.properties` • *UNIX*: `$NnmDataDir/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。

表 53　NNMi 管理サーバー情報 (続く)

フィールド	説明
NNMi ユーザー	NNMi コンソール 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。

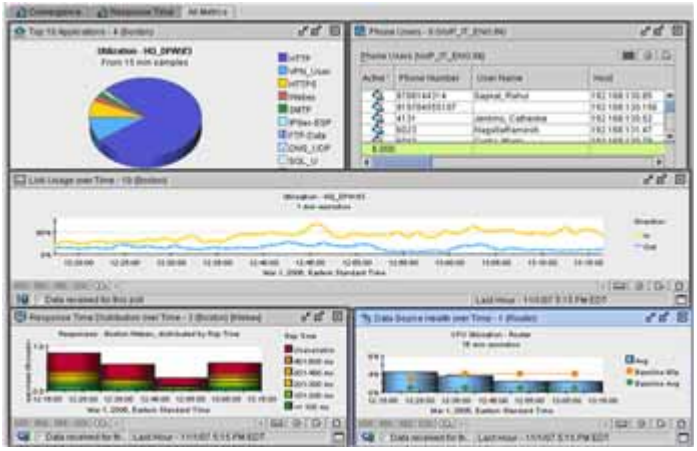
SIM サーバー接続

表 54 に、SIM サーバーに接続して SIM ページを開くためのパラメータを示します。SIM 管理者と協力して、この設定項目に適切な値を決定してください。

表 54　SIM サーバー情報

SIM サーバー パラメータ	説明
SIM SSL 有効化	SIM に接続するための接続プロトコル指定。 • SIM が HTTPS を使用するよう設定されている場合は、**[HP SIM SSLの有効化]** チェック ボックスをオンにします。これがデフォルト設定です。 • SIM が HTTP を使用するよう設定されている場合は、**[HP SIM SSL の有効化]** チェック ボックスをオフにします。
SIM ホスト	SIM サーバーの完全修飾ドメイン名。
SIM ポート	SIM に接続するためのポート。 デフォルトの SIM 設定を使用する場合は、ポート 50000 を使用します (SIM への SSL 接続の場合)。

nGenius Performance Manager



NetScout Systems nGenius Performance Manager では、以下の目的のために、複雑なネットワークを見通すことができます。

- アプリケーションの認識と監視
- パケットとフローの分析とトラブルシューティング
- 応答時間分析
- 報告および容量計画作成
- 集中性管理
- 警報生成とイベント識別

nGenius Performance Manager は、パケットの綿密な調査とフローベースの技術を活用し、いくつかのタイプのデータについて、リアルタイムの稼働インテリジェンスの見通しを提供します。

- 高度で重要なパフォーマンス インジケータ (KPI)。たとえば、応答時間、エラー、ジッターなど
- アプリケーション フロー データ。たとえば、使用率、会話、トップのトーカーなど
- パケットレベルの分析。たとえば、復号化、反発図など

nGenius Performance Manager は、さまざまなネットワーク データ ソースからパフォーマンス データを収集し、すべてのネットワーク インフラストラクチャ、トポロジ、およびアプリケーションの使用パターンを監視できます。nGenius Performance Manager は、一連のリアルタイムおよび履歴のビューおよびレポートの形態で結果を表示し、以下の情報を提供できます。

- アプリケーション パフォーマンス
- ネットワーク リソースのユーザーと悪用者
- ネットワーク容量のリソース消費

nGenius Performance Manager の購入については、HP 販売員にお尋ねください。

この章には、以下のトピックがあります。

- HP NNMi-nGenius Performance Manager 統合
- HP NNMi-nGenius Performance Manager 統合の有効化
- HP NNMi-nGenius Performance Manager 統合の使用法
- HP NNMi-nGenius Performance Manager 統合の無効化
- HP NNMi-nGenius Performance Manager 統合のトラブルシューティング

HP NNMi-nGenius Performance Manager 統合

nGenius Performance Manager を HP Network Node Manager i Software (NNMi) 環境に組み入れることにより、NNMi を使用してネットワーク デバイスを監視および管理するネットワーク管理者は、nGenius デバイスによってアプリケーションレベルの状況を表示できます。

HP NNMi-nGenius Performance Manager 統合では、以下の機能を使用できます。

- nGenius Performance Manager サーバーとプローブのアラームを NNMi インシデント ビューで受信する。
- コンテキスト ビューを nGenius Performance Manager に起動して、インシデントの原因を調査します。
- NNMi マップ ビューに、NetScout アイコンを使って eGenius プローブを表示する。
- NNMi コンソールから nGenius Performance Manager QuickViews を起動する。
- NNMi コンソールから nGenius Performance Manager アプリケーションを起動する。
- NNMi インシデント ビューに表示される nGeneius Performance Manager インシデントの NNMi レイヤー 2 およびレイヤー 3 近隣接続ビューを起動する。
- NNMi インシデント ビューに表示される nGeneius Performance Manager インシデントの NNMi パス ビュー マップを起動する。
- nGenius Performance Manager によって生成されるアラームごとに、クリア トラップ アラームを NNMi に転送する。

値

HP NNMi-nGenius Performance Manager 統合には、以下の利点があります。

- 最大のネットワーク可用性を配信するコストを削減します。
- ネットワーク管理インフラストラクチャを 1 つのコンソールに統合します。
- 統合障害とアプリケーションの認識パフォーマンス データによって、スタッフの生産性および効率性を向上させます。
- フローとパケットレベル詳細のコンテキスト ドリルダウンで MTTR を縮小し、パフォーマンス問題を識別します。

統合製品

この章の情報は、以下の製品に当てはまります。

- nGenius Performance Manager

  サポートされるバージョンは、*NNMi システムおよびデバイスのサポート マトリックス*にリストされています。

- nGenius Performance Manager に同梱された nGenius K2 バージョン
- CDM Agent Firmware
- nGenius InfiniStream アプライアンス
- NNMi 9.10

NNMi と nGenius Performance Manager サーバーは別々のコンピュータにインストールする必要があります。NNMi 管理サーバーと nGenius Performance Manager サーバーコンピュータのオペレーティング システムは、同じでも、異なっていても構いません。

ドキュメント

HP NNMi-nGenius Performance Manager 統合については、以下のドキュメントで詳しく説明されています。

nGenius Performance Manager と HP Network Node Manager i Software の統合
(NetScout パーツ番号 733-0194 Rev.A。
http://www.netscout.com から入手できます)

HP NNMi-nGenius Performance Manager 統合の有効化

HP Network Node Manager インストール ファイル用の nGenius Performance Manager 統合ユーティリティは nGenius Performance Manager サーバーの次の場所で入手できます。

- *Windows*: `%nGenius Install%¥rtm¥bin¥nGeniusNNM8.zip`
- *UNIX*: `$nGenius Install/rtm/bin/nGeniusNNM8.zip`

管理権限または root 権限を持つユーザーとして、NNMi 管理サーバーに統合ユーティリティをインストールします。このユーティリティは、NNMi 統合関連のすべての nGenius Server 設定データを NNMi にインポートします。

nGenius Performance Manager 統合ユーティリティをインストールする高度なステップは次のとおりです。詳細については、「*nGenius Performance Manager と HP Network Node Manager i Software の統合*」を参照してください。

1. インストール ファイルを抽出し、nGenius Performance Manager 内の NNMi サポートを設定します。
2. NNMi で NetScout インシデント (アラーム) を設定します。
3. nGenius Probe が SNMP トラップをポート 395 に送信するように設定します。
4. *オプション。*プローブ ルーター マッピングを設定します。

HP NNMi-nGenius Performance Manager 統合の使用法

HP NNMi-nGenius Performance Manager 統合の使用法については、「*nGenius Performance Manager と HP Network Node Manager i Software の統合*」を参照してください。

HP NNMi-nGenius Performance Manager 統合の無効化

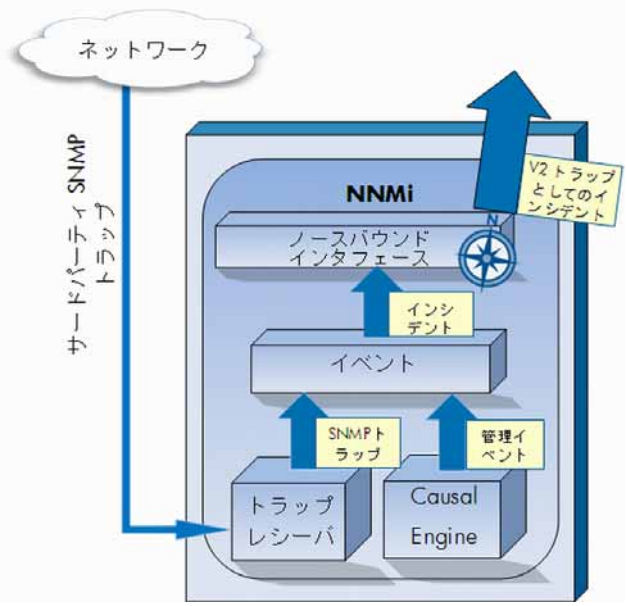
HP NNMi-nGenius Performance Manager 統合の無効化の詳細については、「*nGenius Performance Manager と HP Network Node Manager i Software の統合*」を参照してください。

HP NNMi-nGenius Performance Manager 統合のトラブルシューティング

HP NNMi-nGenius Performance Manager 統合のトラブルシューティングの詳細については、NetScout Systems 顧客サポートにお問い合わせください。問い合わせ情報は次の URL にあります。

http://www.netscout.com/support

NNMi ノースバウンド インタフェース



HP Network Node Manager i Software (NNMi) には、NNMi Northbound インタフェースが用意されており、SNMPv2c トラップを受信できるアプリケーションに NNMi インシデントを転送することができます。各 NNMi 管理サーバーに、別々に設定された複数の NNMi Northbound インタフェースを実装できます。

NNMi には、NNMi Northbound インタフェースを使用して以下の製品との統合をサポートする機能も組み込まれています。

- HP Business Service Management (BSM) の Operations Management 機能。詳細については、521 ページの「HP BSM Operations Management」を参照してください。
- HP Operations Manager (HPOM) アクティブ メッセージ ブラウザ。詳細については、539 ページの「HP NNMi-HPOM 統合 (エージェント実装)」を参照してください。
- IBM Tivoli Netcool/OMNIbus。詳細については、577 ページの「HP NNMi Integration Module for Netcool Software」を参照してください。

異なる Northbound アプリケーションと統合するには、この章の指示に従ってください。

この章には、以下のトピックがあります。

- NNMi ノースバウンド インタフェース
- NNMi ノースバウンド インタフェースの有効化
- NNMi ノースバウンド インタフェースの使用法
- NNMi ノースバウンド インタフェースの変更
- NNMi ノースバウンド インタフェースの無効化
- NNMi ノースバウンド インタフェースのトラブルシューティング
- アプリケーション フェールオーバーと NNMi ノースバウンド インタフェース
- [NNMi Northbound Interface デスティネーション] フォームのリファレンス

NNMi ノースバウンド インタフェース

NNMi Northbound インタフェースは、NNMi 管理イベントを SNMPv2c トラップとして Northbound アプリケーションに転送します。Northbound アプリケーションは、NNMi トラップをフィルタリング、処理、および表示します。Northbound アプリケーションには、NNMi トラップのコンテキストで NNMi コンソールにアクセスするツールも用意されています。

NNMi Northbound インタフェースは、インシデント ライフサイクルの状態変更通知、インシデント相関処理通知、およびインシデント削除通知を Northbound アプリケーションに送信できます。このように、Northbound アプリケーションは NNMi の因果関係分析の結果を複製することができます。

NNMi Northbound インタフェースは、NNMi が受信する SNMP トラップを Northbound アプリケーションに転送することもできます。NNMi Northbound インタフェースは、NNM 6.x または 7.x 管理ステーションによって生成されたイベントは Northbound アプリケーションに転送しません。

値

NNMi ノースバウンド インタフェースにより、サードパーティまたはカスタム イベント統合アプリケーションでイベント統合を実行することができます。NNMi Northbound インタフェースは、その他のアプリケーションと NNMi の統合に使用できる情報でイベントを強化します。

サポートされるバージョン

この章の情報は、NNMi バージョン 9.00 以降に適用されます。

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、『NNMi システムおよびデバイスのサポート マトリックス』を参照してください。

用語

この章では、以下の用語を使用します。

- ノ Northbound アプリケーション - SNMPv2c トラップを受信および処理できる任意のアプリケーション。
- トラップ受信コンポーネント - SNMP トラップを受信する、ノーズバウンド アプリケーションの一部分。
  - 一部のアプリケーションには、SNMP トラップを受信して処理用に別のコンポーネントに転送する、個別にインストール可能なコンポーネントが含まれます。
  - そのようなコンポーネントがない Northbound アプリケーションの場合、「トラップ受信コンポーネント」は「Northbound アプリケーション」と同義語です。
- NNMi Northbound インタフェース - NNMi インシデントを SNMPv2c トラップとして Northbound アプリケーションに転送する NNMi の機能。
- Northbound 転送先 - Northbound アプリケーションのトラップ受信コンポーネントへの接続を定義し、NNMi がその Northbound アプリケーションに送信するトラップのタイプを指定する NNMiNorthbound インタフェースの設定の 1 つ。

ドキュメント

この章では、NNMi インシデントを任意の Northbound アプリケーションに転送するように NNMi を設定する方法を説明します。特定の Northbound アプリケーションの詳細については、そのアプリケーションのマニュアルを参照してください。

NNMi ノースバウンド インタフェースの有効化

NNMi は、UDP を使用して SNMP トラップで送信される情報の量を制限しません。トラップ データのサイズが大きくて処理不能なネットワーク ハードウェアが伝送経路上にあったり、ネットワーク トラフィックの量が多かったりすると、トラップが失われることがあります。そのため、Northbound アプリケーションのトラップ受信コンポーネントを NNMi 管理サーバーにインストールすることをお勧めします。Northbound アプリケーションは、信頼性のある情報を転送する役割を担います。

NNMi ノースバウンド インタフェースを有効にするには、以下の手順を実行します。

1. 必要に応じて、NNMi トラップ定義を認識できるように Northbound アプリケーションを設定します。
2. NNMi 管理サーバーで、NNMi インシデント転送を設定します。
   a. NNMi コンソールで、**[HP NNMi-Northbound Interface デスティネーション**] フォーム (**[統合モジュールの設定] > [Northbound インタフェース]**) を開き、**[新規]** 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。)

   b. **[有効にする]** 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を入力可能にします。
   c. Northbound アプリケーションへの接続情報を入力します。

      これらのフィールドの詳細は、515 ページの「Northbound アプリケーションの接続パラメータ」を参照してください。

   d. 送信オプションおよび Northbound レアプリケーションに送信する内容に対するインシデント フィルタを指定します。

      これらのフィールドの詳細は、516 ページの「NNMi Northbound インタフェース統合の内容」を参照してください。

   e. 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。
3. *オプション。* Northbound アプリケーションから NNMi ビューにアクセスするための URL を作成し、NNMi とのコンテキスト インタラクションを作成します。

   詳細については、NNMi コンソールで、**[ヘルプ] > [NNMi ドキュメント ライブラリ] > [NNMi を別の場所で URL と統合]** をクリックしてください。

NNMi ノースバウンド インタフェースの使用法

NNMi Northbound インタフェースを有効にすると、Northbound 転送先によって NNMi が Northbound アプリケーションに送信する情報が決まります。Northbound アプリケーションを設定して、転送されるトラップがネットワーク環境に応じて表示および解釈されるようにします。NNMi が Northbound アプリケーションに送信するトラップの内容および形式の詳細については、`hp-nnmi-nbi.mib` ファイルを参照してください。

NNMi は、各管理イベント、SNMP トラップ、または通知トラップのコピーを 1 つだけ Northbound 転送先に送信します。NNMi はトラップをキューに入れません。NNMi がトラップを転送するときに Northbound アプリケーションのトラップ受信コンポーネントに接続できないと、そのトラップは失われます。

このセクションでは、統合で送信可能なトラップのタイプを説明します。コンテンツ設定の設定詳細については、516 ページの「NNMi Northbound インタフェース統合の内容」を参照してください。

インシデント転送

管理イベント

Northbound に管理イベントが含まれる場合、そのインシデントのライフサイクル状態が [登録済み] に変更されると、NNMi は各管理イベントを Northbound アプリケーションに転送します。

転送される管理イベントの OID は、NNMi コンソールの **[管理イベントの設定]** フォームに表示される SNMP オブジェクト ID です。NNMi は、OID が 1.3.6.1.4.1.11.2.17.19.2.0.9999 のすべてのカスタム管理イベントを転送します。

サードパーティ SNMP トラップ

Northbound 転送先にサードパーティの SNMP トラップが含まれる場合、関連インシデントのライフサイクル状態が [登録済み] に変更されると、NNMi は SNMPv1、v2c、または v3 形式の各受信ラップを Northbound アプリケーションに転送します。NNMi は、(MIB で定義される) 元のトラップ varbind の順序を維持し、メッセージ ペイロードに NNMi 固有の varbind を追加します。元のトラップに含まれていない定義済み varbind がある場合、NNMi は、その欠落している varbind の部分に NULL 値をパディングします。MIB が NNMi にロードされていない場合、NNMi はトラップを正しく再構成して NNMi インシデント データを追加できません。したがって、NNMi はこのトラップを転送しません。

サードパーティの SNMP トラップの場合は、以下の点に注意してください。

- NNMi は SNMP トラップ インシデントからのトラップを再構成するため、転送されるトラップの形式は、NNMi が受信した元のトラップの形式に関係なく、SNMPv2c となります。
- 転送される SNMP トラップは、NNMi 管理サーバーをトラップ ソースとして示します。元のトラップ ソースを判断するには、(n+21) 番目の varbind の値 IncidentNodeHostname (1.3.6.1.4.1.11.2.17.19.2.2.21) と、(n+24) 番目の varbind の値 IncidentNodeMgmtAddr (1.3.6.1.4.1.11.2.17.19.2.2.24) を調べてください。n は MIB でトラップに定義されている varbind の数です。

NNMi が管理するデバイスのいずれかが Northbound アプリケーションにトラップを送信する場合、Northbound アプリケーションで重複デバイス トラップを管理する必要があります。

トラップ転送メカニズムの比較については、93 ページの「トラップおよびインシデント転送」を参照してください。

インシデント ライフサイクル状態変化通知

解決済みに変化したトラップ

Northbound 転送先にエンハンスド解決済み通知が含まれる場合、NNMi のインシデントのライフサイクル状態が [解決済み] に変化したときに、NNMi は EventLifecycleStateClosed (1.3.6.1.4.1.11.2.17.19.2.0.1000) トラップを Northbound アプリケーションに転送します。EventLifecycleStateClosed トラップは、元のインシデントのデータの多くを含んでいます。前のライフサイクル状態の値は含んでいません。EventLifecycleStateClosed トラップは、6 番目の varbind である IncidentUuid (1.3.6.1.4.1.11.2.17.19.2.2.6) で元のインシデントを識別します。

状態変化トラップ

Northbound 転送先にライフサイクル状態変更通知が含まれる場合、NNMi のインシデントのライフサイクル状態が [進行中]、[完了]、または [解決済み] に変化したときに、NNMi は LifecycleStateChangeEvent (1.3.6.1.4.1.11.2.17.19.2.0.1001) トラップを Northbound アプリケーションに送信します。Northbound アプリケーションは、LifecycleStateChangeEvent と元のインシデントを関連付けできます。

LifecycleStateChangeEvent トラップは、以下の varbind で元のインシデントとライフサイクル状態の変化を識別します。

- IncidentUuid、6 番目の varbind (1.3.6.1.4.1.11.2.17.19.2.2.6)

  この値は、管理イベントの 6 番目の varbind の値、またはサードパーティ SNMP トラップ varbind の (n+6) 番目の varbind の値と一致します。

- IncidentLifecycleStatePreviousValue、7 番目の varbind (1.3.6.1.4.1.11.2.17.19.2.2.200)
- IncidentLifecycleStateCurrentValue、8 番目の varbind (1.3.6.1.4.1.11.2.17.19.2.2.201)

  以下の表は、ライフサイクル状態に使用できる整数値を示したものです。

名前	整数値
登録済み	1
進行中	2
完了	3
解決済み	4
抑止済み	5

インシデント相関処理通知

Northbound 転送先にインシデント相関処理通知が含まれる場合、NNMi の因果関係分析でインシデントが相関処理されると、NNMi はインシデント相関処理トラップを Northbound アプリケーションに送信します。Northbound アプリケーションはトラップ内の情報を使用して相関変更を複製することができます。

単一相関トラップ

単一相関トラップ オプションの場合、この統合では、以下の相関トラップを送信します。

- EventDedupCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1100)
- EventImpactCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1101)
- EventPairwiseCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1102)

- EventRateCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1103)
- EventApaCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1104)
- EventCustomCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1105)

各トラップは、以下の varbind において、1 つの親子インシデント相関関係を示します。

- IncidentCorrelationIndicatorParentUuid、6 番目の varbind (1.3.6.1.4.1.11.2.17.19.2.2.6)
- IncidentCorrelationIndicatorChildUuid、7 番目の varbind (1.3.6.1.4.1.11.2.17.19.2.2.300)

グループ相関トラップ

グループ相関トラップ オプションの場合、この統合では、以下の相関トラップを送信します。

- EventDedupCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2100)
- EventImpactCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2101)
- EventPairwiseCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2102)
- EventRateCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2103)
- EventApaCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2104)
- EventCustomCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2105)

各トラップは、以下の varbind でにおいて、親子インシデント相関関係を示します。

- IncidentCorrelationIndicatorParentUuid、6 番目の varbind (1.3.6.1.4.1.11.2.17.19.2.2.6)
- IncidentCorrelationIndicatorChildCount、7 番目の varbind (1.3.6.1.4.1.11.2.17.19.2.2.301)
- IncidentCorrelationIndicatorChildUuidCsv、8 番目の varbind (1.3.6.1.4.1.11.2.17.19.2.2.302)

  この値は子インシデント UUID のカンマ区切りリストです。

インシデント削除通知

Northbound 転送先にインシデント削除通知が含まれる場合、インシデントが NNMi で削除されると、NNMi は EventDeleted (1.3.6.1.4.1.11.2.17.19.2.0.3000) トラップを Northbound アプリケーションに送信します。EventDeleted トラップは、6 番目の varbind である IncidentUuid (1.3.6.1.4.1.11.2.17.19.2.2.6) で元のインシデントを識別します。

イベント転送フィルタ

Northbound 転送先にインシデント フィルタが含まれる場合、選択した設定オプションに応じて、フィルタのオブジェクト ID (OID) には、以下のイベント タイプが包含または除外されます。

- NNMi 管理イベント インシデント
- サードパーティ SNMP トラップ
- EventLifecycleStateClosed トラップ
- LifecycleStateChangeEvent トラップ
- EventDeleted トラップ

- 相関関係通知トラップ

  以下の注は、相関関係通知トラップに適用されます。

  — インシデント フィルタが相関処理に親インシデントを転送しない場合、NNMi は相関関係通知トラップを Northbound アプリケーションに送信しません。

  — インシデント フィルタが相関処理に子インシデントを転送しない場合、転送される相関関係通知トラップにその子インシデントの UUID は含まれません。(相関関係通知トラップに子インシデント UUID が含まれない場合、NNMi はそのトラップを Northbound アプリケーションに送信しません。)

  — DuplicateCorrelation 管理イベントは、EventDedupCorrelation または EventDedupCorrelationGroup 相関関係通知トラップとは無関係に転送されます。同様に、RateCorrelation 管理イベントは EventRateCorrelation または EventRateCorrelationGroup 相関関係通知トラップとは無関係に転送されます。インシデント フィルタがこれらの相関関係通知トラップのいずれかを転送しない場合でも、NNMi により関連管理イベントが転送される場合があります。

NNMi ノースバウンド インタフェースの変更

NNMi ノースバウンド インタフェースの設定パラメータを変更するには、以下の手順を実行します。

1. NNMi コンソールで、**[HP NNMi-Northbound Interface デスティネーション**] フォーム (**[統合モジュールの設定] > [Northbound インタフェース]**) を開きます。
2. 転送先を選択し、**[編集]** をクリックします。
3. 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は、515 ページの「[NNMi Northbound Interface デスティネーション] フォームのリファレンス」を参照してください。
4. フォームの上端の **[有効にする]** チェック ボックスがオンであることを確認し、フォームの下端の **[送信]** をクリックします。

   変更はただちに有効になります。

NNMi ノースバウンド インタフェースの無効化

Northbound 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。

Northbound アプリケーションへの NNMi の転送を中止するには、以下の手順を実行します。

1. NNMi コンソールで、**[HP NNMi-Northbound Interface デスティネーション**] フォーム (**[統合モジュールの設定] > [Northbound インタフェース]**) を開きます。
2. 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。

3 フォームの上端の **[有効にする]** チェック ボックスをオフにし、フォームの下端の **[送信]** をクリックします。

変更はただちに有効になります。

NNMi ノースバウンド インタフェースのトラブルシューティング

NNMi ノースバウンド インタフェースが正常に機能しない場合は、以下の手順を実行して問題を解決してください。

1 トラップ転送先ポートがファイアウォールによってブロックされていないことを確認します。

NNMi 管理サーバーが、ホストとポートによって Northbound アプリケーションを直接処理できることを確認します。

2 統合が正常に実行されていることを確認します。

a NNMi コンソールで、**[HP NNMi-Northbound Interface デスティネーション]** フォーム (**[統合モジュールの設定] > [Northbound インタフェース]**) を開きます。

b 転送先を選択し、**[編集]** をクリックします。

c **[有効にする]** オプションが選択されていることを確認します。

3 Northbound 転送先に管理イベントが含まれる場合は、この機能を確認します。

a NNMi コンソールの **[解決済みの重要なインシデント]** ビューで、任意のインシデントを開きます。

b インシデント ライフサイクル状態を **[登録済み]** に設定して、 **[保存]** をクリックします。

c インシデント ライフサイクル状態を **[解決済み]** に設定して、 **[保存して閉じる]** をクリックします。

d 30 秒後、Northbound アプリケーションがこのインシデントの EventLifecycleStateClosed トラップ (または LifecyleStateChangeEvent トラップ) を受信したかどうかを確認します。

— Northbound アプリケーションがトラップを受信した場合は、手順 4 を続行します。

— Northbound アプリケーションがトラップを受信しなかった場合は、異なる Northbound アプリケーションに接続する新規 Northbound 転送先を設定してから、手順 a からこのテストを繰り返します。

再テストに合格した場合、問題は最初の Northbound アプリケーションにあります。アプリケーションのドキュメントでトラブルシューティング情報を参照してください。

再テストに不合格になった場合は、HP サポートにご連絡ください。

4 Northbound 転送先に SNMP トラップが含まれる場合は、この機能を確認します。

a 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、NNMi トポロジ内のノードに対する SNMP トラップを生成します。

```
nnmsnmpnotify.ovpl -u username -p password -a ¥
discovered_node NNMi_node linkDown
```

discovered_node は NNMi トポロジのノードのホスト名または IP アドレス、*NNMi_node* は NNMi 管理サーバーのホスト名または IP アドレスです。

b 30 秒後に、Northbound アプリケーションが転送されたトラップを受信したがどうかを確認します。

— Northbound アプリケーションがトラップを受信した場合、NNMi Northbound インタフェースは正常に機能しています。

— Northbound アプリケーションがトラップを受信しなかった場合は、異なる Northbound アプリケーションに接続する新規 Northbound 転送先を設定してから、手順 a からこのテストを繰り返します。

再テストに合格した場合、問題は最初の Northbound アプリケーションにあります。アプリケーションのドキュメントでトラブルシューティング情報を参照してください。

再テストに不合格になった場合は、HP サポートにご連絡ください。

アプリケーション フェールオーバーと NNMi ノースバウンド インタフェース

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関係することになる場合、ここでの情報は、Northbound レシーバにトラップを送信する NNMi Northbound アプリケーションを実装するすべての統合に適用されます。

NNMi が Northbound アプリケーションに送信するトラップには、NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2) の NNMi URL が含まれます。アプリケーション フェイルオーバー前に受信したトラップは、現在のスタンバイ NNMi 管理サーバーを参照します。URL がスタンドバイ NNMi 管理サーバーを指す場合、その URL 値を使用するすべてのアクション (たとえば、NNMi コンソールの起動) は失敗します。

ローカル Northbound アプリケーション

Northbound アプリケーションのトラップ受信コンポーネントが NNMi 管理サーバー上にある場合は、以下の考慮事項が NNMi Northbound インタフェースの設定に適用されます。

- Northbound アプリケーションのトラップ受信コンポーネントは、アクティブおよびスタンバイ NNMi 管理サーバー に同じようにインストールおよび設定する必要があります。両方の NNMi 管理サーバーの同じポートで SNMP トラップ受信を設定します。
- プライマリ NNMi 管理サーバーでのみ、NNMi ノースバウンド インタフェースを設定します。

  [HP NNMi-Northbound Interface デスティネーション] フォームの **[ホスト]** 識別で、**[NNMi FQDN]** または **[ループバックを使用]** オプションを選択します。

NNMi ノースバウンド インタフェースは、起動時に、現在の NNMi 管理サーバーの正しい名前または IP アドレスを判断します。このように、Northbound インタフェースは、トラップをアクティブな NNMi 管理サーバー上の Northbound アプリケーションのトラップ受信コンポーネントに送信します。

リモート Northbound アプリケーション

Northbound アプリケーションのトラップ受信コンポーネントが NNMi 管理サーバー上にない場合は、NNMi Northbound インタフェースをプライマリ NNMi 管理サーバーにのみ設定します。**[HP NNMi-Northbound Interface デスティネーション]** フォームの **[ホスト]** 識別で、**[その他]** オプションを選択します。

[NNMi Northbound Interface デスティネーション] フォームのリファレンス

[HP NNMi-Northbound Interface デスティネーション] フォームには、NNMi と Northbound アプリケーション間の通信設定パラメータがあります。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。(**[HP NNMi-Northbound Interface デスティネーション]** フォームで、**[新規]** をクリックするか、または転送先を選択して、**[編集]** をクリックします)。

Administrator ロールの NNMi ユーザーのみが **[HP NNMi-Northbound Interface デスティネーション]** フォームにアクセスできます。

[HP NNMi-Northbound Northbound Interface デスティネーション] フォームには、以下の領域の情報が表示されます。

- 515 ページの「Northbound アプリケーションの接続パラメータ」
- 516 ページの「NNMi Northbound インタフェース統合の内容」
- 518 ページの「NNMi Northbound インタフェース転送先のステータス情報」

統合設定に変更を適用するには、**[HP NNMi-Northbound Interface デスティネーション]** フォームの値を更新し、**[送信]** をクリックします。

Northbound アプリケーションの接続パラメータ

表 55 は、Northbound アプリケーションへの接続設定用パラメータを示したものです。

表 55　Northbound アプリケーションの接続情報

フィールド	説明
ホスト	Northbound アプリケーションのトラップ受信コンポーネントが実行されるサーバーの完全修飾ドメイン名 (推奨) または IP アドレス。 統合では、以下のサーバーの識別方法がサポートされています。 • **NNMi FQDN** NNMi が NNMi 管理サーバー上の Northbound アプリケーションへの接続を管理し、**[ホスト]** フィールドが読み取り専用になります。 これが、NNMi 管理サーバー上での Northbound アプリケーションの推奨設定です。 • **ユーザー ループバック** NNMi が NNMi 管理サーバー上の Northbound アプリケーションへの接続を管理し、**[ホスト]** フィールドが読み取り専用になります。 • **その他** Northbound アプリケーション サーバーを識別するホスト名または IP アドレスを、**[ホスト]** フィールドに入力します。 NNMi は、**[ホスト]** フィールドのホスト名または IP アドレスがループバック アダプタとして設定されていないことを確認します。 これがデフォルト設定です。 **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にアプリケーション フェイルオーバーが統合に与える影響については、513 ページの「アプリケーション フェールオーバーと NNMi ノースバウンド インタフェース」を参照してください。

表 55　**Northbound アプリケーションの接続情報 (続く)**

フィールド	説明
ポート	Northbound アプリケーションが SNMP トラップを受信する UDP ポート。 Northbound アプリケーション固有のポート番号を入力します。 **注 :** Northbound アプリケーションのトラップ受信コンポーネントが NNMi 管理サーバー上にある場合は、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]** フィールドに設定した、NNMi が SNMP トラップを受信する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 Northbound アプリケーションの読み取り専用コミュニティ文字列。 Northbound アプリケーション設定で、受信した SNMP トラップにコミュニティ文字列が必要な場合は、その値を入力します。 Northbound アプリケーション設定で、特定のコミュニティ文字列が不要な場合は、デフォルト値の `public` を使用します。

NNMi Northbound インタフェース統合の内容

表 56 は、NNMi Northbound インタフェースが Northbound アプリケーションに送信する内容を設定するためのパラメータを示したものです。

表 56　**NNMi ノースバウンド インタフェースの内容設定情報**

フィールド	説明
インシデント	インシデント転送の指定。 • **管理** NNMi は、NNMi が生成した管理イベントのみを Northbound アプリケーションに転送します。 • **サードパーティ SNMP トラップ** NNMi は、NNMi が管理対象デバイスから受信する SNMP トラップのみを Northbound アプリケーションに転送します。 • **両方** NNMi は、NNMi が生成する管理イベントと NNMi が管理対象デバイスから受信する SNMP トラップの両方を Northbound アプリケーションに転送します。 これがデフォルト設定です。 NNMi は、Northbound 転送先を有効にすると直ちにインシデントの転送を開始します。 詳細については、508 ページの「インシデント転送」を参照してください。

表 56　NNMi ノースバウンド インタフェースの内容設定情報 (続く)

フィールド	説明
ライフサイクル状態の変化	インシデント変更通知の仕様。 • **エンハンスド解決済み** 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 Northbound アプリケーションに送信します。 これがデフォルト設定です。 • **状態変化** 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 Northbound アプリケーションに送信します。 • **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 Northbound アプリケーションに送信します。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、インシデントのライフサイクル状態変化トラップを Northbound アプリケーションに送信します。 **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。 詳細については、509 ページの「インシデント ライフサイクル状態変化通知」を参照してください。
相関処理	インシデント相関処理通知の仕様。 • **なし** NNMi は、NNMi 因果関係分析によるインシデント相関処理結果を Northbound アプリケーションに通知しません。 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相関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相関処理ごとに、トラップを 1 つ送信します。 詳細については、509 ページの「インシデント相関処理通知」を参照してください。
削除	インシデント削除の仕様。 • **送信しない** NNMi は、インシデントが NNMi で削除されても Northbound アプリケーションに通知しません。 これがデフォルト設定です。 • **送信** NNMi は、NNMi で削除されるインシデントごとに、削除トラップを Northbound アプリケーションに送信します。 詳細については、510 ページの「インシデント削除通知」を参照してください。

表 56　NNMi ノースバウンド インタフェースの内容設定情報 (続く)

フィールド	説明
NNMi コンソール アクセス	Northbound アプリケーションから NNMi コンソールを参照する URL の接続プロトコル仕様。NNMi が Northbound アプリケーション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。 設定ページのデフォルトは、NNMi 設定と一致する設定になります。 NNMi コンソールが HTTP と HTTPS 両方の接続を承認するよう設定されている場合、NNMi URL で HTTP 接続プロトコルの指定を変更できます。 たとえば、Northbound アプリケーションのすべてのユーザーがイントラネット上にある場合は、Northbound アプリケーションから NNMi コンソールへのアクセスを HTTP 経由に設定できます。Northbound アプリケーションから NNMi コンソールに接続するプロトコルを変更する場合は、必要に応じて、**[HTTP]** オプションまたは **[HTTPS]** オプションを選択します。
Incident Filter(インシデント フィルタ)	Northbound アプリケーションに送信されたイベントを統合でフィルタするときのオブジェクト ID (OID) のリスト。各フィルタ 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。 以下のオプションの 1 つを選択します。 • **なし** NNMi はすべてのイベントを Northbound アプリケーションに送信します。 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。 インシデント フィルタを指定します。 • フィルタ 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 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。 詳細については、510 ページの「イベント転送フィルタ」を参照してください。

NNMi Northbound インタフェース転送先のステータス情報

表 57 に、ノースバウンド転送先の読み取り専用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。

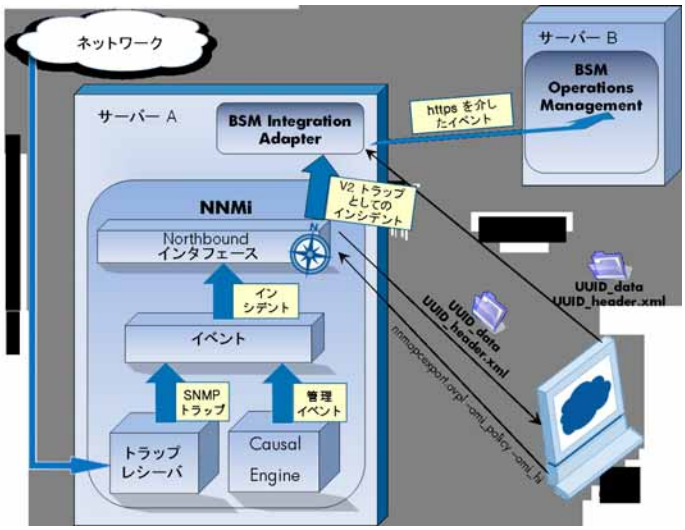
表 57　NNMi Northbound インタフェース転送先のステータス情報

フィールド	説明
トラップ転送先 IP アドレス	転送先ホスト名の解決先となる IP アドレス。 この値は、このノースバウンド転送先に固有です。

表 57　NNMi Northbound インタフェース転送先のステータス情報 (続く)

フィールド	説明
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 Northbound アプリケーション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。 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 Northbound アプリケーション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。 この値は、このノースバウンド転送先に固有です。

HP BSM Operations Management



HP Business Service Management (BSM) 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。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 営業担当者にご相談ください。

この章には、以下のトピックがあります。

- 521 ページの「HP NNMi-HP BSM Operations Management 統合」
- 523 ページの「HP NNMi-HP BSM Operations Management 統合の有効化」
- 526 ページの「HP NNMi-HP BSM Operations Management 統合の使用」
- 528 ページの「HP NNMi-HP BSM Operations Management 統合の変更」
- 530 ページの「HP NNMi-HP BSM Operations Management 統合の無効化」
- 530 ページの「HP NNMi-HP BSM Operations Management 統合のトラブルシューティング」
- 534 ページの「[HP 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)」

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 HP BSM Integration Adapter に転送します。BSM Integration Adapter は、NNMi トラップをフィルタし、それを BSM Operations Management イベント ブラウザに転送します。

HP NNMi-HP BSM Operations Management 統合では、NNMi が受信する SNMP トラップを転送することもできます。この統合では、NNM 6.x または 7.x 管理ステーションで生成されたイベントはアダプタに転送しません。

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統合について説明します。直接統合する代わりに、NNMi と HP Operations Manager (HPOM) を統合し、イベントを BSM Operations Management イベント ブラウザに転送することもできます。

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 505 ページの「NNMi ノースバウンド インタフェース」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 Integration Adapter 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 システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10 (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 Integration Adapter にはライセンスが必要であり、NNMi をインストールした*後*に NNMi 管理サーバー コンピュータ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 Integration Adapter 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。

- *HP BSM Integration Adapter Installation and Configuration Guide*
- *HP BSM Integration Adapter User Guide*
- HP BSM Integration Adapter ヘルプ
- *HP 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 Integration Adapter ユーザーが実行することを推奨します。

NNMi を HP Business Service Management (BSM) トポロジと統合すると、HP NNMi-HP BSM Operations Management 統合では、NNMi 管理デバイスに関係するインシデントを BSM 設定項目 (CI) と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、526 ページの「設定項目の ID」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。

      ```
      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 Integration Adapter 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 Integration Adapter 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 UNIX 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、526 ページの「HP NNMi-HP BSM Operations Management 統合の使用」を参照してください。

2 NNMi 管理サーバーで、BSM Integration Adapter を設定します。

a 『*HP BSM Integration Adapter Installation and Configuration Guide*』の説明に従って、BSM Integration Adapter をインストールおよび設定します。

HPOM の HP Operations Agent と BSM Integration Adapter を 1 つのシステムで同時に実行することはできません。 必要に応じて、BSM Integration Adapter をインストールする前に、HP Operations Agent をアンインストールしてください。

b BSM Integration Adapter ユーザー インタ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、HP BSM Integration Adapter ヘルプの「*Managing policies*」>「*Import policies*」を参照してください。

c BSM Integration Adapter 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、HP BSM Integration Adapter ヘルプの「*Managing policies*」>「*Activate and deactivate policies*」を参照してください。

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

BSM Integration Adapter 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 Integration Adapter 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、`ia-config.bat` (Windows) コマンドまたは `ia-config.sh` (Linux) コマンドで BSM Integration Adapter を設定するときに指定した Apache Tomcat サーバーの HTTP ポートと異なります。

BSM Integration Adapter 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 コンソールで、**[設定]** ワークスペースで **[通信の設定]** フォームを開きます。

b **[SNMP のデフォルト設定]** 領域で、**[SNMP ポート]** の値を確認します。

c **[通信の設定]** フォームの **[SNMP ポート]** の値とは異なるポートを選択します。ポート番号は 162 を含む番号を使用することをお勧めします。これは SNMP トラップを受信する標準的な UDP ポートです。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。

d NNMi 管理サーバーで、コマンド **netstat -a** を実行し、その出力から手順 c 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、おそらく BSM Integration Adapter で使用可能になっています。

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 Integration Adapter 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 Integration Adapter に転送する NNMi インシデントを設定します。

a NNMi コンソールで、**[HP 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 **[HP 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 Integration Adapter 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は、534 ページの「BSM Integration Adapter の接続」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は、535 ページの「BSM Operations Management 統合コンテンツ」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 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、『HP BSM Operations Management 拡張性ガイド』を参照してください。

HP NNMi-HP BSM Operations Management 統合の使用

HP NNMi-HP BSM Operations Management 統合では、NNMi 管理イベントと SNMP トラップが BSM Operations Management イベント ブラウザに向けて一方向に送信されます。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 Integration Adapter 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 ブラウザに表示します。BSM Operations Management イベント ブラウザのメニュー 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 ブラウザでは、送信元のトラップ ソースが、**[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 (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 UCMDB と統合すると、NNMi は、NNMi が管理するデバイスの BSM または 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 管理デバイスに関するインシデントを BSM または UCMDB の CI と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 UCMDB との統合の詳細については、以下を参照してください。

- 423 ページの「HP Business Service Management トポロジ」
- 433 ページの「HP Universal CMDB」

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 ブラウザに表示されます。
  - これらのトラップには、526 ページの「設定項目の ID」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、527 ページの「ヘルス インジケータ」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、526 ページの「設定項目の ID」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 トラップを重複して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相関させるようにポリシーを設定できます。
- EventLifecycleStateClosed トラップ
  - BSM Integration Adapter 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 Integration Adapter 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受諾します。

- 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 Integration Adaper 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 Integration Adaper 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 Integration Adapter 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 Integration Adapter 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 Integration Adapter 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、HP BSM Integration Adapter ヘルプの「*Developing SNMP interceptor policies*」>「*Configure SNMP rules*」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 Integration Adapter に送信するトラップ タイプの説明については、508 ページの「NNMi ノースバウンド インタフェースの使用法」を参照してください。
- NNMi が BSM Integration Adapter 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、『HP BSM Operations Management 拡張性ガイド』を参照してください。

HP NNMi-HP BSM Operations Management 統合の変更

この項では以下の内容について説明します。

- 529 ページの「新規 NNMi トラップの SNMP トラップ ポリシー条件の更新」
- 529 ページの「設定パラメータの変更」

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* リファレンス ページ、または UNIX マンページを参照してください。

2 BSM Integration Adapter 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。この方法を適用する場合は、BSM Integration Adapter 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 Integration Adapter 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 ブラウザに表示されるメッセージを複製します。

設定パラメータの変更

統合設定パラメータを変更するには、以下の手順を実行します。

1 NNMi コンソールで、[**HP 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は、534 ページの「[HP 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)」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 Integration Adapter 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、**[HP 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。

オプションとして、HP BSM Integration Adapter ヘルプの説明に従い、SNMP トラップ ポリシーを非アクティブにするか、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

この項では以下の内容について説明します。

- 530 ページの「BSM Operations Management イベント ブラウザに転送されたインシデントが表示されない」
- 533 ページの「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 ブラウザに転送されたインシデントが表示されない

以下の手順において、`OVBIN` 環境変数は、BSM Integration Adapter 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*: `<drive>¥Program Files¥HP¥HP BTO Software¥bin`
- *Linux*: `/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*:

  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*、**[HP 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、525 ページの手順 4 を繰り返します。
- *<custom_port>* の値が 162 であるか、**[HP 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、必要に応じて 524 ページの手順 3 から 525 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%¥opcagt -status

- *Linux* NNMi 管理サーバー :

  $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 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*: **netstat -an | findstr <*custom_port*>**

— *Linux*: **netstat -an | grep <*custom_port*>**

このとき、*<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。

ovc -restart opctrapi

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 Integration Adapter に配布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、523 ページの手順 1 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 Integration Adapter がトラップを受信していることを確認します。

a BSM Integration Adapter が BSM Operations Management イベント ブラウザにイベントを送信できることを確認します。

b BSM Integration Adapter のトレースを有効にして、トラップが BSM Integration Adapter に到着するかどうか判定します。

7 NNMi が BSM Integration Adapter 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、512 ページの「NNMi ノースバウンド インタフェースのトラブルシューティング」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。

   BSM サーバーがシャット ダウンすると、BSM Integration Adapter は受信したトラップをキューイングします。BSM Integration Adapter 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 Integration Adapter 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。

[HP 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)

[HP NNMi-HPOM Agent デスティネーション] フォームには、NNMi と BSM Integration Adapter の間の通信を設定するためのパラメータが含まれています。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。(**[HP 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。)

[HP 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。

[HP 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。

- 534 ページの「BSM Integration Adapter の接続」
- 535 ページの「BSM Operations Management 統合コンテンツ」
- 537 ページの「BSM Integration Adapter 転送先のステータス情報」

統合設定への変更を適用するには、**[HP 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 Integration Adapter の接続

表 58 に、BSM Integration Adapter への接続を設定するパラメータをリストします。

表 58　BSM Integration Adapter 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 Integration Adapter が NNMi からの SNMP トラップを受信するシステムです。 この統合では、BSM Integration Adapter ホストを特定する手段として、以下の方法がサポートされています。 • **NNMi FQDN** NNMi は NNMi 管理サーバー上の BSM Integration Adapter. への接続を管理し、**[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。 • **ユーザー ループバック** 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。 **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、統合モジュールでのアプリケーション フェイルオーバーの影響について、513 ページの「アプリケーション フェールオーバーと NNMi ノースバウンド インタフェース」を参照してください。

表 58　**BSM Integration Adapter の接続情報（続く）**

フィールド	説明
ポート	BSM Integration Adapter が SNMP トラップを受信する UDP ポート。 BSM Integration Adapter に固有のポート番号を入力します。この値は、524 ページの手順 3 で定義したポートです。 ポートを決定するには、NNMi 管理サーバー上で **`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。 **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 Integration Adapter の読み取り専用コミュニティ文字列。 HP NNMi-HP BSM Operations Management 統合の場合は、デフォルト値の `public` を使用します。

BSM Operations Management 統合コンテンツ

表 59 に、NNMi が BSM Integration Adapter に送信するコンテンツを設定する場合に指定するパラメータをリストします。

表 59　**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指定。 • **管理** NNMi は、NNMi が生成した管理イベントのみを BSM Integration Adapter 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 Integration Adapter に転送します。 • **両方** 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 Integration Adapter に転送します。 これがデフォルト設定です。 NNMi は、転送先が有効になるとすぐにインシデントの転送を開始します。 詳細については、508 ページの「インシデント転送」を参照してください。

表 59　BSM Operations Management 統合コンテンツ設定情報（続く）

フィールド	説明
ライフサイクル状態の変化	インシデント変更通知の仕様。 • **エンハンスド解決済み** 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 Integration Adapter に送信します。 これがデフォルト設定です。 • **状態変化** 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 Integration Adapter 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 Integration Adapter 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、インシデントのライフサイクル状態変化トラップを BSM Integration Adapter 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。 詳細については、509 ページの「インシデント ライフサイクル状態変化通知」を参照してください。
相関処理	インシデント相関処理通知の仕様。 • **なし** NNMi は、NNMi 因果関係分析によって判明したインシデント相関処理について BSM Integration Adapter 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相関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相関処理ごとに、トラップを 1 つ送信します。 詳細については、509 ページの「インシデント相関処理通知」を参照してください。
削除	インシデント削除の仕様。 • **送信しない** NNMi は、NNMi でインシデントが削除されても、BSM Integration Adapter に通知しません。 これがデフォルト設定です。 • **送信** NNMi は、NNMi で削除されるインシデントごとに、削除トラップを BSM Integration Adapter に送信します。 詳細については、510 ページの「インシデント削除通知」を参照してください。
NNMi コンソール アクセス	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ための、URL 内での接続プロトコルの指定。NNMi が BSM Integration Adapter 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。 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。

表 59　BSM Operations Management 統合コンテンツ設定情報（続く）

フィールド	説明
Incident Filter(インシデント フィルタ)	BSM Integration Adapter に送信されたイベントを統合でフィルタするときのオブジェクト ID (OID) のリスト。 各フィルタ 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。 以下のオプションの 1 つを選択します。 • **なし** NNMi はすべてのイベントを BSM Integration Adapter 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。 インシデント フィルタを指定します。 • フィルタ 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 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。 詳細については、510 ページの「イベント転送フィルタ」を参照してください。

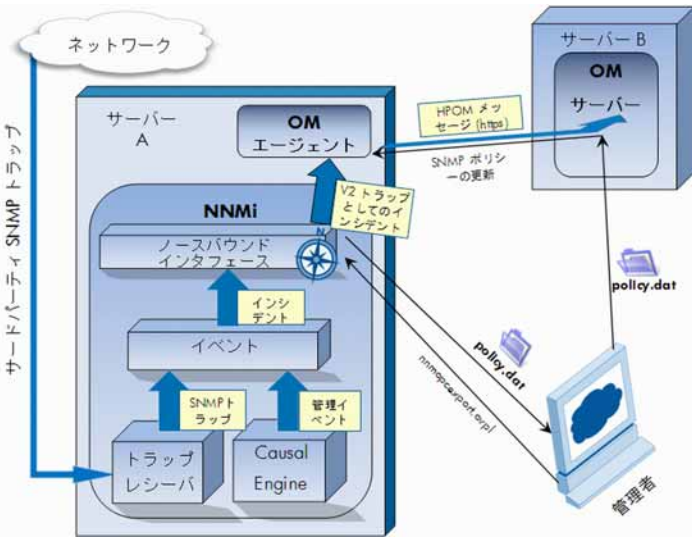
BSM Integration Adapter 転送先のステータス情報

表 60 に、BSM Integration Adapter の読み取り専用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 60　BSM Integration Adapter 転送先のステータス情報

フィールド	説明
トラップ転送先 IP アドレス	BSM Integration Adapter の転送先ホスト名の解決先となる IP アドレス。 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 Integration Adapter 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、この値が含まれています。 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 Integration Adapter 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。 この値は、このノースバウンド転送先に固有です。

HP Operations Manager



HPOM (HP Operations Manager) 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用の自動アラート、レポート、およびグラフが備わっています。HPOM 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。

HPOM の購入については、HP 販売員にお尋ねください。

この章では、以下の使用可能な統合について説明します。

- HP NNMi-HPOM 統合 (エージェント実装)
- HP NNMi-HPOM 統合 (Web サービス実装)

HP NNMi-HPOM 統合 (エージェント実装)

HP NNMi-HPOM 統合のエージェント実装は、HPOM と NNMi との統合に適したソリューションです。

HP NNMi-HPOM 統合のエージェントと Web サービスの両方の実装から、同じ HPOM 管理サーバーにメッセージが転送されると、HPOM アクティブ メッセージ ブラウザに、両方の実装からのメッセージがすべては表示されない可能性があります。そのため、HP では、同時に同じ HPOM 管理サーバーに対し、ある NNMi 管理サーバーから HP NNMi-HPOM 統合の両方の実装を実行することはサポートされていません。

この項では以下の内容について説明します。

- 540 ページの「HP NNMi-HPOM 統合について (エージェント実装)」
- 541 ページの「HP NNMi-HPOM 統合の有効化 (エージェント実装)」
- 546 ページの「HP NNMi-HPOM 統合の使用法 (エージェント実装)」
- 548 ページの「HP NNMi-HPOM 統合設定の変更 (エージェント実装)」
- 549 ページの「HP NNMi-HPOM 統合の無効化 (エージェント実装)」

- 550 ページの「HP NNMi-HPOM 統合のトラブルシューティング (エージェント実装)」
- 553 ページの「[HP NNMi-HPOM Agent デスティネーション] フォーム リファレンス (エージェント実装)」

HP NNMi-HPOM 統合について (エージェント実装)

HP NNMi-HPOM 統合のエージェント実装では、NNMi 管理イベントが NNMi 管理サーバーの HP Operations エージェントに SNMPv2c トラップとして転送されます。エージェントは NNMi トラップをフィルタし、それを HPOM アクティブ メッセージ ブラウザに転送します。エージェントの設定により、転送されたインシデントを受信する HPOM 管理サーバーが決まります。

HP NNMi-HPOM 統合で、NNMi が受信する SNMP トラップをエージェントに転送することもできます。この統合では、NNM 6.x または 7.x 管理ステーションによって生成されるイベントがエージェントに転送されません。

HP NNMi-HPOM 統合により、HPOM 内から NNMi コンソールへのアクセスすることもできます。

HP NNMi-HPOM 統合のエージェント実装は、NNMi Northbound インタフェース特有の実装です。これについては、505 ページの「NNMi ノースバウンド インタフェース」を参照してください。

HP NNMi-HPOM 統合のエージェント実装は、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-HPOM 統合には、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ドメイン用の HPOM アクティブ メッセージ ブラウザ内にイベント統合体が用意されているため、HPOM 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 HP Operations エージェントへの自動インシデント転送。転送されたインシデントは HPOM アクティブ メッセージ ブラウザに表示されます。
- HPOM から NNMi コンソールへのアクセス。
  - HPOM ユーザーは、選択したメッセージのコンテキストで NNMi **[インシデント]** フォームを開くことができます。
  - HPOM ユーザーは、選択したメッセージとノードのコンテキストで、NNMi ビュー (たとえば、Layer 2 Neighbor ビュー) を起動できます。
  - HPOM ユーザーは、選択したメッセージと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) を起動できます。

統合製品

このセクションの情報は、以下の製品に当てはまります。

- Windows 用 HPOM (OMW とも呼ばれる)
- UNIX 用 HPOM (OMU とも呼ばれる)
- Linux 用 HPOM (OML とも呼ばれる)

サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10

NNMi と HPOM は異なるコンピュータにインストールしてください。NNMi 管理サーバーと HPOM 管理サーバーのコンピュータのオペレーティング システムは、同じでも、異なっていても構いません。

HP Operations エージェントにはライセンスが必要で、NNMi をインストールした*後*で NNMi 管理サーバー コンピュータ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、HPOM 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。

HPOM ドキュメントでは、HPOM アクティブ メッセージ ブラウザから NNMi コンソールにアクセスする HPOM 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ています。

- Windows 用 HPOM の詳細は、HPOM ヘルプの HP NNMi アダプタ情報を参照してください。
- UNIX 用 HPOM バージョン 9.xx については、『HP Operations Manager for UNIX システム管理リファレンス ガイド』の「*Integrating NNMi into HPOM (NNMi と HPOM の統合)*」セクションを参照してください。
- UNIX 用 HPOM バージョン 8.3x については『HP NNMi-HPOM Integration for HP Operations Manager User’s Guide (HP 操作マネージャ用 HP NNMi-HPOM 統合ユーザー ガイド)』を参照してください。
- Linux 用 HPOM については、『HP Operations Manager for Linux システム管理リファレンス ガイド』の「*Integrating NNMi into HPOM (NNMi と HPOM の統合)*」セクションを参照してください。

HP NNMi-HPOM 統合の有効化 (エージェント実装)

HP NNMi-HPOM 統合のエージェント実装を有効化する手順の実行は、経験豊富な HPOM 管理者が行うことを推奨します。

NNMi と HP Business Service Management (BSM) トポロジ データベースを統合すると、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 BSM 設定項目 (CI) と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、546 ページの「設定項目の ID」を参照してください。

HP NNMi-HPOM 統合のエージェント実装を有効にするには、以下の手順を実行します。

1 NNMi 管理サーバーで、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。

```
nnmopcexport.ovpl -u <username> -p <password> ¥
-template "NNMi Management Events" -application "NNMi" ¥
-file NNMi_policy.dat
```

<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。

HP OMi イベント ブラウザか BSM Operations Management イベント ブラウザに HPOM で NNMi インシデントを転送する場合も、`-omi_hi` オプションを使用し、管理イベント ポリシー条件にヘルス インジケータを追加します。詳細については、546 ページの「ヘルス インジケータ」を参照してください。

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 UNIX 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、546 ページの「HP NNMi-HPOM 統合の使用法 (エージェント実装)」を参照してください。

2 HPOM 管理サーバーで、NNMi からのメッセージを受信するように HPOM を設定します。

a HPOM コンソールで、NNMi 管理サーバーのノードを追加します。

b NNMi 管理サーバーに HP Operations エージェントをインストールします。

c この手順の手順 1 で作成した `NNMi_policy.dat` ファイルを、NNMi 管理サーバーから HPOM 管理サーバーに転送します。

d `NNMi_policy.dat` ファイルを HPOM にインポートします。

— *Windows 用 HPOM*: `ImportPolicies` コマンドを使用します。

— *UNIX 用 HPOM* バージョン 9.x: `opcpolicy` コマンドを使用します。

— *UNIX 用 HPOM* バージョン 8.x: `opctempl` コマンドを使用します。

— *Linux 用 HPOM*: `opcpolicy` コマンドを使用します。

e `NNMi Management Events` ポリシーを NNMi 管理対象ノードに配布します。

f HPOM コンソールで、転送されるすべての NNMi インシデントを取り込む外部ノードを追加します。

初期テストのため、ノード フィルタを <*>.<*>.<*>.<*> (IP フィルタ用) または <*> (名前フィルタ用) に設定します。統合を検証した後、ご使用のネットワークに合わせて外部ノード フィルタを制限します。

NNMi インシデント ソース ノード用の HPOM 管理対象ノードを設定しないと、HPOM 管理サーバーは、そのノードに関する全インシデントを破棄します。

詳細については、以下を参照してください。

- *Windows 用 HPOM*:
  - HPOM ヘルプの「*UNIX 用 OVO テンプレートのインポート*」
  - HPOM ヘルプの「*外部ノードの設定*」
- *UNIX 用 HPOM*:
  - 『HP Operations Manager for UNIX HTTPS エージェント コンセプトと設定ガイド』
  - 『HP Operations Manager for UNIX コンセプト ガイド』
  - 『HP Operations Manager for UNIX システム管理リファレンス ガイド』
  - 『HP Operations Manager for UNIX Developer’s Toolkit Developer’s Reference』
  - *opcnode(1M)*、*opcbbcdist(1M)*、*opcragt(1M)*、*opccfgupl(1M)*、*opcpolicy(1M)* (バージョン 9.xx)、および *opctempl(1M)* (バージョン 8.3x) マンページ
- *Linux 用 HPOM*:
  - 『HP Operations Manager for Linux HTTPS エージェント コンセプトと設定ガイド』
  - 『HP Operations Manager for Linux コンセプト ガイド』
  - 『HP Operations Manager for Linux システム管理リファレンス ガイド』
  - 『HP Operations Manager for Linux Developer’s Toolkit Developer’s Reference』
  - *opcnode(1M)*、*opcbbcdist(1M)*、*opcragt(1M)*、*opccfgupl(1M)*、および *opcpolicy(1M)* マンページ

3 NNMi と HP Operations エージェントとの間の SNMP 通信に使用可能なポートを指定します。

HP Operations エージェントは、このポートで、NNMi がこのポートに転送する SNMP トラップを待機します。 統合を有効化している間、この手順の手順 4 (HP Operations エージェント用) と手順 5 (NNMi 用) の両方でこのポート番号が使用されます。

HP Operations エージェントが NNMi 管理サーバーにインストールされているため、このポート番号は NNMi が SNMP トラップを受信するポートとは違うものにしてください。

a NNMi コンソールで、**[設定]** ワークスペースで **[通信の設定]** フォームを開きます。

b **[SNMP のデフォルト設定]** 領域で、**[SNMP ポート]** の値を確認します。

c **[通信の設定]** フォームにある値とは異なるポートを選択します。 ポート番号は 162 を含む番号を使用することをお勧めします。これは SNMP トラップを受信する標準的な UDP ポートです。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。

d NNMi 管理サーバーで、コマンド **`netstat -a`** を実行し、その出力から手順 c で選択したポートを検索します。出力にそのポート番号が見つからない場合、HP Operations エージェントで高い確率で使用可能です。

4 NNMi 管理サーバーで以下のコマンドを入力して、NNMi から SNMP トラップを受信するためのカスタム ポートを HP Operations エージェントに設定します。

- *Windows* NNMi 管理サーバー :
  - — 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
    ```

  - — エージェントを再起動します。

    ```
    ovc -restart opctrapi
    ```

- *UNIX* NNMi 管理サーバー :
  - — 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
    ```

  - — 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、HP Operations エージェントへの NNMi インシデント転送を設定します。

a NNMi コンソールで、**[HP 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 **[HP 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 HP Operations エージェント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は、553 ページの「HP Operations エージェント接続」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は、554 ページの「HPOM 統合コンテンツ」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*。HPOM で、NNMi インシデント用のカスタム メッセージ属性をアクティブ メッセージ ブラウザに追加します。該当する手順に従ってください。

- *Windows 用 HPOM*:
  - ブラウザで、いずれかの列見出しを右クリックし、**[オプション]** をクリックします。
  - **[カスタム メッセージ属性入力]** リストで、属性を選択し、**[追加]** をクリックします。
- *UNIX 用 HPOM* または *Linux 用 HPOM*:
  - Java GUI メッセージ ブラウザで、任意の列見出しを右クリックし、**[メッセージ ブラウザ列のカスタマイズ]** をクリックします。
  - **[カスタム]** タブで、**[使用可能なカスタム メッセージ属性]** から選択し、**[OK]** をクリックします。

以下の情報に注意してください。

- NNMi インシデントの多くのカスタム メッセージ属性の先頭は `nnm` というテキストです。
- HP NNMi-HPOM 統合のエージェント実装の場合、NNMi インシデントの一部の重要な属性は以下のとおりです。

  ```
  nnm.name
  nnm.server.name
  ```

  その他の重要な CMA の詳細については、546 ページの「HP NNMi-HPOM 統合の使用法 (エージェント実装)」を参照してください。
- カスタム メッセージ属性がメッセージ ブラウザに表示される順序を変更するには、列見出しを新しい場所にドラッグします。

7 *オプション*。HPOM 管理サーバーで、NNMi ビューのコンテキスト起動を有効にします。

- *Windows 用 HPOM*: NNMi ソース ノードを HP NNMi Web ツール グループに関連付けます。

  詳細については、HPOM ヘルプの「*By Node ツール グループでツールを有効化*」を参照してください。
- *UNIX 用 HPOM*: NNMi アプリケーションの基本セットをインストールし、オプションで、その他の NNMi アプリケーションをインストールします。

  HPOM バージョン 9.00 以降では、自動的に基本の NNMi アプリケーションがインストールされます。

  詳細は、『HP Operations Manager for UNIX システム管理リファレンス ガイド』(バージョン 9.xx)、または『HP NNMi-HPOM Integration for HP Operations Manager User' s Guide (HP 操作マネージャ用 HP NNMi-HPOM 統合ユーザーガイド)』(バージョン 8.3x) の HP NNMi-HPOM 統合のインストールと設定に関するセクションを参照してください。
- *Linux 用 HPOM*: HPOM では自動的に基本の NNMi アプリケーションがインストールされます。オプションで、追加の NNMi アプリケーションをインストールします。

  詳細については、『HP Operations Manager for Linux システム管理リファレンス ガイド』で HP NNMi-HPOM 統合のインストールと設定に関するセクションを参照してください。

HP NNMi-HPOM 統合の使用法 (エージェント実装)

HP NNMi-HPOM 統合のエージェント実装では、NNMi 管理イベントと SNMP トラップが HP Operations エージェントに向けて一方向に送信されます。HPOM が着信トラップをどのように処理して表示するかは、SNMP トラップ ポリシー条件によって決まります。たとえば、トラップ カスタム メッセージ属性 (CAM) の値をメッセージのテキストに含めるようポリシー条件を変更できます。

NNMi は、HP Operations エージェントに対し、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 インシデントは HPOM アクティブ メッセージ ブラウザに表示されます。HPOM メニュー コマンドから、選択したメッセージに合った NNMi ビューにアクセスできます。各メッセージに含まれている情報が、このクロス ナビゲーションをサポートします。

- メッセージ内の CMA `nnmi.server.name` と `nnmi.server.port` は、NNMi 管理サーバーを指定します。
- CMA `nnmi.incident.uuid` は、NNMi データベース内のインシデントを指定します。

送信元のトラップ ソースは HPOM アクティブ メッセージ ブラウザの **[オブジェクト]** 列と CMA `nnm.source.name` に表示されます。(HP NNMi-HPOM 統合の Web サービス実装では、送信元のトラップ ソースは CMA `nnm.source.name` でのみ使用可能です。)

設定項目の ID

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

- 423 ページの「HP Business Service Management トポロジ」
- 433 ページの「HP Universal CMDB」

ヘルス インジケータ

`nnmopcexport.ovpl` に `-omi_hi` オプションを指定して NNMi SNMP トラップのポリシー ファイルを作成した場合、このポリシー ファイルにより、必要に応じて、SNMP トラップ ポリシー ファイルの各標準 NNMi 管理イベントにヘルス インジケータが関連付けられます。(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 CMA `EtiHint` 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メッセージは、HPOM のアクティブなメッセージ ブラウザに表示されます。
  - これらのトラップには、546 ページの「設定項目の ID」で説明されている CI 情報が含まれます。
  - このトラップから作成されたメッセージには、546 ページの「ヘルス インジケータ」で説明されているヘルス インジケータが含まれる場合があります。
- 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 トラップから作成されたメッセージは、HPOM のアクティブなメッセージ ブラウザに表示されます。
  - これらのトラップには、546 ページの「設定項目の ID」で説明されている CI 情報が含まれます。
  - このトラップから作成されたメッセージには、ヘルス インジケータは含まれません。
  - 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、HPOM 管理サーバーが SNMP トラップを NNMi が管理するデバイスから直接受信すると、HPOM はデバイス トラップを重複して受信します。NNMi からの SNMP トラップを HPOM が管理対象デバイスから直接受信したトラップと相関付けるようにポリシーを設定できます。
- EventLifecycleStateClosed トラップ
  - HP Operations エージェントは、このトラップから作成されたメッセージをログに記録します。一般的に、このメッセージは HPOM アクティブ メッセージ ブラウザに表示されます。
  - NNMi SNMP トラップ ポリシー ファイルにより、HP Operations エージェントは、HPOM アクティブ メッセージ ブラウザで解決済みの NNMi インシデントに対応するメッセージを受諾します。
- 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。HP Operations エージェントは、HPOM アクティブ メッセージ ブラウザにこのトラップを転送しません。
- 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。HP Operations エージェントは、HPOM アクティブ メッセージ ブラウザにこのトラップを転送しません。

- 相関関係通知トラップ
  - HP Operations エージェントは、このトラップから作成されたメッセージをログに記録します。このメッセージは、HPOM アクティブ メッセージ ブラウザに表示されます。
  - このトラップは、HPOM アクティブ メッセージ ブラウザに影響しません。

ポリシー条件のカスタマイズ

デフォルト ポリシー条件をカスタマイズするには、HPOM 管理サーバーで条件を編集してから、NNMi 管理サーバーの HP Operations エージェントにそのポリシーを再配布します。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。

- *HPOM for Windows*: HPOM ヘルプの「*SNMP Interceptor Policies*」(バージョン 9.0x) または「*Policy development*」(バージョン 8.1x)
- *UNIX 用 HPOM*: 『HP Operations Manager for UNIX コンセプト ガイド』
- *Linux 用 HPOM*: 『HP Operations Manager for Linux コンセプト ガイド』

詳細情報

HP NNMi-HPOM 統合のエージェント実装の詳細については、以下のリファレンスを参照してください。

- 統合によって HP Operations エージェントに送信されるトラップ タイプの詳細については、508 ページの「NNMi ノースバウンド インタフェースの使用法」を参照してください。
- NNMi が HP Operations エージェント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-HPOM 統合使用の詳細については、HPOM ドキュメントを参照してください。
  - *Windows 用 HPOM*: HPOM ヘルプの「*NNMi アダプタのエージェント実装*」を参照してください。
  - *UNIX 用 HPOM*: 『HP Operations Manager for UNIX システム管理リファレンス ガイド』(バージョン 9.xx) または『HP NNMi-HPOM Integration for HP Operations Manager User’s Guide (HP 操作マネージャ用 HP NNMi-HPOM 統合ユーザー ガイド)』(バージョン 8.3x) で HP NNMi-HPOM 統合のインストールと設定に関するセクションを参照してください。
  - *Linux 用 HPOM*: 『HP Operations Manager for Linux システム管理リファレンス ガイド』で HP NNMi-HPOM 統合のインストールと設定に関するセクションを参照してください。

HP NNMi-HPOM 統合設定の変更 (エージェント実装)

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。

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* リファレンス ページ、または UNIX マンページを参照してください。

2 新しい SNMP トラップ ポリシー ファイルを NNMi 管理サーバーから HPOM 管理サーバーに転送し、それを HPOM にインポートします。

3 HPOM 管理サーバーで NNMi 管理対象ノードに新しいポリシーを配布します。

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。この方法では、新しいポリシー ファイルを HPOM にインポートすると、カスタマイズした既存のポリシーは上書きされます。

設定パラメータの変更

統合設定パラメータを変更するには、以下の手順を実行します。

1 NNMi コンソールで、[**HP 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は、553 ページの「[HP NNMi-HPOM Agent デスティネーション] フォーム リファレンス (エージェント実装)」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-HPOM 統合の無効化 (エージェント実装)

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。

HP Operations エージェントへの 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、[**HP 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。

HPOM マニュアルの説明に従って、SNMP トラップ ポリシーの非アクティブ化または削除を必要に応じて実行します。

HP NNMi-HPOM 統合のトラブルシューティング (エージェント実装)

HPOM アクティブ メッセージ ブラウザが転送されたインシデントを受信しない

以下の手順で、OVBIN 環境変数は HP Operations エージェント コマンド用の bin ディレクトリを参照します。デフォルトでは、以下の値になります。

- *Windows*: *<drive>*¥Program Files¥HP¥HP BTO Software¥bin
- *UNIX*: /opt/OV/bin

HPOM アクティブ メッセージ ブラウザに NNMi からのインシデントが含まれていない場合、以下の手順を実行します。

1 NNMi 管理サーバーで、HP Operations 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

- *UNIX* 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*: SNMP_SESSION_MODE=NNM_LIBS
- *UNIX*: SNMP_SESSION_MODE=NO_TRAPD
- SNMP_TRAP_PORT=*<custom_port>*

  <custom_port> の値は、162 *ではなく*、**[HP 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 HP Operations エージェント設定を評価します。

- HP Operations エージェント設定が期待どおりの場合、この手順の手順 3 に進みます。
- SNMP_SESSION_MODE パラメータ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、544 ページの手順 4 を繰り返します。
- *<custom_port>* の値が 162 であるか、**[HP 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、必要に応じて 543 ページの手順 3 から 544 ページの手順 5 を繰り返します。

3 NNMi 管理サーバーで、HP Operations エージェントが動作していることを確認します。

- *Windows* NNMi 管理サーバー :

  %OVBIN%¥opcagt -status

- *UNIX* NNMi 管理サーバー :

  $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
```

出力が期待どおりでない場合、HP Operations 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、HP Operations エージェントが期待されている SNMP トラップ ポート上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*: **netstat -an | findstr <*custom_port*>**

— *UNIX*: **netstat -an | grep <*custom_port*>**

このとき、*<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。

出力が期待どおりでない場合、HP Operations エージェントを再起動します。

```
ovc -restart opctrapi
```

5 HPOM 管理サーバーで、NNMi 管理サーバー ノードの外部ノード フィルタを確認します。

HPOM 管理サーバーは、NNMi が管理するデバイスからのインシデントを受信するよう設定する必要があります。HPOM は、542 ページの手順 2 で説明したように、管理対象ノードとして設定されていなかったり、外部ノード フィルタに含まれていない NNMi ソース ノードから転送されたインシデントは無視します。

6 NNMi 管理サーバーで、NNMi の SNMP トラップ ポリシーが NNMi 管理サーバーの HP Operations エージェントに配布されていることを確認します。

- *Windows* NNMi 管理サーバー :

```
%OVBIN%¥ovpolicy -list
```

- *UNIX* 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、542 ページの手順 1 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。

7 HP Operations エージェントがトラップを受信していることを確認します。

a HP Operations エージェントが HPOM 管理サーバーにメッセージを送信できることを確認します。

b HP Operations エージェントのトレースを有効化して、トラップが HP Operations エージェントに到着するかどうか判定します。

HP Operations エージェントのトラブルシューティングについては、以下のリファレンスを参照してください。

- *Windows 用 HPOM*: HPOM ヘルプ
- *UNIX 用 HPOM*:『HP Operations Manager for UNIX HTTPS エージェント コンセプトと設定ガイド』
- *Linux 用 HPOM*:『HP Operations Manager for Linux HTTPS エージェント コンセプトと設定ガイド』

8 NNMi が HP Operations エージェント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、512 ページの「NNMi ノースバウンド インタフェースのトラブルシューティング」を参照してください。

HPOM アクティブ メッセージ ブラウザが転送された一部のインシデントを受信しない

HPOM アクティブ メッセージ ブラウザに NNMi インシデントが 1 つも表示されない場合、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 HPOM 管理サーバーで、NNMi 管理サーバー ノードの外部ノード フィルタを確認します。

HPOM 管理サーバーは、NNMi が管理するデバイスからのインシデントを受信するよう設定する必要があります。HPOM は、542 ページの手順 2 で説明したように、管理対象ノードとして設定されていなかったり、外部ノード フィルタに含まれていない NNMi ソース ノードから転送されたインシデントは無視します。

3 HPOM 管理サーバーで、HPOM が実行されていることを確認します。

HPOM 管理サーバーがシャット ダウンすると、HP Operations エージェントは受信したトラップをキューイングします。HPOM 管理サーバーが使用可能になると、HP Operations エージェントはキューイングしたトラップを転送します。

HP Operations エージェント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。

4 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。

[HP NNMi-HPOM Agent デスティネーション] フォーム リファレンス (エージェント実装)

[HP NNMi-HPOM Agent デスティネーション] フォームには、NNMi と HP Operations エージェントの間の通信を設定するためのパラメータが含まれています。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。(**[HP 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。)

[**HP 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。

[HP 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。

- 553 ページの「HP Operations エージェント接続」
- 554 ページの「HPOM 統合コンテンツ」
- 556 ページの「HP Operations エージェント転送先ステータス情報」

統合設定への変更を適用するには、**[HP 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。

HP Operations エージェント接続

表 61 に、HP Operations エージェントへの接続を設定するパラメータをリストします。

表 61　HP Operations エージェント接続情報

フィールド	説明
ホスト	完全修飾ドメイン名 (推奨) または NNMi 管理サーバーの IP アドレス。HP Operations エージェントが NNMi からの SNMP トラップを受信するシステムです。 この統合では、HP Operations エージェント ホストを特定する手段として、以下の方法がサポートされています。 • **NNMi FQDN** NNMi が NNMi 管理サーバー上の HP Operations エージェントへの接続を管理し、**[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。 • **ユーザー ループバック** 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。 **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、統合モジュールでのアプリケーション フェイルオーバーの影響について、513 ページの「アプリケーション フェールオーバーと NNMi ノースバウンド インタフェース」を参照してください。

表 61　HP Operations エージェント接続情報 (続く)

フィールド	説明
ポート	HP Operations エージェントが SNMP トラップを受信する UDP ポート。 HP Operations エージェント固有のポート番号を入力してください。この値は、543 ページの手順 3 で定義したポートです。 ポートを決定するには、NNMi 管理サーバー上で **`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。 **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	HP Operations エージェントがトラップを受信するための読み取り専用のコミュニティ文字列。 HP NNMi-HPOM 統合では、デフォルト値 `public` を使用します。

HPOM 統合コンテンツ

表 62 に、NNMi が HP Operations エージェントに送信するコンテンツを設定するパラメータをリストします。

表 62　HPOM 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指定。 • **管理** NNMi は NNMi が生成した管理イベントのみを HP Operations エージェントに転送します。 • **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 HP Operations エージェントに転送します。 • **両方** 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 HP Operations エージェントに転送します。 これがデフォルト設定です。 NNMi は、転送先が有効になるとすぐにインシデントの転送を開始します。 詳細については、508 ページの「インシデント転送」を参照してください。

表 62　HPOM 統合コンテンツ設定情報 (続く)

フィールド	説明
ライフサイクル状態の変化	インシデント変更通知の仕様。 • **エンハンスド解決済み** 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 HP Operations エージェントに送信します。 これがデフォルト設定です。 • **状態変化** 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 HP Operations エージェントに送信します。 • **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 HP Operations エージェントに送信します。さらに統合により、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が HP Operations エージェントに送信されます。 **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。 詳細については、509 ページの「インシデント ライフサイクル状態変化通知」を参照してください。
相関処理	インシデント相関処理通知の仕様。 • **なし** NNMi は、NNMi 因果関係分析によって判明したインシデント相関処理について、HP Operations エージェントに通知しません。 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相関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相関処理ごとに、トラップを 1 つ送信します。 詳細については、509 ページの「インシデント相関処理通知」を参照してください。
削除	インシデント削除の仕様。 • **送信しない** NNMi は、NNMi でインシデントが削除されても、HP Operations エージェントに通知しません。 これがデフォルト設定です。 • **送信** NNMi は、NNMi で削除されるインシデントごとに、削除トラップを HP Operations エージェントに送信します。 詳細については、510 ページの「インシデント削除通知」を参照してください。
NNMi コンソール アクセス	HPOM メッセージ ブラウザから 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 HP Operations エージェントに送信するトラップでは、NmsUrl varbind に NNMi URL が含まれます (1.3.6.1.4.1.11.2.17.19.2.2.2)。 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。

表 62　HPOM 統合コンテンツ設定情報 (続く)

フィールド	説明
Incident Filter(インシデント フィルタ)	HP Operations エージェントに送信されたイベントを統合でフィルタするときのオブジェクト ID (OID) のリスト。各フィルタ 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。 以下のオプションの 1 つを選択します。 • **なし** NNMi はすべてのイベントを HP Operations エージェントに送信します。 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。 インシデント フィルタを指定します。 • フィルタ 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 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。 詳細については、510 ページの「イベント転送フィルタ」を参照してください。

HP Operations エージェント転送先ステータス情報

表 63 に、HP Operations エージェントの読み取り専用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 63　HP Operations エージェント転送先ステータス情報

フィールド	説明
トラップ転送先 IP アドレス	HP Operations エージェント転送先ホスト名で解決する IP アドレス。 この値は、この HP Operations エージェント転送先に対して一意です。
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 HP Operations エージェントに送信するトラップでは、sysUptime フィールドにこの値が含まれます (1.3.6.1.2.1.1.3.0)。 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 HP Operations エージェントに送信するトラップでは、NmsUrl varbind にこの値が含まれます (1.3.6.1.4.1.11.2.17.19.2.2.2)。 この値は、このノースバウンド転送先に固有です。

HP NNMi-HPOM 統合 (Web サービス実装)

HP NNMi-HPOM 統合のエージェント実装は、HPOM と NNMi との統合に適したソリューションです。

HP NNMi-HPOM 統合のエージェントと Web サービスの両方の実装から、同じ HPOM 管理サーバーにメッセージが転送されると、HPOM アクティブ メッセージ ブラウザに、両方の実装からのメッセージがすべては表示されない可能性があります。そのため、HP では、同時に同じ HPOM 管理サーバーに対し、ある NNMi 管理サーバーから HP NNMi-HPOM 統合の両方の実装を実行することはサポートされていません。

この項では以下の内容について説明します。

- 557 ページの「HP NNMi-HPOM 統合について (Web サービス実装)」
- 559 ページの「HP NNMi-HPOM 統合の有効化 (Web サービス実装)」
- 563 ページの「HP NNMi-HPOM 統合の使用法 (Web サービス実装)」
- 564 ページの「HP NNMi-HPOM 統合設定の変更 (Web サービス実装)」
- 565 ページの「HP NNMi-HPOM 統合の無効化 (Web サービス実装)」
- 565 ページの「HP NNMi-HPOM 統合のトラブルシューティング (Web サービス実装)」
- 570 ページの「[HP NNMi-HPOM Web サービスの統合設定] フォーム リファレンス」

HP NNMi-HPOM 統合について (Web サービス実装)

HP NNMi-HPOM 統合の Web サービス実装では、NNMi インシデントが HPOM アクティブ メッセージ ブラウザに転送されます。統合によって、NNMi と HPOM の間でインシデントが同期されます。HPOM 内部から NNMi コンソール にアクセスすることもできます。

HP NNMi-HPOM 統合は、「多対多」の配置をサポートします。各 NNMi 管理サーバーは、複数の HPOM 管理サービスにインシデントを転送できます。同じように、各 HPOM 管理サーバーは複数の NNMi 管理サーバーからインシデントを受信できます。統合では、インシデントの一意の識別子を解釈して、ソース NNMi 管理サーバーを決定します。

HP NNMi-HPOM 統合は以下のコンポーネントで構成されます。

- **HP NNMi-HPOM 統合モジュール**

  HP NNMi-HPOM 統合モジュールは、NNMi から HPOM にインシデントを転送します。これは NNMi 管理サーバーにインストールおよび設定されます。

- **HP Operations Manager インシデント Web サービス**

  HPOM は、HP Operations Manager インシデント Web サービス (IWS) を使用して、NNMi から転送されたインシデントを受信します。

- **NNMi コンソールのコンテキスト アクセス用の HPOM アプリケーション**

  HPOM には、NNMi コンソール のフォーム、ビュー、およびツールにアクセスするアプリケーションがあります。たとえば、HPOM アクティブ メッセージ ブラウザから直接 NNMi インシデントを開けます。特定のアプリケーションによって、NNMi コンソール が開かれるコンテキストが決定されます。アプリケーション使用する前に、そのアプリケーションを設定する必要があります。

値

HP NNMi-HPOM 統合には、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ドメイン用の HPOM アクティブ メッセージ ブラウザ内にイベント統合体が用意されているため、HPOM 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 HPOM への自動インシデント転送。
  - 転送されたインシデントは HPOM アクティブ メッセージ ブラウザに表示されます。
  - NNMi がどのインシデントを転送するか制限するフィルタを作成できます。
- 以下の表で説明するような、NNMi と HPOM の間のインシデント更新の同期。

トリガ	結果
HPOM では、メッセージは肯定応答されます。	NNMi では、対応するインシデントのライフサイクル状態は [解決済み] に設定されます。
HPOM では、メッセージは肯定応答されません。	NNMi では、対応するインシデントのライフサイクル状態は [登録済み] に設定されます。
NNMi では、インシデントのライフサイクル状態は [解決済み] に設定されます。	HPOM では、対応するメッセージは肯定応答されます。
NNMi では、インシデントのライフサイクル状態は [解決済み] から他の状態に設定されます。	HPOM では、対応するメッセージは肯定応答されません。

- HPOM から NNMi コンソールへのアクセス。
  - HPOM ユーザーは、選択したメッセージのコンテキストで NNMi **[インシデント]** フォームを開くことができます。
  - HPOM ユーザーは、選択したメッセージとノードのコンテキストで、NNMi ビュー (たとえば、Layer 2 Neighbor ビュー) を起動できます。
  - HPOM ユーザーは、選択したメッセージと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) を起動できます。
  - HPOM が複数の NNMi 管理サーバーの NNMi インシデントを統合するとき、正しい NNMi 管理サーバーにアクセスするために、各インシデントの一意の識別子が解釈されます。

統合製品

このセクションの情報は、以下の製品に当てはまります。

- Windows 用 HPOM (OMW とも呼ばれる)
- UNIX 用 HPOM (OMU とも呼ばれる)
- Linux 用 HPOM (OML とも呼ばれる)

サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- NNMi 9.10

NNMi と HPOM は異なるコンピュータにインストールしてください。NNMi 管理サーバーと HPOM 管理サーバーのコンピュータのオペレーティング 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、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

この章では、HPOM 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。

HPOM ドキュメントには、NNMi と通信するように HPOM を設定する方法の説明が記載されています。HP NNMi-HPOM 統合の使用方法についての説明もあります。

- Windows 用 HPOM の詳細は、HPOM ヘルプの HP NNMi アダプタ情報を参照してください。
- UNIX 用 HPOM バージョン 9.xx については、『HP Operations Manager for UNIX システム管理リファレンス ガイド』の「*Integrating NNMi into HPOM (NNMi と HPOM の統合)*」セクションを参照してください。
- UNIX 用 HPOM バージョン 8.3x については『HP NNMi-HPOM Integration for HP Operations Manager User’s Guide (HP 操作マネージャ用 HP NNMi-HPOM 統合ユーザー ガイド)』を参照してください。
- Linux 用 HPOM については、『HP Operations Manager for Linux システム管理リファレンス ガイド』の「*Integrating NNMi into HPOM (NNMi と HPOM の統合)*」セクションを参照してください。

HP NNMi-HPOM 統合の有効化 (Web サービス実装)

このセクションでは、HP NNMi-HPOM 統合を有効化する手順について説明します。統合に組み入れる各 NNMi 管理サーバーと各 HPOM 管理サーバーについては、ご使用の HPOM バージョン用手続きの該当するステップを完了してください。

Windows 用 HPOM

1. NNMi 管理サーバーで、HPOM 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、**[HP 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. **[Web サービスの実装]** をクリックします。
   c. **[HP NNMi-HPOM Web サービスの統合設定]** フォームで、**[統合の有効化]** 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 管理サーバーへの接続情報を入力します。

統合には、NNMi コンソールへの HTTP 接続が必要であるため、**[NNMi SSL の有効化]** チェック ボックスはオフのままにします。

これらのフィールドの詳細は、570 ページの「NNMi 管理サーバー接続」を参照してください。

e HPOM 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は、571 ページの「HPOM Management Server Connection (HPOM 管理サーバー接続)」を参照してください。

f 以下のフィールドに値を入力します。

— **Forward Only(転送のみ)**

— **Holding period (minutes)(保持期間 (分単位))**

— **Incident Filter(インシデント フィルタ)**

これらのフィールドの詳細は、572 ページの「統合動作」を参照してください。

g NNMi から複数の HPOM 管理サーバーにインシデントを転送するには、**[別の HPOM サーバーを追加]** をクリックしてから、HPOM フィールドに以下の HPOM 管理サーバー情報を入力します。

最初のサーバーの情報が **[追加 HPOM Server]** リストに表示されます。

h 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。HPOM サーバーに接続できないというメッセージが表示されたら、**[HP NNMi-HPOM Web サービスの統合設定]** フォームを再び開き (またはメッセージ ウィンドウで **[ALT]+ 左矢印**を押し)、エラー メッセージを参考に HPOM 管理サーバーに接続するための値を調整します。

2 HPOM で、HPOM ヘルプの「*NNMi サーバー名とポートの設定*」の説明に従って、NNMi 管理サーバーに接続する NNMi アダプタを設定します。

3 HPOM で、各 NNMi ノードの管理対象ノードを追加します。このノードは、HPOM 管理サーバーに転送される NNMi インシデント内でソース ノードとして指名されます。また、HPOM 管理サーバーにインシデントを転送する各 NNMi 管理サーバーの管理対象ノードも追加します。

この代わりに、転送される全 NNMi インシデントを取得する 1 つの外部ノードを作成することもできます。初期テストのため、ノード フィルタを <*>.<*>.<*>.<*> (IP フィルタ用) または <*> (名前フィルタ用) に設定します。統合を検証した後、ご使用のネットワークに合わせて外部ノード フィルタを制限します。

詳細については、HPOM ヘルプの「*NNMi サーバー ノードの設定*」を参照してください。

NNMi インシデント ソース ノード用の HPOM 管理対象ノードを設定しないと、HPOM 管理サーバーは、そのノードに関する全インシデントを破棄します。

4 *オプション*。HPOM で、次のように、NNMi インシデント用のカスタム メッセージ属性をアクティブなメッセージ ブラウザに追加します。

a ブラウザで、いずれかの列見出しを右クリックし、**[オプション]** をクリックします。

b **[カスタム メッセージ属性入力]** リストで、属性を選択し、**[追加]** をクリックします。

— NNMi インシデントのカスタム メッセージ属性の先頭は `nnm` というテキストです。

— HP NNMi-HPOM 統合の Web サービス実装の場合、NNMi インシデントの最も重要な属性は以下のとおりです。

```
nnm.assignedTo
nnm.category
nnm.emittingNode.name
nnm.source.name
```

— カスタム メッセージ属性がメッセージ ブラウザに表示される順序を変更するには、列見出しを新しい場所にドラッグします。

5 *オプション*。HPOM で、NNMi ソース ノードを HP NNMi Web ツール グループと関連付けして、NNMi ビューのコンテキスト起動を有効にします。

詳細については、HPOM ヘルプの「*By Node ツール グループでツールを有効化*」を参照してください。

UNIX 用 HPOM または Linux 用 HPOM

1 *UNIX 用 HPOM バージョン 8.3x のみ*。次のように、UNIX 管理サーバー用に HPOM を準備します。

a 『*HP Operations Manager Incident Web Service Integration Guide*』の説明に従って、UNIX 用 HPOM 管理サーバーに HP Operations Manager インシデント Web サービス (IWS) をインストールします。

b UNIX 管理サーバー用の HPOM で、最新の HPOM 統合パッチをインストールします。パッチは次の URL で入手できます。

http://h20230.www2.hp.com/selfsolve/patches

2 NNMi 管理サーバーで、HPOM 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、**[HP 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 **[Web サービスの実装]** をクリックします。

c **[HP NNMi-HPOM Web サービスの統合設定]** フォームで、**[統合の有効化]** 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 管理サーバーへの接続情報を入力します。

統合には、NNMi コンソールへの HTTP 接続が必要であるため、**[NNMi SSL の有効化]** チェック ボックスはオフのままにします。

これらのフィールドの詳細は、570 ページの「NNMi 管理サーバー接続」を参照してください。

e HPOM 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は、571 ページの「HPOM Management Server Connection (HPOM 管理サーバー接続)」を参照してください。

f 以下のフィールドに値を入力します。

— **Forward Only(転送のみ)**

— **Holding period (minutes)(保持期間 (分単位))**

— **Incident Filter(インシデント フィルタ)**

これらのフィールドの詳細は、572 ページの「統合動作」を参照してください。

g NNMi から複数の HPOM 管理サーバーにインシデントを転送するには、**[別の HPOM サーバーを追加]** をクリックしてから、HPOM フィールドに以下の HPOM 管理サーバー情報を入力します。

最初のサーバーの情報が **[追加 HPOM Server]** リストに表示されます。

h 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。HPOM サーバーに接続できないというメッセージが表示されたら、**[HP NNMi-HPOM Web サービスの統合設定]** フォームを再び開き (またはメッセージ ウィンドウで **[ALT]+ 左矢印**を押し)、エラー メッセージを参考に HPOM 管理サーバーに接続するための値を調整します。

i フォームの下部にある **[送信]** をクリックします。

3 HPOM で、各 NNMi ノードの管理対象ノードを追加します。このノードは、HPOM 管理サーバーに転送される NNMi インシデント内でソース ノードとして指名されます。また、HPOM 管理サーバーにインシデントを転送する各 NNMi 管理サーバーの管理対象ノードも追加します。

この代わりに、転送される全 NNMi インシデントを取得する 1 つの外部ノードを作成することもできます。初期テストのため、ノード フィルタを <*>.<*>.<*>.<*> (IP フィルタ用) または <*> (名前フィルタ用) に設定します。統合を検証した後、ご使用のネットワークに合わせて外部ノード フィルタを制限します。

詳細については、『HP Operations Manager for UNIX システム管理リファレンス ガイド』または『HP Operations Manager for Linux システム管理リファレンス ガイド』を参照してください。

NNMi インシデント ソース ノード用の HPOM 管理対象ノードを設定しないと、HPOM 管理サーバーは、そのノードに関する全インシデントを破棄します。

4 *オプション*。HPOM で、次のように、NNMi インシデント用のカスタム メッセージ属性をアクティブなメッセージ ブラウザに追加します。

a Java GUI メッセージ ブラウザで、任意の列見出しを右クリックし、**[メッセージ ブラウザ列のカスタマイズ]** をクリックします。

b **[カスタム]** タブで、**[使用可能なカスタム メッセージ属性]** から選択し、**[OK]** をクリックします。

— NNMi インシデントのカスタム メッセージ属性の先頭は nnm というテキストです。

— HP NNMi-HPOM 統合の Web サービス実装の場合、NNMi インシデントの最も重要な属性は以下のとおりです。

```
nnm.assignedTo
nnm.category
nnm.emittingNode.name
nnm.source.name
```

— カスタム メッセージ属性がメッセージ ブラウザに表示される順序を変更するには、列見出しを新しい場所にドラッグします。

5 *オプション。* HPOM 管理サーバーで、NNMi コンソール にアクセスするために HPOM アプリケーションの準備をします。

a *必須。* NNMi アプリケーションの基本セットをインストールします。

HPOM バージョン 9.00 以降では、自動的に基本の NNMi アプリケーションがインストールされます。

b *オプション。* 追加の NNMi アプリケーションをインストールします。

詳細については、『HP Operations Manager for UNIX システム管理リファレンス ガイド』(バージョン 9.xx)、HP NNMi-HPOM Integration for HP Operations Manager User’s Guide (HP 操作マネージャ用 HP NNMi-HPOM 統合ユーザー ガイド) (バージョン 8.3x)、または『HP Operations Manager for Linux システム管理リファレンス ガイド』の HP NNMi-HPOM 統合のインストールと設定に関するセクションを参照してください。

HP NNMi-HPOM 統合の使用法 (Web サービス実装)

使用例

図 29 に、NNMi コンソールのインタフェース停止中インシデントを示します。**[ソース オブジェクト]** 列と **[メッセージ]** 列の情報が状況を記述しています。

図 29 NNMi コンソールにおけるインタフェース停止中のインシデント

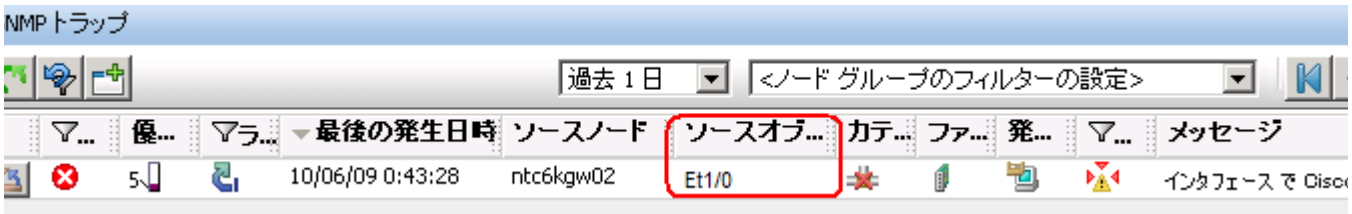


図 30 は、Windows 用 HPOM で受信された NNMi インシデントを示します。図 31 は、UNIX 用 HPOM で受信された NNMi インシデントを示します。**[nnm.source.name]** 列および **[テキスト]** 列は、NNMi コンソール の **[ソース オブジェクト]** 列および **[メッセージ]** 列と同等です。

561 ページの手順 4 (Windows 用 HPOM) および 562 ページの手順 4 (UNIX 用 HPOM および Linux 用 HPOM) で説明したように、**[nnm.source.name]** カスタム メッセージ属性列の表示を有効にする必要があります。

図 30 Forwarded Incident in HPOM for Windows(Windows 用 HPOM で転送済みのインシデント)

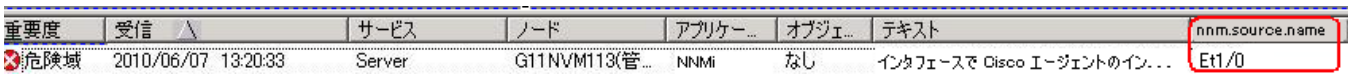


図 31 Forwarded Incident in HPOM for UNIX(UNIX 用 HPOM で転送済みのインシデント)

正常な状況 : 不明な MSI 条件

HPOM サーバーは、転送された NNMi インシデントを (通常のトラップ ポリシーではなく) MSI から受信します。HPOM メッセージ ブラウザでは、メッセージ ソースの形式は **MSI** の後ろに MSI インタフェースの名前がついた形式です。条件名は、メッセージ内の `condition_id` フィールドに対応し、関連するポリシーがないため設定されていません。

- *Windows 用 HPOM*: ポリシー タイプは空です。
- *UNIX 用 HPOM* または *Linux 用 HPOM*: メッセージ ソースの形式は以下のとおりです。
  MSI: <*MSI_Interface*>: Unknown Condition.

詳細情報

HP NNMi-HPOM 統合使用の詳細については、HPOM ドキュメントを参照してください。

- *Windows 用 HPOM*: HPOM ヘルプの「HP NNMi アダプタのエージェント実装」に関するトピックを参照してください。
- *UNIX 用 HPOM*: 『HP Operations Manager for UNIX システム管理リファレンス ガイド』(バージョン 9.xx) または『HP NNMi-HPOM Integration for HP Operations Manager User’s Guide (HP 操作マネージャ用 HP NNMi-HPOM 統合ユーザー ガイド)』(バージョン 8.3x) で HP NNMi-HPOM 統合のインストールと設定に関するセクションを参照してください。
- *Linux 用 HPOM*: 『HP Operations Manager for Linux システム管理リファレンス ガイド』で HP NNMi-HPOM 統合のインストールと設定に関するセクションを参照してください。

HPOM メッセージ ブラウザで、転送済み NNMi インシデントの詳細はカスタム メッセージ属性として入手できます。

HP NNMi-HPOM 統合設定の変更 (Web サービス実装)

1. NNMi コンソールで、[**HP 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. **[Web サービスの実装]** をクリックします。
3. 該当するように値を変更します。
   - Incident Filter リストと Additional HPOM Servers リストのエントリの構文を知っていると、直接にエントリを変更できます。
   - リスト項目の構文を知らない場合は、そのエントリを削除し、再入力します。

   このフォームのフィールドの詳細は、570 ページの「[HP NNMi-HPOM Web サービスの統合設定] フォーム リファレンス」を参照してください。
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-HPOM 統合の無効化 (Web サービス実装)

すべての HPOM 管理サーバーについて

NNMi インシデントのすべての HPOM 管理サーバーへの転送を継続停止にするには、次のステップを実行します。

1 NNMi コンソールで、**[HP 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 **[Web サービスの実装]** をクリックします。

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。

必要な場合は、すべての NNMi 管理サーバーについてこのプロセスを繰り返します。

1 つの HPOM 管理サーバーについて

NNMi インシデントの 1 つの HPOM 管理サーバーへの転送のみを継続停止にするには、次のステップを実行します。

1 NNMi コンソールで、**[HP 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 **[Web サービスの実装]** をクリックします。

3 **[追加の HPOM サーバー]** リストで、HPOM 管理サーバーを統合から切断するエントリ (1 つまたは複数) を削除するテキストを編集します。

   [クリア] をクリックすると、リストからすべての HPOM サーバーが削除されます。

4 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-HPOM 統合のトラブルシューティング (Web サービス実装)

HPOM は転送されたインシデントを受信しない

統合が過去においては正常に動作していた場合は、構成の何か (たとえば、NNMi または HPOM のパスワード) が最近変更された可能性があります。564 ページの「HP NNMi-HPOM 統合設定の変更 (Web サービス実装)」に説明されているように統合設定を更新してから、この手順全体を段階的に行うこともできます。

1 NNMi コンソールで、**[HP 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 **[Web サービスの実装]** をクリックします。

   このフォームのフィールドの詳細は、570 ページの「[HP NNMi-HPOM Web サービスの統合設定] フォーム リファレンス」を参照してください。

3 統合のステータスを確認するには、**[HP NNMi-HPOM Web サービス統合]** フォームで、フォームの下端の **[送信]** をクリックします (設定の変更は行いません)。

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。

- 正常な完了がメッセージに示されている場合は、NNMi が管理するデバイスからインシデントを受信するように HPOM が設定されていないことが問題であると考えられます。560 ページの手順 3 (Windows 用の HPOM) と 562 ページの手順 3 (UNIX 用の HPOM および Linux 用 HPOM) で説明したように、HPOM で管理対象ノードとして設定されていない NNMi ソース ノードから転送されたインシデントを HPOM は無視します。HPOM 設定を確認し、この手順の手順 10 で説明したように統合をテストします。
- HPOM サーバーへの接続に問題があることがメッセージに示されている場合、NNMi と HPOM は通信できません。この手順の 手順 4 を継続します。

4 HPOM コンソールにログインし、HPOM アクティブ メッセージ ブラウザを表示して、HPOM 資格情報の正確さとアクセス レベルを確認します。

- *Windows 用 HPOM*: **[HPOM ユーザ]** として **[HP NNMi-HPOM Web サービスの統合設定]** フォームからコンピュータにログオンし、HPOM コンソールを起動します。

  ユーザー名の形式は、*<Windows_domain>*¥*<username>* です。

- *UNIX 用 HPOM* または *Linux 用 HPOM*: **[HP NNMi-HPOM Web サービスの統合設定]** フォームから **[HPOM ユーザ]** の資格情報を使用して、HPOM コンソールにログオンします。

HPOM コンソールにログオンできない場合は、HPOM 管理者に連絡してログオン資格情報を確認してください。

5 次のように、HPOM 管理サーバーへの接続が正しく設定されていることを確認します。

a Web ブラウザで、次の URL を入力します。

<*protocol*>://<*omserver*>:<*port*>/opr-webservice//Incident.svc?wsdl

このとき、以下のように、変数は **[HP NNMi -HPOM Web サービス統合]** フォームの値に関連があります。

— **[HPOM SSL が有効になっています]** チェック ボックスがオンの場合、*<protocol>* は `https` です。

— **[HPOM SSL が有効になっています]** チェック ボックスがオフになっている場合、*<protocol>* は `http` です。

— *<omserver>* は **[HPOM ホスト]** の値です。

— *<port>* は、**[HPOM ポート]** の値です。

b プロンプトが表示されたら、**[HP NNMi-HPOM Web サービスの統合設定]** フォームから **[HPOM ユーザー]** の資格認定を入力します。

結果の Web ページは IWS を記述する XML ファイルです。

— XML ファイルが表示された場合、HPOM サーバーへの接続は正常に設定されています。手順 6 を継続します。

— エラー メッセージが表示された場合、HPOM 管理サーバーへの接続は正常に設定されていません。HPOM 管理者に連絡して、HPOM Web サービスへの接続に使用している情報を確認してください。XML ファイルが表示されるまで、HPOM への接続のトラブルシューティングを継続します。

6 NNMi への接続が正常に設定されていることを確認します。

この手順の 手順 1 で NNMi コンソール に接続するために、このステップで説明してある情報を使用した場合は、NNMi コンソール に再接続する必要はありません。手順 7 を継続します。

a Web ブラウザで、次の URL を入力します。

<protocol>://<NNMiserver>:<port>/nnm/

このとき、以下のように、変数は **[HP NNMi -HPOM Web サービス統合]** フォームの値に関連があります。

— **[NNMi SSL が有効になっています]** チェック ボックスがオンの場合、*<protocol>* は `https` です。

[NNMi SSL が有効になっています] チェック ボックスが選択されている場合、以下のコマンドを入力して KeyManager プロセスが実行されていることを確認します。

```
ovstatus -v ovjboss
```

— **[NNMi SSL が有効になっています]** チェック ボックスがオフになっている場合、*<protocol>* は `http` です。

— *<NNMiserver>* は **[NNMi ホスト]** の値です。

NNMi 管理サーバーの完全修飾ドメイン名または IP アドレスを使用します。`localhost` は使用しないでください。

— *<port>* は、**[NNMi ポート]** の値です。

NNMi ポートが HTTP か HTTPS かを確認するには、570 ページの表 64 の説明のように、`nms-local.properties` ファイルを確認します。

b プロンプトが表示されたら、管理者ロールで NNMi ユーザーの資格認定を入力します。

NNMi コンソール が表示されるはずです。NNMi コンソールが表示されない場合は NNMi 管理者に連絡して、NNMi に接続するために使用している情報を確認してください。NNMi コンソール が表示されるまで、NNMi への接続のトラブルシューティングを継続します。

「Web サービス クライアント」ロールを持つユーザーとして NNMi コンソールにサインインすることはできません。

c **[NNMi ユーザー]** と **[NNMi パスワード]** の値を確認します。

— **[HP NNMi-HPOM Web サービスの統合設定]** フォームにリストされている **[NNMi ユーザー]** が「管理者」ロールを持っており、以前にこのユーザー名で NNMi コンソールに接続できた場合は、対応するパスワードを **[HP NNMi-HPOM Web サービスの統合設定]** フォームに再入力します。

— **[HP NNMi-HPOM Web サービスの統合設定]** フォームにリストされている **[NNMi ユーザー]** が「Web サービス クライアント」ロールを持っている場合は、NNMi 管理者に連絡し、**[NNMi ユーザー]** と **[NNMi パスワード]** の値を確認してください。

パスワードは NNMi コンソール では非表示です。NNMi ユーザー名のパスワードが何か確信がない場合は、NNMi 管理者に問い合わせするか、またはパスワードをリセットします。

7 この手順の手順 5 と手順 6 で接続に成功したときに使用した値で **[HP NNMi-HPOM Web サービスの統合設定]** フォームを更新します。

詳細については、570 ページの「[HP NNMi-HPOM Web サービスの統合設定] フォーム リファレンス」を参照してください。

8 フォームの下部にある **[送信]** をクリックします。

9 HPOM サーバーに接続できないというステータス メッセージがまだ表示されるようなら、以下を実行します。

a Web ブラウザのキャッシュをクリアします。

b Web ブラウザから、すべての保存フォームまたはパスワード データをクリアします。

c Web ブラウザ ウィンドウを完全に閉じてから、もう一度開きます。

d この手順の手順 7 と手順 8 を繰り返します。

10 設定をテストするには、NNMi 管理サーバー上でインシデントを生成し、それが HPOM 管理サーバーに到着するかどうか判定します。

あるいは、NNMi 管理イベントのライフサイクル状態を [未解決] に変更します。(現在のライフサイクル状態が [未解決] の場合は、ライフサイクル状態を [解決済み] に設定してから [未解決] に戻します。)

転送されたインシデントの中に HPOM が受信しないものがある

HPOM ノードとインシデント フィルタを確認します。

HPOM 管理サーバーは、NNMi が管理するデバイスからのインシデントを受信するよう設定する必要があります。560 ページの手順 3 (Windows 用の HPOM) と 562 ページの手順 3 (UNIX 用の HPOM および Linux 用 HPOM) で説明したように、HPOM で管理対象ノードとして設定されていない NNMi ソース ノードから転送されたインシデントを HPOM は無視します。

NNMi ソース ノードが HPOM 内で管理対象ノードとして設定されている場合は、**[HP NNMi-HPOM Web サービスの統合設定]** フォームのインシデント フィルタ設定を確認します。フィルタをテストするには、NNMi 管理サーバーでインシデントを生成し、それが HPOM 管理サーバーに到達するかどうか判定します。

NNMi インシデント情報が HPOM メッセージ ブラウザでは入手できない

NNMi インシデントからの重要情報は、カスタム メッセージ属性として HPOM に渡されます。561 ページの手順 4 (Windows 用 HPOM) および 562 ページの手順 4 (UNIX 用 HPOM および Linux 用 HPOM) で説明した NNMi インシデントの複数のカスタム メッセージ属性を追加します。

NNMi と HPOM が同期されない

どちらかの管理サーバーが到達不可能になった場合、NNMi インシデント ビューのインシデントと HPOM アクティブ メッセージ ブラウザのインシデントが一致しなくなる可能性があります。次のようにすると、HP NNMi-HPOM 統合はインシデントを再同期できます。

- HP NNMi-HPOM 統合モジュールが HPOM 管理サーバーを利用できなくなると、統合モジュールはその HPOM 管理サーバーの可用性を定期的に確認し、接続を再確立できた時点でインシデント転送を再開します。HPOM 管理サーバーへの接続が利用できるようになると、統合モジュールは、HPOM 管理サーバーの停止の間に失われた可能性のあるインシデントを転送します。

- HPOM ユーザーが転送されたインシデントを受諾または受諾解除するときに NNMi 管理サーバーが利用できない場合、NNMi は状態変化を受信しません。NNMi と HPOM はこのインシデントについて異なる状態を示す可能性があります。

統合がファイアウォールを経由して動作しない

NNMi 管理サーバーが、ホストとポートによって、HPOM IWS を直接取り扱えることを確認します。

[HP NNMi-HPOM Web サービスの統合設定] フォーム リファレンス

[HP NNMi-HPOM Web サービスの統合設定] フォームには、NNMi と HPOM の間の通信を設定するためのパラメータが含まれています。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。(**[HP NNMi-HPOM の統合選択]** フォームで、**[Web サービスの実装]** をクリックします。)

[HP NNMi-HPOM Web サービスの統合設定] 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。

[HP NNMi HPOM Web サービスの統合設定] フォームでは、以下の一般的な情報を収集します。

- 570 ページの「NNMi 管理サーバー接続」
- 571 ページの「HPOM Management Server Connection (HPOM 管理サーバー接続)」
- 572 ページの「統合動作」
- 573 ページの「Incident Filter (インシデント フィルタ)」

統合設定への変更を適用するには、**[HP NNMi-HPOM Web サービスの統合設定]** 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 64 に、NNMi 管理サーバーへの接続パラメータをリストします。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 64　NNMi 管理サーバー接続情報

フィールド	説明
NNMi SSL 有効化	NNMi コンソールに接続するための接続プロトコルの指定。 統合には、NNMi コンソールへの HTTP 接続が必要であるため、**[NNMi SSL の有効化]** チェック ボックスはオフのままにします。
NNMi ホスト	NNMi 管理サーバーの完全修飾ドメイン名。このフィールドには、NNMi コンソールへのアクセスに使用するホスト名があらかじめ入力されています。この値が、NNMi 管理サーバー上で **`nnmofficialfqdn.ovpl -t`** コマンド実行によって返された名前であることを確認します。
NNMi Port(NNMi ポート)	NNMi コンソール に接続するためのポート。このフィールドには、次のファイルで指定されているように、NNMi コンソール との通信のために jboss アプリケーション サーバーが使用するポートがあらかじめ記入されています。 • *Windows*: `%NnmDataDir%¥conf¥nnm¥props¥nms-local.properties` • *UNIX*: `$NnmDataDir/conf/nnm/props/nms-local.properties` `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)。

表 64　NNMi 管理サーバー接続情報 (続く)

フィールド	説明
NNMi User(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。 注 : このユーザー名のパスワードはクリアテキストで渡されます。 ベスト プラクティス :「Web サービス クライアント」ロールを持つ `NNMiIntegration` ユーザー アカウントを作成して使用します。
NNMi Password(NNMi パスワード)	指定の NNMi ユーザーのパスワード。

HPOM Management Server Connection (HPOM 管理サーバー接続)

表 65 に、HPOM 管理サーバー上の Web サービスに接続するためパラメータをリストします。HPOM 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。

表 65　HPOM 管理サーバー接続情報

HPOM サーバー パラメータ	説明
HPOM SSL Enabled(HPOM SSL 有効化)	接続プロトコル指定。 • HPOM が HTTPS を使用するよう設定されている場合、**[HPOM SSL が有効になっています]** チェック ボックスをオンにします。これがデフォルト設定です。 • HPOM が HTTP を使用するよう設定されている場合は、**[HPOM SSL が有効になっています]** チェック ボックスをオフにします。
HPOM Host(HPOM ホスト)	HPOM 管理サーバーの完全修飾ドメイン名。 コマンド `nslookup` または `ping` を使用して、NNMi 管理サーバーからこの名前を解決できることを確認します。 DNS に問題があるようなら、HPOM 管理サーバーの IP アドレスを使用します。可能ならば、`traceroute` コマンドを使用して、NNMi 管理サーバーから HPOM 管理サーバーへのネットワーク パスを確認します。
HPOM Port(HPOM ポート)	HPOM Web サービスに接続するためのポート。どのポート番号を指定するか決定するには、HPOM 管理サーバーで以下を行います。 • *Windows 用 HPOM*: IIS Manager のポート設定を調べます。これは **[スタート]** メニューから利用できます。たとえば、**[スタート] > [管理ツール] > [インターネット情報サービス (IIS) マネージャ]** です。 • *UNIX 用 HPOM* または *Linux* 用 HPOM: コマンド **`ovtomcatbctl -getconf`** を実行します。 このフィールドには `443` という値があらかじめ記入されています。Windows の場合の、HPOM への SSL 接続のデフォルト ポートです。UNIX 用 HPOM または Linux 用 HPOM への SSL 接続の場合、デフォルト ポートは 8443 または 8444 です。

表 65　HPOM 管理サーバー接続情報 (続く)

HPOM サーバー パラメータ	説明
HPOM User (HPOM ユーザー)	HPOM Administrator ロールのある、有効な HPOM ユーザー アカウント名。このユーザーには、HPOM アクティブ メッセージ ブラウザと HPOM インシデント Web サービス WSDL を表示する許可が必要です。 *Windows のみ* : Windows オペレーティング システムでは、HPOM は Microsoft インターネット情報サービス (IIS) を経由して動作し、ユーザー資格認定を認証します。Windows ユーザーを *<Windows_domain>*¥*<username>* の形式で指定します。 ベスト プラクティス : • *Windows 用 HPOM*: HP-OVE-ADMINS ユーザー グループに所属するユーザーを指定します。(Microsoft 管理コンソールの [ローカル ユーザーとグループ] 領域で、グループ メンバーシップを確認します。**[コントロール パネル] > [管理ツール] > [コンピュータの管理]** から操作できます。) • *UNIX 用 HPOM* または *Linux 用 HPOM*: ユーザー アカウント opc_adm を使用します。
HPOM Password (HPOM パスワード)	指定の HPOM ユーザーのパスワード。

統合動作

表 66 に、統合動作を記述するパラメータをリストします。NNMi 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。

表 66　統合動作情報

フィールド	説明
Forward Only (転送のみ)	HP NNMi-HPOM 統合モジュールの動作指定。デフォルトで、統合モジュールは、**[HP NNMi-HPOM Web サービスの統合設定]** フォームで指定された HPOM 管理サーバーにインシデントを転送し、同じサーバーからインシデント受諾を受信します。インシデント肯定応答の受信を無効にすることもできます。 • 単方向通信 (HPOM にインシデントを転送するが、HPOM からのインシデント肯定応答は無視する) の場合は、**[転送のみ]** チェック ボックスをオンにします。 • 双方向通信の場合は、**[転送のみ]** チェック ボックスをオフにします。これがデフォルト動作です。
Holding period (minutes) (保持期間 (分単位))	HPOM に設定済みインシデントを転送するまで待機できる時間 (分単位)。この待機時間の間にインシデントが閉じられた場合 (たとえば、SNMPLinkUp インシデントが SNMPLinkDown インシデントをキャンセルした場合)、HPOM はそのインシデントを受信することはありません。NNMi がただちにインシデントを転送するようにするには、値 0 を入力します。 デフォルト値は 5 分です。
Incident Filter (インシデント フィルタ)	インシデント転送を制限する NNMi インシデント属性を基礎にしたフィルタ。デフォルトのフィルタ (nature=ROOTCAUSE origin=MANAGEMENTSOFTWARE) は、NNMi が生成するすべての根本原因インシデントを指定します。フィルタを修正して、どのインシデントが HPOM に転送されるか変更できます。 **注 : [インシデント フィルタ]** フィールドのテキスト (属性名と値) はすべて、大文字小文字が区別されます。 詳細については、Incident Filter (インシデント フィルタ) を参照してください。

Incident Filter (インシデント フィルタ)

インシデント フィルタは、**[インシデント フィルタ]** リスト内の全エントリの組み合わせです。同じ属性を持つフィルタ エントリはフィルタを拡張します (論理和)。異なる属性を持つフィルタ エントリはフィルタを制限します (論理積)。すべてのフィルタ エントリがともに機能します。`(a AND b) OR c` の形のフィルタは作成 *できません*。フィルタ エントリ例は、574 ページの「インシデント フィルタの例」を参照してください。

インシデント フィルタを作成するには、以下のステップを行います。

1. NNMi コンソールで、**[HP 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. **[Web サービスの実装]** をクリックします。
3. フィルタ エントリを削除するには、**[インシデント フィルタ]** リストで、テキストを編集してエントリ (1 つまたは複数) を削除します。

   [クリア] をクリックすると、リストからすべてのフィルタ エントリが削除されます。

4. インシデント フィルタ エントリを追加する方法
   a. **[名前]** リストから属性を選択します。サポートされている属性については、手順 c の表を参照してください。
   b. 実行する比較演算子を選択します。サポートされている演算子は次のとおりです。
      - =
      - !=
      - <
      - <=
      - >
      - >=
   c. 比較値を入力します。次表に、サポートされている属性、および各属性について受け入れられる値をリストします。

属性	使用できる値
name (名前)	NNMi コンソール のインシデント設定を調べ、使用可能なインシデント名を決定します。
nature(性質)	• ROOTCAUSE • SECONDARYROOTCAUSE • SYMPTOM • SERVICEIMPACT • STREAMCORRELATION • INFO • なし

属性	使用できる値
origin(ソース)	• MANAGEMENTSOFTWARE • MANUALLYCREATED • SYMPTOM • REMOTELYGENERATED • SNMPTRAP • SYSLOG • OTHER
family(ファミリ)	• com.hp.nms.incident.family.Address • com.hp.nms.incident.family.Interface • com.hp.nms.incident.family.Node • com.hp.nms.incident.family.OSPF • com.hp.nms.incident.family.HSRP • com.hp.nms.incident.family.AggregatePort • com.hp.nms.incident.family.Board • com.hp.nms.incident.family.Connection • com.hp.nms.incident.family.Correlation
category(カテゴリ)	• com.hp.nms.incident.category.Fault • com.hp.nms.incident.category.Status • com.hp.nms.incident.category.Config • com.hp.nms.incident.category.Accounting • com.hp.nms.incident.category.Performance • com.hp.nms.incident.category.Security • com.hp.nms.incident.category.Alert
severity(重要度)	• NORMAL • WARNING • MINOR • MAJOR • CRITICAL

5 すべてのフィルタ エントリが定義されるまで、手順 4 を繰り返します。

6 フォームの下部にある **[送信]** をクリックします。

インシデント フィルタの例

NNMi から HPOM に NodeDown インシデントを転送

```
name=NodeDown
```

NNMi から HPOM に NodeDown インシデントと InterfaceDown インシデントを転送

```
name=NodeDown
name=InterfaceDown
```

NNMi から HPOM に CiscoLinkDown インシデントを転送

```
name=CiscoLinkDown
```

severity(重要度) が MAJOR または MINOR の NNMi 管理イベントを転送

```
origin=MANAGEMENTSOFTWARE
severity=MAJOR
severity=MINOR
```

severity(重要度) が少なくとも MINOR で nature(性質) が ROOTCAUSE または SERVICEIMPACT の NNMi インシデントを転送

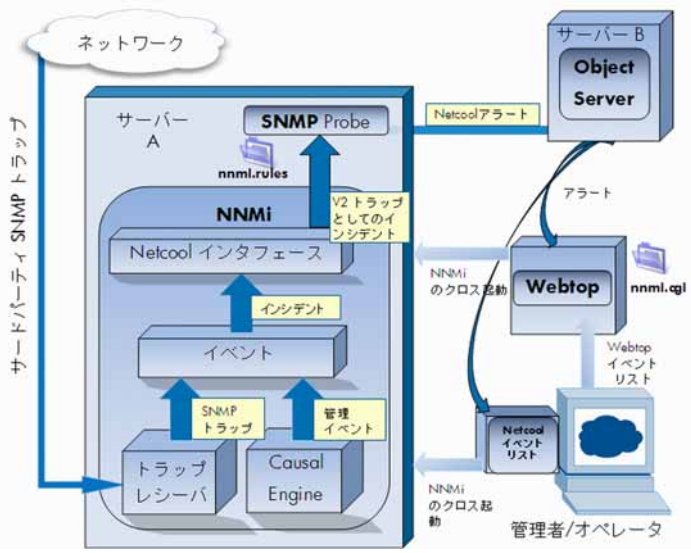
```
severity>=MINOR
nature=ROOTCAUSE
nature=SERVICEIMPACT
```

インシデント フィルタの制限

すべてのフィルタ エントリが結合して NNMi 管理サーバー用の 1 つのインシデント フィルタを作成するので、次の制限が適用されます。

- 記述された severity(重要度) がすべてのインシデントに適用されます。たとえば重大度 [警戒域] 以上の NodeDown インシデントおよび重大度が [重要警戒域] の InterfaceDown インシデントを転送するには、フィルタの重大度を `>=MINOR` に設定し、不要な InterfaceDown メッセージを除外する HPOM ロジックを使用します。
- インシデント フィルタには、特定のソース ノードへのインシデント転送を制限するメカニズムが備わっていません。HPOM 管理対象ノード (または外部ノード) 設定は、HPOM が受信する転送済みインシデントを制限します。

HP NNMi Integration Module for Netcool Software



IBM Tivoli Netcool/OMNIbus 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。

この章には、以下のトピックがあります。

- HP NNMi Integration Module for Netcool Software
- HP NNMi Integration Module for Netcool Software の有効化
- HP NNMi Integration Module for Netcool Software の使用法
- HP NNMi Integration Module for Netcool Software の変更
- HP NNMi Integration Module for Netcool Software の無効化
- HP NNMi Integration Module for Netcool Software のトラブルシューティング
- HP NNMi Integration Module for Netcool Software 転送先フォームのリファレンス

HP NNMi Integration Module for Netcool Software

HP NNMi Integration Module for Netcool Software は、NNMi 管理イベントを SNMPv2c トラップとして NNMi 管理サーバー上の Netcool/OMNIbus SNMP Probe に転送します。プローブは、NNMi トラップをフィルタし、Netcool/OMNIbus サーバーに転送します。

統合では NNMi が管理対象デバイスから受け取る SNMP トラップもプローブに転送できますが、NNMi SNMP トラップ転送メカニズムを使用することを推奨します。詳細については、`hp-nnmi-nbi.mib` ファイルを参照してください。

統合は、NNM 6.x または 7.x 管理ステーションが生成するイベントをプローブに転送しません。

統合は、選択されたイベントのコンテキストで NNMi のフォームとビューを起動するための、Netcool イベント ビューアを拡張するメニュー項目を提供します。

Netcool ソフトウェア用 NNMi 統合モジュールは、NNMi ノースバウンド インタフェースの具体的な実装で、これについては 505 ページの「NNMi ノースバウンド インタフェース」に説明されています。

Netcool ソフトウェア用 NNMi 統合モジュールは以下のコンポーネントで構成されます。

- nnmi-northbound 統合モジュール
- NNMi トラップを Netcool/OMNibus イベントに変更し、Netcool/Webtop イベント リストと Netcool/OMNIbus イベント リストに新しいメニューを作成するための設定ファイル

値

Netcool ソフトウェア用 NNMi 統合モジュールは、Netcool/OMNIbus ユーザーが潜在的なネットワークの問題を検知して調査できるように、ネットワークレベル障害とパフォーマンス情報と Netcool/OMNIbus に追加します。

統合の主要な機能は以下のとおりです。

- NNMi から Netcool/OMNIbus に転送する自動管理イベント 転送された管理イベントは Netcool/Webtop イベント リストと Netcool/OMNIbus イベント リストに表示されます。
- Netcool/Webtop および Netcool/OMNIbus からの NNMi コンソールへのアクセス
  - Netcool ユーザーは、選択したイベントとトポロジ オブジェクトのコンテキストで、NNMi フォーム (ノード フォームなど) を起動できます。
  - Netcool ユーザーは、選択したイベントとノードのコンテキストで、NNMi ビュー (Layer 2 Neighbor ビューなど) を起動できます。
  - Netcool ユーザーは、選択したイベントのコンテキストで、NNMi インシデント フォームを起動できます。

統合製品

この章の情報は、以下の製品に当てはまります。

- Netcool/OMNIbus

サポートされるバージョンは、*NNMi システムおよびデバイスのサポート マトリックス*にリストされています。

- Netcool/OMNIbus SNMP Probe
- NNMi 9.10 (Netcool ソフトウェア用 NNMi 統合モジュールライセンス付き)

NNMi 9.00 では、NNMi をインストールすることによって、Netcool ソフトウェア用 NNMi 統合モジュールの一時試用ライセンス キーが有効になります。試用ライセンス キーが有効期限切れになった後に統合を使用するには、Netcool ソフトウェア用 NNMi 統合モジュールの恒久ライセンス キーを取得してインストールします。

NNMi および Netcool/OMNIbus は、別々のコンピュータにインストールする必要があります。NNMi 管理サーバーと Netcool/OMNIbus サーバーのコンピュータで使用するオペレーティング システムは同一である必要はありません。

Netcool/OMNIbus SNMP Probe は、NNMi 管理サーバーのコンピュータ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、NNMi の対応マトリックスおよび Netcool/OMNIbus の製品ドキュメントを参照してください。

ドキュメント

この章では、NNMi 管理イベントを Netcool/OMNIbus SNMP Probe に転送するように Netcool ソフトウェア用 NNMi 統合モジュールを設定する方法を説明します。また、統合機能の使用方法の説明もあります。

Netcool/OMNIbus の詳細については、アプリケーションのドキュメントを参照してください。

HP NNMi Integration Module for Netcool Software の有効化

Netcool ソフトウェア用 NNMi 統合モジュールには、Netcool/OMNIbus SNMP Probe と Netcool イベント ビューアの設定に使用するファイルが含まれます。Netcool は機能を高度に設定できるため、Netcool の設定に関する指示がご使用の Netcool システムと正確に一致しない場合もあります。統合を有効にする手順は、経験のある Netcool 管理者が実行することを推奨します。

Netcool ソフトウェア用 NNMi 統合モジュールを有効にするには、以下の手順を実行します。

1 Netcool を設定するための情報を収集します。

   a 任意のコンピュータで、管理者ロールを持つ NNMi ユーザーとして NNMi コンソールにサインインします。

   b NNMi コンソールで、**[HP NNMi Integration Module for Netcool Software 設定アクション]** フォームを開きます (**[統合モジュールの設定] > [Netcool]**)。

   c **nnmi.include.rules** リンクを右クリックして、ファイルをコンピュータに保存し、Netcool/OMNIbus SNMP Probe の rules インクルード ファイルをダウンロードします。

   `nnmi.include.rules` ファイルには、NNMi 管理イベントの SNMPv2c トラップを解釈するルールが定義されています。

   — NNMi がプローブに送信するトラップの内容と形式については、`hp-nnmi-nbi.mib` ファイルを参照してください。

   — `nnmi.include.rules` ファイルのカスタマイズについては、Netcool/OMNIbus ドキュメントを参照してください。

   d *オプション*。Netcool/Webtop イベント リストの設定情報をダウンロードし、NNMi ビューを起動します。以下を両方とも実行します。

   — **nnmi_launch.cgi** リンクを右クリックし、ファイルをコンピュータに保存します。

   — **nmi_launch_cfg.txt** リンクを右クリックし、ファイルをコンピュータに保存します。

   e *オプション*。Netcool/OMNIbus イベント リストの設定情報をダウンロードし、NNMi ビューを起動します。以下のいずれかを行います。

   — *Windows* Netcool/OMNIbus サーバー :

   nnmi_confpack.zip リンクを右クリックし、ファイルをコンピュータに保存します。

   — *UNIX* Netcool/OMNIbus サーバー :

   nnmi_confpack.gz リンクを右クリックし、ファイルをコンピュータに保存します。

2 NNMi 管理サーバーに Netcool/OMNIbus SNMP Probe をインストールします。

a 利用できる UDP ポートで SNMP トラップを受け取るようにプローブを設定します。

— NNMi に統合を設定するこのポート番号を書き留めます。

— プローブ ポートと NNMi が SNMP トラップを受け取るポートが異なっていることを確認します。プローブ ポートは、NNMi コンソールの **[通信の設定]** フォームで設定されています。

b 手順 1c の `nnmi.include.rules` ファイルを NNMi 管理サーバーにコピーします。

c マスター ルール ファイルをバックアップし、そのファイルを任意のテキスト エディタで開きます。

d Netcool エンタープライズ トラップ スイッチ ブロックに、`nnmi.include.rules` ファイルに使用する `include` ディレクティブを追加し、マスター ルール ファイルを保存します。

e プローブを再起動し、プローブ ログ ファイルでルール ファイルの再ロードに問題がないことを確認します。

プローブのインストールと設定については、プローブのドキュメントを参照してください。

3 NNMi インシデントの転送を設定します。

a 任意のコンピュータで、管理者ロールを持つ NNMi ユーザーとして NNMi コンソールにサインインします。

b NNMi コンソールで、**[HP NNMi Integration Module for Netcool Software 設定アクション]** フォームを開きます (**[統合モジュールの設定] > [Netcool]**)。

c Netcool ソフトウェア用 NNMi 統合モジュールの **[有効化 / 無効化]** をクリックし、**[新規]** 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。)

d **[HP NNMi Integration Module for Netcool Software デスティネーション]** フォームで **[有効にする]** チェック ボックスを選択し、フォームのほかのフィールドを有効にします。

e Netcool/OMNIbus SNMP Probe への接続情報を入力します。

これらのフィールドの詳細は、585 ページの「Netcool/OMNIbus SNMP Probe の接続」を参照してください。

f 送信オプションを指定します。

これらのフィールドの詳細は、586ページの「統合コンテンツ」を参照してください。

g 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。

4 *オプション*。NNMi を起動するように Netcool/OMNIbus SNMP Probe を設定します。

a 手順 1d の `nnmi_launch.cgi` ファイルを Netcool/Webtop サーバーの `cgi-bin` ディレクトリにコピーします。

b 手順 1d の `nnmi_launch_cfg.txt` ファイルに記載されている指示に従って、CGI ファイルを準備し、Netcool/Webtop メニューを設定します。

5 *オプション*。NNMi ビューを起動するように Netcool/OMNIbus イベント リストを設定します。

a 手順 1e の `nnmi_confpack.*` アーカイブ ファイルを Netcool/OMNIbus ObjectServer のインスタンスが実行しているコンピュータにコピーします。

b 一時保存場所に nnmi_confpack.* アーカイブ ファイルを解凍します。

c 一時保存場所から以下のコマンドを実行します。

— *Windows* Netcool/OMNIbus サーバー :

```
%OMNIBUSHOME%¥bin¥nco_confpack -import ¥
-package nnmi.confpack ¥
-user <objectserver_administrator_username> ¥
-server <objectserver_name>
```

— *UNIX* Netcool/OMNIbus サーバー :

```
$OMNIBUSHOME/bin/nco_confpack -import ¥
-package nnmi.confpack ¥
-user <objectserver_administrator_username> ¥
-server <objectserver_name>
```

d *UNIX* のみ: $OMNIBROWSER が Mozilla Firefox ブラウザの場所に設定されていることを確認します。

HP NNMi Integration Module for Netcool Software の使用法

Netcool ソフトウェア用 NNMi 統合モジュールを有効にすると、NNMi は SNMPv2c トラップを Netcool/OMNIbus SNMP Probe に送信します。NNMi から転送されたコンテンツは Netcool/Webtop イベント リストと Netcool/OMNIbus イベント リストに表示されます。

統合モジュールがプローブに転送するトラップのタイプについては、508ページの「NNMi ノースバウンド インタフェースの使用法」を参照してください。トラップの内容と形式については、hp-nnmi-nbi.mib ファイルを参照してください。トラップ転送メカニズムの比較については、93 ページの「トラップおよびインシデント転送」を参照してください。

NNMi は、各管理イベント トラップ (または受信した SNMP トラップ) のコピーを 1 つだけ Netcool/OMNIbus SNMP Probe に送信します。NNMi はトラップをキューに入れません。NNMi がトラップを転送するときにプローブに接続できないと、そのトラップは失われます。

統合モジュールでは、Netcool イベント ビューアから NNMi コンソールへのリンクを使用できます。NNMi コンソール ビューを表示するには、NNMi ユーザーの資格を入力します。

579 ページの「HP NNMi Integration Module for Netcool Software の有効化」では、手順 4 と 手順 5 は、Netcool イベント ビューアに以下のメニュー項目を追加します。

- **ソース オブジェクト** - Netcool/OMNIbus で選択されると、オブジェクトの NNMi フォームを起動します。
- **ノード** - Netcool/OMNIbus で選択されると、ノードの NNMi フォームを起動します。
- **L2 隣接ノード** - Netcool/OMNIbus で選択されると、ノードの NNMi レイヤー 2 隣接ノード ビューを起動します。
- **L3 隣接ノード** - Netcool/OMNIbus で選択されると、ノードの NNMi レイヤー 3 隣接ノード ビューを起動します。

- **インシデントの詳細** - Netcool/OMNIbus で選択されると、NNMi インシデント フォームを起動します。

UNIX Netcool/OMNIbus サーバー :

- Mozilla Firefox は、Netcool/OMNIbus イベント リストからの NNMi ビューの起動に使用するデフォルトの Web ブラウザである必要があります。
- `$OMNIBROWSER` 環境変数は、Mozilla Firefox ブラウザの場所に設定されている必要があります。

HP NNMi Integration Module for Netcool Software の変更

Netcool ソフトウェア用 NNMi 統合モジュール設定パラメータを変更するには、以下の手順を実行します。

1. NNMi コンソールで、**[HP NNMi Integration Module for Netcool Software 設定アクション]** フォームを開きます (**[統合モジュールの設定] > [Netcool]**)。
2. Netcool ソフトウェア用 NNMi 統合モジュールの **[有効化 / 無効化]** 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は、585 ページの「HP NNMi Integration Module for Netcool Software 転送先フォームのリファレンス」を参照してください。
5. フォームの上にある **[有効にする]** チェック ボックスがオンになっていることを確認し、フォームの下にある **[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 Integration Module for Netcool Software 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。

Netcool/OMNIbus SNMP Probe への NNMi 管理イベントの転送を解除するには、以下の手順を実行します。

1. NNMi コンソールで、**[HP NNMi Integration Module for Netcool Software 設定アクション]** フォームを開きます (**[統合モジュールの設定] > [Netcool]**)。
2. Netcool ソフトウェア用 NNMi 統合モジュールの **[有効化 / 無効化]** 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. **[HP NNMi Integration Module for Netcool Software デスティネーション]** フォームで、フォームの上にある **[有効にする]** チェック ボックスをオフにし、フォームの下にある **[送信]** をクリックします。

   変更はただちに有効になります。
5. システム リソースを節約するには、転送先が無効になっている間、Netcool/OMNIbus SNMP Probe をシャットダウンします。

永久的に統合を無効にするには、以下も実行します。

- プローブのドキュメントに記載されているとおり、Netcool/OMNIbus SNMP Probe をアンインストールします。
- Netcool/Webtop および Netcool/OMNIbus イベント リスト設定から NNMi メニュー項目を削除します。

HP NNMi Integration Module for Netcool Software のトラブルシューティング

Netcool/OMNIbus は転送された NNMi 管理イベントを受信しない

Netcool イベント ビューアに、NNMi から受信するトラップが含まれていない場合は、以下の手順を実行します。

1. Netcool/OMNIbus SNMP Probe がトラップを受信していることを確認します。
   a. プローブが Netcool/OMNIbus サーバーにメッセージを送信できることを確認します。
   b. プローブ マスター ルール ファイルに `nnmi.include.rules` ファイルの内容が含まれていることを確認します。
   c. マスター ルール ファイルの構文を確認します。
   d. プローブ ログ ファイルに、ルール ファイルのロードに関する問題がないことを確認します。
   e. プローブ ログ ファイルで NNMi トラップがプローブに届いているかどうかを確認します。
   f. プローブ ログ ファイルで、プローブが受信トラップを処理しているか、ドロップしているかを確認します。

   プローブのトラブルシューティングについては、Netcool/OMNIbus ドキュメントを参照してください。
2. NNMi が Netcool/OMNIbus SNMP Probe 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、512 ページの「NNMi ノースバウンド インタフェースのトラブルシューティング」を参照してください。

転送された NNMi 管理イベントの中に Netcool/OMNIbus が受信しないものがある

Netcool イベント ビューアに 1 つ以上の NNMi 管理イベント トラップが表示されない場合は、以下の手順を実行します。

1. Netcool/OMNIbus SNMP Probe マスター ルール ファイルに `nnmi.include.rules` ファイルの内容が含まれていることを確認します。

2 Netcool/OMNIbus が実行していることを確認します。

Netcool/OMNIbus サーバーがシャットダウンした場合、Netcool/OMNIbus SNMP Probe は受信したトラップをキューに追加します。Netcool/OMNIbus サーバーが利用できるようになると、プローブはキューに追加されたトラップを転送します。

NNMi によるトラップのキューへの追加と転送は、プローブに依存します。プローブがシャットダウンすると、転送されたトラップは喪失してしまいます。

3 NNMi プロセスが実行中であることを確認します。

レイヤー 2 接続に対して NNMi フォームを起動するとエラーが発生する

NNMi 管理サーバーのソース オブジェクトがレイヤー 2 接続である場合、管理者以外のロールを持つ NNMi ユーザーは、Netcool イベント ビューアの **[ソース オブジェクト]** メニュー項目から直接 NNMi フォームを開くことはできません。代わりに、Netcool イベント ビューアで **[L2 隣接ノード]** メニュー項目を使用して NNMi に接続し、その後でレイヤー 2 隣接ノード ビューの接続をダブルクリックします。

HP NNMi Integration Module for Netcool Software 転送先フォームのリファレンス

[HP NNMi Integration Module for Netcool Software デスティネーション] フォームには、NNMi と Netcool/OMNIbus SNMP Probe 間の通信設定パラメータが含まれています。有効な Netcool ソフトウェア用 NNMi 統合モジュールライセンスが NNMi 管理サーバーにインストールされている場合、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利用できます (**[HP NNMi Integration Module for Netcool Software 設定アクション]** フォームで、Netcool ソフトウェア用 NNMi 統合モジュールの **[有効化 / 無効化]** 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。)

管理者ロールを持つ NNMi ユーザーのみが **[HP NNMi Integration Module for Netcool Software デスティネーション]** フォームにアクセスできます。

[HP NNMi Integration Module for Netcool Software 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。

- 585 ページの「Netcool/OMNIbus SNMP Probe の接続」
- 586 ページの「統合コンテンツ」
- 589 ページの「転送先ステータス情報」

統合設定への変更を適用するには、**[HP NNMi Integration Module for Netcool Software デスティネーション]** フォームの値を更新し、**[送信]** をクリックします。

Netcool/OMNIbus SNMP Probe の接続

表 67 には、Netcool/OMNIbus SNMP Probe への接続設定パラメータがリストされています。

表 67　Netcool/OMNIbus SNMP Probe 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。これは、Netcool/OMNIbus SNMP Probe が SNMP トラップを NNMi から受信するシステムです。 統合は、以下のプローブ ホストの識別方法をサポートしています。 • **NNMi FQDN** NNMi が NNMi 管理サーバーのプローブへの接続を管理しているため、**[ホスト]** フィールドは読み取りのみです。 これがデフォルトの推奨設定です。 • **ユーザー ループバック** NNMi が NNMi 管理サーバーのプローブへの接続を管理しているため、**[ホスト]** フィールドは読み取りのみです。 • **その他** このオプションは使用しないでください。 **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にアプリケーション フェイルオーバーが統合に与える影響については、513 ページの「アプリケーション フェールオーバーと NNMi ノースバウンド インタフェース」を参照してください。

表 67　Netcool/OMNIbus SNMP Probe の接続情報 (続く)

フィールド	説明
ポート	Netcool/OMNIbus SNMP Probe が SNMP トラップを受信する UDP ポート。 そのプローブ固有のポート番号を入力します。 ポートを特定するには、NNMi 管理サーバーにあるプローブの `mttrapd.properties` ファイルを確認します。 **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	Netcool/OMNIbus SNMP Probe がトラップを受信するための読み取りのみのコミュニティ文字列。 プローブの設定で、受信した SNMP トラップに特定のコミュニティ文字列を指定する必要がある場合は、その値を入力します。 プローブの設定で、特定のコミュニティ文字列を必要としない場合は、デフォルトの値である `public` を使用します。

統合コンテンツ

表 68 には、Netcool/OMNIbus SNMP Probe に Netcool ソフトウェア用 NNMi 統合モジュールが送信する内容を設定するパラメータがリストされています。

表 68　Netcool ソフトウェア用 NNMi 統合モジュールコンテント設定情報

フィールド	説明
インシデント	インシデント転送の指定。 • **管理** NNMi は、NNMi が生成した管理イベントのみを Netcool/OMNIbus SNMP Probe に転送します。 これがデフォルト設定です。 • **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 トラップのみをプローブに転送します。 • **両方** 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 トラップの両方をプローブに転送します。 NNMi は、転送先が有効になるとすぐにインシデントの転送を開始します。 詳細については、508 ページの「インシデント転送」を参照してください。

表 68　Netcool ソフトウェア用 NNMi 統合モジュールコンテント設定情報 (続く)

フィールド	説明
ライフサイクル状態の変化	インシデント変更通知の仕様。 • **エンハンスド解決済み** 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 Netcool/OMNIbus SNMP Probe に送信します。 これがデフォルト設定です。 • **状態変化** 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個々に、インシデント ライフサイクル状態変化トラップをプローブに送信します。 • **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プローブに送信します。さらに、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 ライフサイクル状態変化トラップをプローブに送信します。 **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。 詳細については、509 ページの「インシデント ライフサイクル状態変化通知」を参照してください。
相関処理	インシデント相関処理通知の仕様。 • **なし** NNMi は、NNMi 因果関係分析によって判明したインシデント相関処理について、Netcool/OMNIbus SNMP Probe 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相関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相関処理ごとに、トラップを 1 つ送信します。 詳細については、509 ページの「インシデント相関処理通知」を参照してください。
削除	インシデント削除の仕様。 • **送信しない** NNMi は、NNMi でインシデントを削除しても、Netcool/OMNIbus SNMP Probe に通知しません。 これがデフォルト設定です。 • **送信** NNMi は、NNMi で削除されるインシデントごとに、削除トラップをプローブに送信します。 詳細については、510 ページの「インシデント削除通知」を参照してください。

表 68　Netcool ソフトウェア用 NNMi 統合モジュールコンテント設定情報 (続く)

フィールド	説明
NNMi コンソール アクセス	Netcool イベント ビューアから NNMi コンソールを参照するときの URL の接続プロトコル仕様。NNMi が Netcool/OMNIbus SNMP Probe に送信するトラップは、NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2) に NNMi URL を含めます。 設定ページのデフォルトは、NNMi 設定と一致する設定になります。 NNMi コンソールが HTTP と HTTPS 両方の接続を承認するよう設定されている場合、NNMi URL で HTTP 接続プロトコルの指定を変更できます。たとえば、Netcool ユーザーがインターネットを使用している場合、HTTP を介して Netcool イベント ビューアから NNMi コンソールにアクセスするように設定できます。Netcool イベント ビューアから NNMi コンソールに接続するプロトコルを変更するには、**[HTTP]** オプションまたは **[HTTPS]** オプションを必要に応じて選択します。
Incident Filter(インシデント フィルタ)	Netcool/OMNIbus SNMP Probe に送信されたイベントを統合でフィルタするときのオブジェクト ID (OID) のリスト。各フィルタ 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。 以下のオプションの 1 つを選択します。 • **なし** NNMi はすべてのイベントをプローブに送信します。 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。 インシデント フィルタを指定します。 • フィルタ 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 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。 詳細については、510 ページの「イベント転送フィルタ」を参照してください。

転送先ステータス情報

表 69 には、Netcool ソフトウェア用 NNMi 統合モジュールの転送先に使用する読み取りのみのステータス情報がリストされています。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 69　Netcool ソフトウェア用 NNMi 統合モジュール ステータス情報

フィールド	説明
トラップ転送先 IP アドレス	Netcool/OMNIbus SNMP Probe 転送先 ホスト名が解決する IP アドレス。 この値は、このプローブ 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 Netcool/OMNIbus SNMP Probe に送信するトラップは、sysUptime field (1.3.6.1.2.1.1.3.0) にこの値を含めます。 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 Netcool/OMNIbus SNMP Probe に送信するトラップは、NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2) にこの値を含めます。 この値は、このノースバウンド転送先に固有です。

xMatters (以前の AlarmPoint)

xMatters, Inc. の xMatters は対話型のアラート生成プラットフォームで、重要なイベントを収集して内容を補強し、任意の通信デバイスによって適切なユーザーにそれらのイベントを転送し、そのユーザーが問題点の解決したり、エスカレートしたり、他のユーザーの支援を得たりすることができるように設計されています。

xMatters は、統合により、自動化エンジンまたは HP Network Node Manager i Software (NNMi) などのインテリジェント アプリケーションの音声関連のインタフェースとして使用できます。注意が必要なイベントを NNMi が検出すると、xMatters から、適切な担当者、ベンダー、ユーザーに電話をかけるか、またはポケベル、インスタント メッセージ、電子メールなどを送信します。

また、xMatters は、複数のデバイス、通信メディア、および担当者を通してエスカレートし、いずれかの担当者が責任を受け入れるか、またはイベントを解決するまで、その処理を継続します。xMatters により、通知先のユーザーは、NNMi と瞬時に双方向の通信を行うことができます。応答は NNMi 管理サーバーで即時に処理されるため、イベントのリモート解決が実現できます。

すべての xMatters Enterprise ライセンスに含まれる xMatters mobile access は、xMatters プラットフォームの機能を拡張して、重要なアプリケーションへのモバイル Web アクセスを提供します。xMatters mobile access により、モバイル デバイスから企業のアプリケーションにアクセスして、チケット情報を入手および変更し、ダッシュボードを監視し、洗練されたレポートを生成できます。

xMatters および xMatters mobile access の購入については、HP 営業担当にお尋ねになるか、**sales@xmatters.com** をご覧ください。

この章では、以下の使用可能な統合について説明します。

- HP NNMi-xMatters 統合
- HP NNMi-xMatters mobile access 統合

HP NNMi-xMatters 統合

HP NNMi-xMatters 統合について

NNMi を使用してネットワーク デバイスの監視と管理を担当するネットワーク運用スタッフは、NNMi 環境に xMatters を統合することにより、インテリジェントなアラート生成手段を獲得し、個人用通信ツールと NNMi 間の双方向通信メカニズムを利用できます。

HP NNMi-xMatters 統合では、NNMi インシデント タイプを設定することにより、NNMi から xMatters へのイベント通知をサポートします。また、原因となったインシデントの受諾、その優先度の変更、注釈の追加など、xMatters から NNMi へのインバウンド アクションもサポートします。

各 NNMi 管理サーバーは、xMatters、xMatters mobile access、または xMatters と xMatters mobile access の両方と統合できます。

値

HP NNMi-xMatters 統合により、音声、電子メール、ポケベル、その他のデバイスを利用して、適切な技術者に直接通知することができます。イベント解決の担当者は、障害に関する情報を受信し、イベントの受諾、無視、注釈追加、優先度変更などをリアルタイムで判断できます。

受信者がリモート デバイスからの応答を選択した後、xMatters は NNMi インシデントをリアルタイムで更新します。このようなメカニズムの利点は、処理が即座に行われることです。すなわち、運用スタッフが障害または誤動作に気付き、適切な担当者を判断し、その担当者に手動で通知するよりも、はるかに迅速に処理できます。単純なアクションで各種デバイスのインシデントを更新できるため、イベント解決の担当者にとっては、多くの問題を処理したり、インシデントの現在のステータスを他のチーム メンバーに通知するための高速な手段となります。

処理中、xMatters は、すべての通知、応答、アクションをログに記録します。また、xMatters は、元の NNMi インシデントに対してステータス情報を注釈として自動的に付加します。

xMatters 製品には、各ジョブに適切な担当者を割り当てるための、セルフ サービスの Web ベース ユーザー インタフェース機能が備わっています。また、xMatters には、機能が強化されたサブスクリプション パネルもオプションで用意されており、これを使用することにより、NNMi インシデントに対して管理されたサブスクリプションと自動サブスクリプションの両方を行うことができます。

xMatters の機能限定版である xMatters lite は、NNMi の特定バージョンで使用できます。xMatters lite for HP NNMi の機能セットは限定されており、NNMi 統合用に設定済みの状態で出荷されます。xMatters lite は、xMatters 製品ファミリーを初めて使用する場合に最適な製品です。xMatters lite は、音声や負荷分散機能が不要な小規模な生産環境に適しています。

統合製品

この章の情報は、以下の製品に当てはまります。

- xMatters

サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- AlarmPoint Java Client
- NNMi 9.10

NNMi 統合実施可能ライセンスは、NNMi と xMatters 製品のいずれかとの統合では必要*ありません*。

ドキュメント

HP NNMi-xMatters 統合については、この統合に付属する『AlarmPoint 対応 HP Network Node Manager i-series 統合ガイド』で詳しく説明されています。

xMatters のドキュメント スイートでは、xMatters 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、以下の xMatters Customer Connect サイトからダウンロードできます。

https://connect.xmatters.com

『*AlarmPoint Express for HP NNMi Quick Start Guide*』では、xMatters の特徴についての概要が説明されています。このガイドでは、HP NNMi-xMatters lite 統合のインストール方法、設定方法、および管理方法を説明しています。

HP NNMi-xMatters 統合の有効化

NNMi との両方の xMatters 統合を実装する場合は、まず HP NNMi-xMatters 統合を有効にし、それから HP NNMi-xMatters mobile access 統合を有効にすることを推奨します。

xMatters for NNMi 統合のインストール方法と設定方法の手順の概要は、以下のとおりです。詳細については、『AlarmPoint 対応 HP Network Node Manager i-series 統合ガイド』を参照してください。

1. AlarmPoint Java Client を NNMi 管理サーバーにインストールします。
2. AlarmPoint Java Client 用の NNMi 固有の統合スクリプトをインストールします。
3. xMatters Web サーバーと xMatters Application サーバーに、Web Services Library をインストールします。
4. *オプション*。xMatters Web サーバーに、NNMi 用の xMatters サブスクリプション パネルをインストールします。
5. xMatters Developer IDE を使って、NNMi 用の xMatters アクション スクリプトをインストールします。
6. xMatters Application サーバーに、統合音声ファイルをインストールします。
7. xMatters に、イベント ドメイン (および、オプションでサブスクリプション ドメイン) を設定します。
8. Web Services Client ロールの NNMi ユーザーを設定します。
9. xMatters スクリプトをトリガする、NNMi インシデント タイプを設定します。

10 統合によって、xMatters 通知に NNMi インシデント パラメータが挿入されることと、xMatters が NNMi インシデントを正しく更新することを検証します。

HP NNMi-xMatters 統合の使用法

NNMi と xMatters は、相互動作して、ユーザーに通知を配信し、NNMi にその応答を戻します。NNMi は、ネットワーク内に問題点 (たとえば、インシデント) を検出すると、以下の処理を行います。

1 NNMi は、問題点を説明するパラメータ (たとえば、影響を受けるコンピュータと状況) を伴って、AlarmPoint Client (APClient) を呼び出します。

2 APClient は、AlarmPoint エージェント (APAgent) に情報を送信します。

3 APAgent は問題点の詳細情報を xMatters に送信し、xMatters はその情報を適切な受信者に通知します。

4 受信者は、表 70 に示すいずれかのアクションを行うことによって通知に応答します。Web サービス コールを通じて、受信者による受諾、注釈付加、または優先度変更に従って、NNMi が更新されます。

表 70　受信したインシデント通知に対する応答方法

アクション	説明
受諾	ユーザーはインシデント所有権を取得し、それ以上他のユーザーに対して通知されることのないようにします。 例外は、サービス障害について報告するサブスクリプション FYI 通知です。これらの通知は、問題が解決されるまで送信され続けます。
無視	現在のユーザーへの通知を停止します。
優先度を上げる	NNMi でのインシデントの優先度を 1 レベル上げます。(音声のみ)
優先度を下げる	NNMi でのインシデントの優先度を 1 レベル下げます。(音声のみ)
優先度を最上位に設定する	インシデントの優先度を最上位に設定します。(電子メール、BES、およびブラウザのみ)
優先度を高に設定する	インシデントの優先度を高に設定します。(電子メール、BES、およびブラウザのみ)
優先度を中に設定する	インシデントの優先度を中に設定します。(電子メール、BES、およびブラウザのみ)
優先度を低に設定する	インシデントの優先度を低に設定します。(電子メール、BES、およびブラウザのみ)
注釈付加	NNMi インシデントの [注] フィールドにユーザーがメッセージを入力できるようにします。(非 HTML 電子メールのみ)

HP NNMi-xMatters 統合の無効化

統合を無効にするには、統合の実行可能アーカイブによってインストールされたコンポーネントを削除します。

xMatters 配備の削除については、『AlarmPoint 対応 HP Network Node Manager i-series 統合ガイド』を参照してください。

HP NNMi-xMatters 統合のトラブルシューティング

統合の最適化と拡張、および既知の問題については、『AlarmPoint 対応 HP Network Node Manager i-series 統合ガイド』を参照してください。

HP NNMi-xMatters mobile access 統合

HP NNMi-xMatters mobile access 統合について

NNMi 環境に xMatters mobile access を組み込むことにより、ネットワーク運用スタッフは、モバイル デバイスの Web ブラウザで NNMi のインシデントとやり取りできます。

各 NNMi 管理サーバーは、xMatters、xMatters mobile access、または xMatters と xMatters mobile access の両方と統合できます。

値

HP NNMi-xMatters mobile access 統合により、NNMi オペレータは、モバイル デバイスの Web ブラウザを使用して NNMi のインシデントとリアルタイムでやり取りできます。

- 現在のインシデントについて NNMi に対してクエリを実行する
- インシデントの詳細を表示する
- ステータス、ライフサイクル状態、または割り当てられた NNMi オペレータなど、インシデントのプロパティを変更する

統合製品

この章の情報は、以下の製品に当てはまります。

- xMatters mobile access

  サポートされるバージョンは、NNMi システムおよびデバイスのサポート マトリックスにリストされています。

- xMatters integration agent
- NNMi 9.10

  NNMi 統合実施可能ライセンスは、NNMi と xMatters 製品のいずれかとの統合では必要ありません。

ドキュメント

HP NNMi-xMatters mobile access 統合については、この統合に付属する『AlarmPoint Mobile Gateway 対応 HP Network Node Manager i-series Software 統合ガイド』で詳しく説明されています。

xMatters のドキュメント スイートでは、xMatters 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、以下の xMatters Customer Connect サイトからダウンロードできます。

https://connect.xmatters.com

HP NNMi-xMatters mobile access 統合の有効化

NNMi との両方の xMatters 統合を実装する場合は、まず HP NNMi-xMatters 統合を有効にし、それから HP NNMi-xMatters mobile access 統合を有効にすることを推奨します。593 ページの「HP NNMi-xMatters 統合の有効化」を参照してください。

xMatters mobile access for NNMi 統合のインストール方法と設定方法の手順の概要は、以下のとおりです。詳細については、『AlarmPoint Mobile Gateway 対応 HP Network Node Manager i-series Software 統合ガイド』を参照してください。

HP NNMi-AlarmPoint 統合が初期バージョンの NNMi を対象に設定された場合は、統合設定に影響を与えずに、NNMi 9.0x から NNMi 9.10 にアップグレードできます。xMatters のバージョンが 4.0 以降であることを確認してください。

1. xMatters integration agent を xMatters サーバーにインストールします。
2. Web Service Library を xMatters integration agent サーバーと Web サーバーにインストールします。
3. xMatters mobile access を xMatters Web サーバーにインストールします。
4. NNMi Integration Service をインストールします。
5. Web Service Client ロールの NNMi ユーザーを作成します。
6. xMatters で、イベント ドメイン (HP NNMi-xMatters 統合がまだ設定されていない場合) と Integration Service を設定します。
7. xMatters mobile access と NNMi の間のやり取りを確認します。

HP NNMi-xMatters mobile access 統合の使用法

HP NNMi-xMatters mobile access 統合により、モバイル Web ブラウザで、インシデントに関して以下のアクションを実行できます。

- 注を追加する
- 優先度を更新する
- ライフサイクル状態を更新する
- 割り当て先オペレータを更新する
- インシデントの詳細のほとんどを表示する (xMatters mobile access 管理者が表示可能にした情報)
- ソース オブジェクトおよびノードのクイック ビューを表示する

統合の使用法の詳細については、『AlarmPoint Mobile Gateway 対応 HP Network Node Manager i-series Software 統合ガイド』および『*xMatters (alarmpoint) mobile access Guide*』を参照してください。

HP NNMi-xMatters mobile access 統合の無効化

統合を無効にするには、統合の実行可能アーカイブによってインストールされたコンポーネントを削除します。

xMatters mobile access 配備の削除については、『AlarmPoint Mobile Gateway 対応 HP Network Node Manager i-series Software 統合ガイド』を参照してください。

HP NNMi-xMatters mobile access 統合のトラブルシューティング

統合の最適化と拡張、および既知の問題については、『AlarmPoint Mobile Gateway 対応 HP Network Node Manager i-series Software 統合ガイド』を参照してください。

追加情報

この項では以下の付録について説明します。

- NNMi 環境変数
- NNMi 9.10 およびウェルノウン ポート
- 設定変更の提案

NNMi 環境変数

HP 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
- 他の使用可能な環境変数

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 2008*:
  - `%NnmInstallDir%`: `<drive>¥Program Files¥HP¥HP BTO Software`
  - `%NnmDataDir%`: `<drive>¥ProgramData¥HP¥HP BTO Software`

  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。

  最初に NNMi 8.00 をインストールした場合、ご使用のシステムでは、604 ページの「」で説明しているようにこれらの環境変数で異なる値を使用しています。

- UNIX:
  - `$NnmInstallDir`: `¥opt¥OV`
  - `$NnmDataDir`: `¥var¥opt¥OV`

  UNIX システムでは、これらの環境変数を使用する場合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、601 ページの「他の使用可能な環境変数」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環境変数を設定するスクリプトが用意されています。

最初に NNMi 8.00 を Windows オペレーティング システムにインストールした場合は、604 ページの「」を参照してください。

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:「`C:¥Program Files¥HP¥HP BTO Software¥bin¥nnm.envvars.bat`」
- UNIX: `. /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 71 (Windows) または 表 72 (UNIX) 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 71　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¥nnm¥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¥nonOV¥jboss¥nms
%NNM_JBOSS_DEPLOY%	C:¥Program Files (x86)¥HP¥HP BTO Software¥nonOV¥jboss¥nms¥server¥nms¥deploy
%NNM_JBOSS_LOG%	C:¥Program Files (x86)HP¥HP BTO Software¥nonOV¥jboss¥nms¥server¥nms¥log
%NNM_JBOSS_ROOT%	C:¥Program Files (x86)¥HP¥HP BTO Software¥nonOV¥jboss¥nms
%NNM_JBOSS_SERVERCONF%	C:¥Program Files (x86)¥HP¥HP BTO Software¥nonOV¥jboss¥nms¥server¥nms
%NNM_JRE%	C:¥Program Files (x86)¥HP¥HP BTO Software¥nonOV¥jdk¥nnm
%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

表 71　**Windows OS** での環境変数のデフォルトの場所 (続く)

変数	Windows (例)
%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 72　**UNIX OS** での環境変数のデフォルトの場所

変数	HP-UX
$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/nnm/bin/java
$NNM_JAVA_DIR	/opt/OV/java
$NNM_JAVA_PATH_SEP	:
$NNM_JBOSS	/opt/OV/nonOV/jboss/nms
$NNM_JBOSS_DEPLOY	/opt/OV/nonOV/jboss/nms/server/nms/deploy
$NNM_JBOSS_LOG	/opt/OV/nonOV/jboss/nms/server/nms/log
$NNM_JBOSS_ROOT	/opt/OV/nonOV/jboss/nms
$NNM_JBOSS_SERVERCONF	/opt/OV/nonOV/jboss/nms/server/nms
$NNM_JRE	/opt/OV/nonOV/jdk/nnm
$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

NNMi 9.10 およびウェルノウン ポート

表 73 に、NNMi が使用する管理サーバーのポートを示します。NNMi はそれらのポートで待機します。ポートの競合が発生した場合は、「*設定の変更*」列の説明に従ってそのポート番号のほとんどを変更できます。詳細については、*nnm.port.4* リファレンス ページまたは UNIX のマンページを参照してください。

アプリケーションフェイルオーバーを正しく機能させるために、TCP ポート 7800-7810 をオープンにしてください。アプリケーション フェイルオーバーが正しく機能するには、アクティブ NNMi 管理サーバーとスタンバイ NNMi 管理サーバーは相互のネットワーク アクセスに制限のないことが必要です。

.

表 73　NNMi 管理サーバー で使用されるポート

ポート	タイプ	名前	目的	設定の変更
80	TCP	`jboss.http.port`	デフォルト HTTP ポート - Web UI と Web サービスで使用	`nms-local.properties` ファイルを変更します インストール時に変更することもできます
162	UDP	`trapPort`	SNMP トラップ ポート	`nnmtrapconfig.ovpl` Perl スクリプトを使用して変更します。詳細については、*nnmtrapconfig.ovpl* リファレンス ページまたは UNIX のマンページを参照してください。
443	TCP	`jboss.https.port`	デフォルトのセキュア HTTPS ポート (SSL) - Web UI と Web サービスで使用	`nms-local.properties` ファイルを変更します
1098	TCP	`jboss.rmi.port`	RMI ネーム サービスのデフォルト ポート	`nms-local.properties` ファイルを変更します
1099	TCP	`jboss.jnp.port`	デフォルトのブートストラップ JNP サービス ポート (JNDI プロバイダ)	`nms-local.properties` ファイルを変更します
3873	TCP	`jboss.ejb3.port`	デフォルトの EJB3 リモート コネクタ ポート	`nms-local.properties` ファイルを変更します
4444	TCP	`jboss.jrmp.port`	デフォルトの RMI オブジェクト ポート (JRMP 呼び出し元)	`nms-local.properties` ファイルを変更します
4445	TCP	`jboss.pooled.port`	デフォルトの RMI プール済み呼び出し元ポート	`nms-local.properties` ファイルを変更します

表 73　NNMi 管理サーバー (続く) で使用されるポート

ポート	タイプ	名前	目的	設定の変更
4446	TCP	jboss.socket.port	デフォルトの RMI リモート サーバー コネクタ ポート	nms-local.properties ファイルを変更します
4457	TCP	jboss.bisocket.port	デフォルトのメッセージング バイソケット コネクタ	nms-local.properties ファイルを変更します
4458	TCP	jboss.jmsControl.port	デフォルトの JMS 制御ポート、グローバル ネットワーク管理通信で使用	nms-local.properties ファイルを変更します
4459	TCP	jboss.sslbisocket.port	デフォルトのメッセージング バイソケット コネクタ、セキュアなグローバル ネットワーク管理通信で使用	nms-local.properties ファイルを変更します
4460	TCP	jboss.ssljmsControl.port	デフォルトの JMS 制御ポート、セキュアなグローバル ネットワーク管理通信で使用	nms-local.properties ファイルを変更します
5432	TCP		Postgres ポート	設定不可
7800-7810	TCP		アプリケーションのフェイルオーバーで使用する JGroups ポート	nms-cluster.properties ファイルを変更します
8083	TCP	jboss.ws.port	デフォルトの jboss Web サービス ポート	nms-local.properties ファイルを変更します
8886	TCP	OVsPMD_MGMT	NNMi ovspmd (プロセス マネージャ) 管理ポート	/etc/services ファイルを変更します
8887	TCP	OVsPMD_REQ	NNMi ovsmpd (プロセス マネージャ) 要求ポート	/etc/services ファイルを変更します

表 74 に、他のシステムとの通信で NNMi が使用するポートの一部を示します。ファイアウォールによって NNMi がこれらのシステムから分断される場合は、そのファイアウォールでこれらのポートの多くを開く必要があります。実際のポート セットは、NNMi で使用するように設定した統合セットと、それらの統合の設定方法に応じて異なります。4 列目が*クライアント*であれば NNMi はそのポートに接続または送信し、4 列目が *サーバー*であれば NNMi はそのポートで待機します。

表 74　NNMi 管理サーバーと他のシステム の通信で使用されるポート

ポート	タイプ	目的	クライアント、サーバー
80	TCP	NNMi のデフォルト HTTP ポート、Web UI と Web サービスで使用	サーバー
80	TCP	NNMi が他のアプリケーションに接続するときのデフォルト HTTP ポート。実際のポートは NNMi の設定によって異なります。	クライアント
161	UDP	SNMP 要求ポート	クライアント
162	UDP	SNMP トラップ ポート - NNMi が受信するトラップ	サーバー

表 74　NNMi 管理サーバーと他のシステム (続く) の通信で使用されるポート

ポート	タイプ	目的	クライアント、サーバー
162	UDP	SNMP トラップ ポート。トラップ転送、Northbound インタフェース、または NetCool 統合	クライアント
389	TCP	デフォルト LDAP ポート	クライアント
395	UDP	nGenius Probe SNMP トラップ ポート	クライアント
443	TCP	NNMi が他のアプリケーションに接続するときのデフォルトのセキュア HTTPS ポート、実際のポートは NNMi の設定によって異なります。 HP OM on Windows のデフォルト HTTPS ポート	クライアント
443	TCP	デフォルトのセキュア HTTPS ポート、Web UI と Web サービスで使用	サーバー
636	TCP	デフォルトのセキュア LDAP ポート (SSL)	クライアント
1741	TCP	デフォルトの CiscoWorks LMS Web サービス ポート	クライアント
4457	TCP	グローバル ネットワーク管理通信で使用するデフォルトのメッセージング バイソケット コネクタ。グローバル マネージャからリージョナル マネージャに対して接続を行います。	クライアント、サーバー
4458	TCP	グローバル ネットワーク管理通信で使用するデフォルトの JMS 制御ポート。グローバル マネージャからリージョナル マネージャに対して接続を行います。	クライアント、サーバー
4459	TCP	セキュアなグローバル ネットワーク管理通信で使用するデフォルトのメッセージング バイソケット コネクタ。グローバル マネージャからリージョナル マネージャに対して接続を行います。	クライアント、サーバー
4460	TCP	セキュアなグローバル ネットワーク管理通信で使用するデフォルトの JMS 制御ポート。グローバル マネージャからリージョナル マネージャに対して接続を行います。	クライアント、サーバー
7800-7810	TCP	アプリケーションのフェイルオーバーで使用する JGroups ポート	クライアントとサーバー
8004	TCP	別の Web サーバーがすでにポート 80 を使用している場合の NNMi のデフォルト HTTP ポート。Web UI と Web サービスで使用。NNMi 管理サーバーの実際の HTTP ポートを検証します。	サーバー
8080	TCP	NNMi と同じシステムにインストールされている場合に、NA に接続するときのデフォルト HTTP ポート。 HP UCMDB Web サービスのデフォルト HTTPS ポート	クライアント
8443 または 8444	TCP	HP OM for UNIX に接続するときのデフォルト HTTP ポート	クライアント
9300	TCP	NNM iSPI for Performance に接続するときのデフォルト HTTP ポート	クライアント
50000	TCP	SIM に接続するときのデフォルト HTTPS ポート	クライアント

検出のために ICMP 障害ポーリングまたは ping スィープを使用するように NNMi を設定する場合は、ICMP パケットを通過させるようにファイアウォールを設定してください。

NNMi-HP OM 統合の Web サービス方式は、ファイアウォールを介して機能することはありませんが、Northbound インタフェースを使用する NNMi-HP OM 統合はファイアウォールを介して機能します。

グローバル ネットワーク管理機能を使用する場合は、グローバル NNMi 管理サーバーから地域 NNMi 管理サーバーに対して、表 75 に示すウェルノウン ポートがアクセス可能になっている必要があります。グローバル ネットワーク管理機能では、TCP アクセス用にグローバル NNMi 管理サーバーからリージョナル NNMi 管理サーバーに対して、これらのポートが開いている必要があります。リージョナル NNMi 管理サーバーが逆に、グローバル NNMi 管理サーバーに対してソケットを開くことはありません。

表 75　グローバル ネットワーク管理で必須のアクセス可能ソケット

セキュリティ	パラメータ	TCP ポート
非 SSL	jboss.http.port	80
	jboss.bisocket.port	4457
	jboss.jmsControl.port	4458
SSL	jboss.https.port	443
	jboss.sslbisocket.port	4459
	jboss.ssljmsControl.port	4460

設定変更の提案

パフォーマンス改善のための一般的なアクションとその実行方法。

メッセージおよび解決方法

メッセージ : データベース プールに使用可能な接続が *number* あります。

解決方法 : これは、データベース プールが大量に使用されていることを意味する警告です。短時間だけ表示される場合は、NNMi の負荷が高い状態にあることを示している可能性があります。頻繁に表示される場合は、パフォーマンスに問題があることを示している可能性があります。

メッセージ : データベース接続プールが使い果たされています。 NNM を直ちに再起動する必要があります。

解決方法 : これは、データベース プールが何らかの理由で使用できず、NNMi がデータベースにアクセスできないことを示す深刻なエラーです。問題解決のため、ovjboss を再起動するか、サポートに連絡する必要があります。

メッセージ : 見つからないデータベース接続が *number* 検出されました。 この問題を解決するために、なるべく早く NNM を再起動する必要があります。

解決方法 : これは、NNMi がデータベース プールに矛盾を検出したという警告です。この問題に対応するため、都合のよいときに ovjboss を再起動します。

メッセージ : ディスク場所 *location name* には *number*% の空き容量しかありません。

解決方法 : NNMi は、NNMi が使用するディスクの空きスペースが少なくなると、この警告を表示します。

メッセージ : 平均システム負荷は *number* です。

解決方法 : NNMi は、システムの負荷がしきい値を超えると、この警告を表示します。重要なアクティビティの最中に時折このメッセージが表示される場合は、無視してもかまいません。ただし、常に表示されるような場合は、大規模な環境でシステムの処理能力が落ちていないか、システム上のかなりのリソースを消費している他のプロセスがないかを調べる必要があります。

メッセージ : システムのスワップ領域が低下しています。残存空き容量は *number* です。

解決方法 : NNMi は、スワップ領域が低下した状態でシステムを実行中であることを NNMi が検出すると、このメッセージを表示します。空きスワップ領域を増やすか、スワップの使用を抑える必要があります。

メッセージ: 現在、NNMi 処理で許容オープン ファイル数の *number*% を使用しています。

解決方法 : このメッセージは、ファイル ハンドルが不足した状態で NNMi を実行していることを示します。1,000 未満のファイルを同時に開くことが予期されていますが、特定環境ではさらに多くのファイルを開く必要がある場合があります。開いているファイルのハンドルの数は増加し続けますが、これは製品の欠陥を示すことがあります。

メッセージ : NNMi CPU の使用率は 100% です。

解決方法 : これは、かなりの時間にわたって、objboss プロセスがシステムの CPU を 100% 消費していることを示します。負荷が短期間に大きくなることが予期されることがありますが、この警告が常に表示される場合は、システムの負荷処理能力が不足している可能性があります。

メッセージ : グローバル マネージャ ''*hostname*'' には、配信待機中の未処理メッセージが *number* あります。

解決方法 : これは、このシステムに接続されているグローバル マネージャがダウンしているか、十分な速さでメッセージを受信できないことを示しています。グローバル マネージャは、メンテナンスのために停止している場合、オンラインに戻ったときに復旧しますが、この数が数十万以上になる場合は、手動で消去する必要が生じる可能性があります (サポートに連絡)。

メッセージ : リージョナル マネージャ *regional name* への接続は停止しています。

解決方法 : リージョナル マネージャへの通信に割り込みがかかった場合の警告メッセージ。これは、短時間しか表示されない場合は心配する必要はありませんが、このメッセージが長時間表示される場合は、トラブルシューティングが必要になることがあります。この状態のとき、グローバル マネージャはリージョナル マネージャから状態の変更を受け取りません。

メッセージ : 現在、最大接続数 *number* のうち *number* が組み込みデータベースに開かれています。

解決方法 : このメッセージは、NNMi が使用する組み込みデータベースが、開いている接続数の制限に近づいていることを警告します。システムの負荷が過剰であること、またはインストールされている SPI が多すぎることを示している可能性があります。この数が最大値になる前に、SPI をシャットダウンするなどの対応を行うことをお勧めします。

メッセージ : メモリ領域 ''*region name*'' の使用率は *number*% です。

メッセージ : システムでは、''*number*'' コレクタ内で合計アップタイムの *collector name*% を消費しています。

解決方法 : これらのメッセージはどちらも、ovjboss のメモリが少ないことを示しています。特定のリージョンのメモリ設定について、その環境規模に対して推奨されるものかどうかを確認し、システムに使用可能なメモリがあれば、その数を増やす必要があります。

問題および解決策

問題：NNMi が、SNMP データおよび MIB 文字列を正しく解釈して表示しないことがある。

解決方法：これは、NNMi がどの文字セットを使用してこのデータを解釈するのかを認識しないことがあることが原因です。その結果、NNMi は、sysDescription、sysContact、その他のデータなど、一部の SNMP トラップからの文字化けした文字列およびその他の octetstring データを表示します。正しい文字セットを使用してこのデータを解釈することで解決できます。

不適切な文字セットを使用しているために、SNMP トラップおよびその他の octetstring データが文字化けしたテキストで表示されてしまう場合は、以下の手順を実行してください。

a 以下のファイルを編集します。

— *Windows:* `%NNM_PROPS%¥nms-jboss.properties`

— *UNIX:* `$NNM_PROPS/nms-jboss.properties`

b `#!com.hp.nnm.sourceEncoding=` で始まる行からコメント (`#!` 文字) を削除します。

c `nms-jboss.properties` ファイルの例を使用し、ご使用の環境で現在サポートされているソース エンコーディングをカンマで区切ったリストに `com.hp.nnm.sourceEncoding` JVM プロパティを設定します。この例は、Shift_JIS、EUC_JP、UTF-8、ISO-8859-1 の文字セットの組み合わせを示します。

d 変更を保存します。

e コマンド プロンプトから **ovstop ovjboss** を実行します。

f コマンド プロンプトから **ovstart ovjboss** を実行します。

g 変更内容をテストするには、疑わしいトラップを NNMi に再送信し、文字化け表示の問題が発生しないことを確認します。

バイナリ データ、または何らかの理由で解釈できないデータが文字化けテキストに含まれる場合は、以下の手順を実行し、16 進数形式で文字列を表示するように NNMi を設定します。

a 以下のファイルを編集します。

— *Windows*: `%NNMDATADIR%¥shared¥nnm¥conf¥nnmvbnosrcenc.conf`

— *UNIX*: `$NNMDATADIR/shared/nnm/conf/nnmvbnosrcenc.conf`

b NNMi が文字化けした形式で表示するトラップ OID、varbind OID 値の組み合わせを追加します。バイナリ データなど、NNMi にデコードさせない varbind 値からの組み合わせも追加します。`nnmvbnosrcenc.conf` ファイルの例をテンプレートとして使用し、組み合わせを設定します。これは、NNMi に 16 進値を使用してインシデント フォームのカスタム インシデント属性値を表示するように指示します。

c 変更を保存します。

d コマンド プロンプトから **ovstop ovjboss** を実行します。

e コマンド プロンプトから **ovstart ovjboss** を実行します。

f 変更内容をテストし、この変更によって、以前文字化けしていた文字列が 16 進数で表示されるようになったことを確認します。

問題：NNMi が、ホスト (NNMi 管理サーバー) と一致しないライセンス キーに関するメッセージを表示する。

解決方法 : これは、NNMi 管理サーバーの IP アドレスと一致しない IP アドレスで作成された NNMi ライセンス キーがインストールされた後に発生します。以下の手順で無効なライセンス キーを削除することで解決できます。

1 コマンド プロンプトで、以下のコマンドを開き、Autopass ユーザーインターフェースを開きます。

```
nnmlicense.ovpl NNM -gui
```

2 [Autopass] ウィンドウの左側で **[ライセンス キーの削除]** をクリックします。

3 無効なライセンス キーを選択します。

4 **[削除]** をクリックします。

NNM を影響される製品で置き換えて、その他の影響される NNMi 製品統合に手順 1 から手順 4 を繰り返します。たとえば NNM iSPI ネットワーク エンジニアリング ツールセット ソフトウェアに関連するライセンスを操作するには、以下のコマンドを使用して Autopass ユーザー インタフェースを開きます。

```
nnmlicense.ovpl iSPI-NET -gui
```

ライセンスの詳細については、115 ページの「NNMi ライセンスの取得」を参照してください。

問題：ESXi サーバー、および ESXi サーバーで動作する仮想マシンと仮想サーバーが NNMi マップに表示される。NNMi では、すべてのシステムが雲のシンボルで接続されて表示されます。これは、仮想マシンと仮想サーバーを含む ESXi サーバーを NNMi マップに表示しない場合に限り問題となります。

解決方法: 仮想マシンと仮想サーバーを含む ESXi サーバーが NNMi に表示されないようにするには、以下の手順を実行します。

1 NNMi コンソールを開きます。

2 削除するノードを表示しているトポロジ マップに移動し、ESXi サーバー、仮想マシン、および仮想サーバーを表すノードを削除します。

3 **[設定]** ワークスペースの **[検出の設定]** をクリックします。

4 **[自動検出ルール]** タブをクリックします。

5 新しい自動検出ルールを作成します。

6 比較的に小さい数値を [順序] フィールドに入力し、このルールの優先順位を高くします。[含められたノードを検出する] チェックボックスがオフになっていることを確認します。

7 このルールの新しい IP アドレス範囲を追加します。

8 ESXi サーバー、仮想マシン、および仮想サーバーを表すノードの場合は、このノードのそれぞれの IP アドレスまたは IP アドレス範囲を追加し、[範囲のタイプ] を [ルールにより無視] ではなく [ルールにより含める] に変更します。

9 **[保存して閉じる]** を 3 回クリックして作業を保存します。

この手順によって既存ノードが削除されるのではなく、除外された IP アドレス範囲内のノードが今後検出されなくなります。

問題：ESXi サーバーとノードではなく、Linux サーバーが NNMi マップに表示される。

解決方法： Net-SNMP エージェントが有効になっている Linux サーバーで VMWARE が導入されました。NNMi によって ESXi サーバーを検出して表示する場合は、ESXi サーバーとノードのベア メタル インストールを完了する必要があります。詳細については、http://www.vmware.com を参照してください。

問題: ESXi デバイスではなく、[SNMP なし] が NNMi マップに表示される。

解決方法：NNMi が ESXi サーバーとノードを検出してマッピングするためには、ESXi SNMP エージェントをインストールして有効にする必要があります。ESXi SNMP エージェントをアンインストールしたか無効にした可能性があります。これを解決するには、ESXi SNMP エージェントをインストールするか有効にします。詳細については、http://www.vmware.com を参照してください。

問題：NNMi で Oracle データベースを使用している。大きいノードグループを設定すると、ノードグループマップの生成中にエラーが発生する。

解決方法：これは、NNMi を以下のように設定した場合に生じる可能性があります。

- NNMi で Oracle データベースを使用している。
- 子ノードグループを含む最上位レベルのノードグループを作成している。
- いずれかの子ノードグループに 1000 以上のメンバーが含まれている。
- これらのノードグループの **[ノードグループマップの設定]** -> **[接続]** -> **[ノードグループ接続]** セクションで、以下のいずれか、あるいは両方を選択している。
  - **ノードからノードグループへ**
  - **ノード グループからノードグループへ**

これを修正するには、子ノードグループに含まれるメンバーを 1000 未満にするか、これらのノードグループの **[ノードグループマップの設定]** -> **[接続]** -> **[ノードグループ接続]** セクションで、**[ノードからノードグループへ]** または **[ノード グループからノードグループへ]** のいずれか、あるいは両方を選択しないようにします。

用語集

A

ARP キャッシュ

ARP (アドレス解決プロトコル) キャッシュは、データ リンク層 (OSI レイヤー 2) アドレスをネットワーク層 (OSI レイヤー 3) アドレスにマップするオペレーティング システム テーブルです。データ リンク層アドレスは通常は MAC アドレスですが、ネットワーク層アドレスは通常は IP アドレスです。ルールベースの検出 では、NNMi は、検出されたノードで ARP キャッシュ エントリ (ならびに他のテクニック) を使って、現在の検出ルールに照らしてチェックできる追加ノードを見つけます。

C

Causal Engine

因果関係ベースの方法を使って、根本原因解析 (RCA) をネットワーク現象に適用する NNMi テクノロジ。Causal Engine RCA をトリガするのは、状態ポーリング、SNMP トラップ、特定のインシデントの結果として検出された変更など、特定のオカレンスです。Causal Engine は RCA を使って、管理対象オブジェクトのステータスを調べ、これらオブジェクトに関する結論を明確化し、根本原因インシデントを生成します。

H

HA

高可用性を参照してください。

HA リソース グループ

HP ServiceGuard、Veritas Cluster Server、Microsoft Cluster Service などの最新の高可用性環境では、アプリケーションは、アプリケーション自体、その共有ファイル システム、仮想 IP アドレスのようなリソースの復合物として表わされます。リソースは *HA リソース グループ*で構成されます。これはクラスタ環境で実行中のアプリケーションを表します。

HP Network Node Manager i Software

ネットワーク管理の支援や統合のために設計された HP のソフトウェア商品です (短縮形は NNMi)。ネットワーク ノードの継続検出、イベントの監視、ネットワーク障害管理といった機能を備えています。おもに NNMi コンソールからアクセスします。

I

ICMP

インターネット制御メッセージ プロトコルを参照してください。

iSPI

NNM iSPI を参照してください。

L

L2

レイヤー 2 を参照してください。

L3

レイヤー 3 を参照してください。

M

MIB

管理情報ベースを参照してください。

N

NNM 6.x/7.x イベント

古い NNM 管理ステーションから NNMi に転送されたイベント用の NNMi 用語。NNMi には、転送されたイベントから NNMi が生成するインシデントを参照するためのインシデント ビューがあります。

NNM iSPI

l ファミリ内のスマート プラグイン。NNM iSPI は、MPLS のような特殊テクノロジ用に、またはネットワーク エンジニアリングのような特定の分野用に、NNMi に機能を追加します。

NNMi

HP Network Node Manager i Software を参照してください。

NNMi コンソール

NNMi ユーザー インタフェース。オペレータや管理者は、NNMi コンソールを使って NNMi ネットワーク管理タスクを実行できます。

O

OID

オブジェクト識別子を参照してください。

ovstatus コマンド

NNMi が管理するプロセスの現在のステータスを報告するコマンドです。NNMi コンソール (**[ツール] > [NNMi ステータス]**) またはコマンド プロンプトで起動できます。*ovstatus* リファレンス ページまたは UNIX のマンページを参照してください。

ovstart コマンド

NNMi の管理プロセスを起動するためのコマンドです。コマンド プロンプトで起動します。*ovstart* リファレンス ページまたは UNIX のマンページを参照してください。

ovstop コマンド

NNMi の管理プロセスを停止するためのコマンドです。コマンド プロンプトで起動します。*ovstop* リファレンス ページまたは UNIX のマンページを参照してください。

P

Ping スィープ

ICMP ECHO 要求を複数の IP アドレスに送信し、応答するノードにどのアドレスが割り当てられているか調べるネットワーク プローブ テクニック。ルールベースの検出で有効にすると、NNMi は、設定された IP アドレス範囲で ping スィープを使用してその他のノードを検索できます。サービス拒絶攻撃に ping スィープを使用できるので、ICMP ECHO 要求をブロックするネットワーク管理者もいます。

PostgreSQL

トポロジ、インシデント、設定情報のような情報を保存するために NNMi がデフォルトで使用するオープン ソース リレーショナル データベース。NNMi では、ほとんどのテーブルについて PostgreSQL の代わりに Oracle を使用するよう設定することもできます。

R

RCA

根本原因解析を参照してください。

S

SNMP

簡易ネットワーク管理プロトコル (SNMP) を参照してください。

SNMP トラップ

ポーリングを使ったネットワーク管理 (SNMP エージェントから請求された応答) は、処理をできるだけ簡単にするための SNMP の設計原則です。しかし、このプロトコルは、SNMP エージェントから SNMP マネージャ プロセス (この場合、NNMi) への要請されないメッセージの通信も提供します。要請されないエージェント メッセージは、「トラップ」として知られており、内部状態の変化または障害条件に応答して SNMP エージェントが生成します。 NNMi は、受信した SNMP トラップ (**[SNMP トラップ]** インシデントの参照ビューに表示) からインシデントを生成します。

SNMP トラップ ストーム

要請されない大量の SNMP エージェント メッセージ。SNMP マネージャ プロセス (この場合、NNMi) を圧倒する可能性があります。`nnmtrapconfig.ovpl` コマンドを使用して NNMi に SNMP トラップ ストームしきい値を指定できます。受信トラップ レートが指定のしきい値レートを超えるとき、NNMi は、トラップ レートが再対応レート未満に下がるまでトラップをブロックします。

sysObjectID

システム オブジェクト ID を参照してください。

あ

アカウント

ユーザー アカウントを参照してください。

アクティブなクラスタ ノード

アクティブなサーバーを参照してください。

アクティブなサーバー

アプリケーション フェイルオーバーまたは高可用性設定で NNMi プロセスを現在実行しているサーバー。

アドレスのヒント

検出のヒントを参照してください。

アプリケーション フェイルオーバー

NNMi で、現在アクティブなサーバーが停止した場合に、NNMi のプロセスの制御をスタンバイ サーバーに移行するオプション機能 (ユーザーが設定し、jboss クラスタリング サポートを利用)。

い

因果関係

あるイベント (原因) と別のイベント (影響) の間の関係を示します。イベント (影響) は最初のイベント (原因) の直接的な結果です。NNMi は、因果関係分析アルゴリズムを使用して、イベントのサイクルを分析し、ネットワーク問題を解決するソリューションを明らかにします。

インシデント

NNMi では、ネットワークに関連するオカレンスの通知は、NNMi コンソールインシデント ビューとフォームに表示されます。NNMi には、インシデント属性に基づいてユーザーがインシデントをフィルタできるようにするいくつもの **[インシデントの管理]** ビューと **[インシデントの参照]** ビューがあります。ほとんどのインシデント ビューには、NNMi (*管理イベント*と呼ばれることもあります) が直接生成したインシデントが表示されます。NNMi には、SNMP トラップ から生成されたインシデントおよび NNM 6.x/7.x イベントから生成されたインシデントを参照するビューもあります。

インタフェース

ノードをネットワークに接続するのに使われる物理ポート。

インタフェース グループ

NNMi の主要なフィルタ テクニックの 1 つ。ただし、グループごとに、グループまたはフィルタ視覚化に設定を適用する目的で、インタフェースはグループにまとめられます。インタフェース グループは、監視の設定、テーブル ビューのフィルタ、マップ ビューのカスタマイズのいずれか、またはすべてに使用できます。「ノード グループ」も参照。

インターネット制御メッセージ プロトコル

中核的なインターネット プロトコル スイート (TCP/IP) の 1 つ。ICMP ping は、状態ポーリング用の SNMP クエリーとともに NNMi が使います。

え

エピソード

NNMi 根本原因解析で、特定の持続時間を指すのに使う用語。この持続時間は一次的な障害によってトリガーされ、その間、二次障害は抑制されるか、または一次的障害の下で相互に関連付けられます。

お

オブジェクト識別子

SNMP で、MIB データ オブジェクトを識別する数字のシーケンス。OID は、小数点で分離された数字で構成されます。各数字は、MIB 階層のそのレベルにおける特定のデータ オブジェクトを表します。OID は MIB オブジェクト名と同等の数字です。たとえば、MIB オブジェクト名 `iso.org.dod.internet.mgmt.mib-2.bgp.bgpTraps.bgpEstablished` はその OID `1.3.6.1.2.1.15.0.1` と同等です。

か

仮想ホスト名

仮想 IP アドレスと関連付けられたホスト名。

仮想 IP アドレス

特別なネットワーク ハードウェアに結び付かれていない IP アドレス。現在のフェイルオーバーまたはロードバランシングのニーズに基づいて、最も該当するサーバーに中断されないネットワーク トラフィックを送信するため、高可用性設定で使われます。

簡易ネットワーク管理プロトコル (SNMP)

OSI モデルのアプリケーション層 (レイヤー 7) で機能する簡易なプロトコル。リモート ユーザーは、このプロトコルによって、ネットワーク要素の管理情報を検査または変更できます。SNMP は、管理対照ノード上のエージェント プロセッサとネットワーク管理情報を交換するために NNMi が使う主要なプロトコルです。NNMi は、SNMP の最も一般的なバージョンである SNMPv1、SNMPv2c、および SNMPv3 と 3 つをサポートしています。

管理サーバー

NNMi 管理サーバーは、NNMi ソフトウェアがインストールされるコンピュータ システムです。NNMi のプロセスとサービスは、NNMi 管理サーバーで稼働します。(以前の NNM リビジョンはこのシステムについて「NNM 管理ステーション」という用語を使用していました)

管理情報ベース

SNMP で、管理対照ネットワークに関するデータの階層的に組織化された集合。管理情報ベース内のデータオブジェクトは管理対照デバイスの特色を参照します。NNMi は、ネットワーク管理情報を収集する場合、MIB データ オブジェクト (「MIB オブジェクト」、「オブジェクト」、「MIB」と呼ばれることもあります) を使って、管理対象ノードとの間で SNMP クエリを出し、または SNMP トラップを受け取ります。

く

組み込みデータベース

NNMi に組み込まれたデータベース。NNMi は、ほとんどのテーブルについて、組み込みデータベースの代わりに外部の Oracle データベースを使うよう設定することもできます。「PostgreSQL」も参照。

クラスタ

NNMi の関係では、高可用性テクノロジまたは jboss クラスタ化機能の使用によってリンクされるハードウェアおよびソフトウェアのグループ化のことです。これらは、一緒に機能して、コンポーネントに過剰負荷または障害が発生した場合、機能とデータの連続性を確実にします。クラスタ内のコンピュータは一般に高速 LAN 経由でお互いに接続されます。クラスタは、通常、可用性かパフォーマンス、またはその両方を向上させるために導入します。

クラスタ メンバーまたはノード

NNMi の関係では、NNMi 高可用性またはアプリケーション フェイルオーバーをサポートするよう設定された、または設定される予定の高可用性または jboss クラスタ内のシステム。

グローバル ネットワーク管理

地理的に分散している 1 つ以上のリージョナル マネージャからのデータを統合する 1 つ以上のグローバル マネージャを持つ、NNMi の分散型の配備です。

グローバル マネージャ

分散 NNMi リージョン マネージャ サーバーからのデータを統合する、グローバル ネットワーク管理配備内の NNMi 管理サーバーです。グローバル マネージャは、環境全体のトポロジおよびインシデントの統合ビューを提供します。グローバル マネージャには、NNMi Advanced ライセンスが必要です。

け

結論

NNMi で、管理対象オブジェクト用に Causal Engine がステータスと根本原因インシデントを決定した方法を明らかにする Causal Engine が生成および使用するサポート詳細。

検出シード

シードを参照してください。

検出のヒント

SNMP ARP キャッシュ クエリ、CDP、EDP、またはその他の検出プロトコル クエリ、または ping スィープを使用して NNMi が見つけた IP アドレス。NNMi はさらに、検出ヒントとして見つかった IP アドレスについてクエリーを実行し、結果をルールベースの検出内の現在の検出ルールに照らしてチェックします。

検出プロセス

NNMi が、ネットワーク ノードを管理下におくために、これらの情報を収集するプロセス。初期検出は、まずデバイス インベントリの情報を収集し、次にネットワーク接続情報を収集するという 2 つのフェーズのプロセスで実行されます。

最初の検出の後も検出プロセスは継続されます。つまり、リストに基づいた検出では、シード リスト内のデバイスは、設定が変更されると更新されます。ルールベースの検出では、新しいデバイスは現在の検出ルールに合致すると追加されます。検出プロセスは、NNMi コンソールまたはコマンド ラインから、デバイスまたはデバイス セットについてオンデマンドで開始できます。

「スパイラル検出」、「ルールベースの検出」、および「リストに基づいた検出」も参照してください。

検出ルール

ルールベースの検出プロセスを制限するのに使われる、ある範囲のユーザー定義 IP アドレスかシステム オブジェクト ID (OID)、またはその両方。検出ルールは、NNMi コンソールの **[自動検出ルール]** の **[検出の設定]** 部分に設定します。「ルールベースの検出」も参照。

こ

高可用性

このガイドでは、設定の一部に障害があっても中断されないサービスを提供するハードウェアおよびソフトウェアの設定のことです。高可用性 (HA) とは、コンポーネントに障害があった場合でもアプリケーションを実行し続けるよう冗長コンポーネントを備えた構成

を意味します。NNMi は、市販されているいくつかの HA ソリューションの 1 つをサポートするように設定できます。アプリケーション フェイルオーバーと比べてください。

コミュニティ文字列

SNMP エージェントで SNMP クエリを認証するために、SNMPv1 および SNMPv2c システムで使用されるパスワードのような仕組み。コミュニティ文字列は SNMP パケット内のクリアテキストに渡されるので、パケット傍受に対して脆くなります。SNMPv3 は、認証用の強力なセキュリティ メカニズムを用意します。

コンソール

NNMi コンソールを参照してください。

コントローラ

NNMi アプリケーション フェイルオーバーでの、マスター クラスタの状態を持つクラスタ メンバーを表す JGroups 用語。コントローラは、常にクラスタで最も古いメンバーです。

根本原因インシデント

Correlation Nature(相関関係の性質) 属性が *Root Cause(根本原因)* に設定されている NNMi インシデント。NNMi は、関連問題の現象が処理されていない場合、根本原因解析 (RCA) を使って現象を解決するすぐ実施できる課題として根本原因インシデントを確定します。根本原因解析を参照してください。

根本原因解析

NNMi で、根本原因解析 (RCA) とは、ネットワーク問題の原因を調べるために NNMi が使う問題解決方法のクラスのことです。NNMi で、根本原因とは、関連付けられた問題の現象が処理されていない場合、すぐに実施できる問題です。NNMi は、次の 2 つの主要な方法で根本原因の識別を使います。根本原因が解決されるまで、すぐに実施できる問題についてユーザーに通知し、二次的問題の現象を報告しないようにします。根本原因を判別すると、管理対象オブジェクトのステータス変更、または根本原因インシデントの生成、あるいはその両方が行われることがあります。

NNMi が RCA を使用する例として、管理対象ルーターで障害が発生し、NNMi 管理サーバーからみてルーターの反対側にある管理対象ノードが状態ポーリングクエリに応答できなくなることが挙げられます。NNMi は RCA を使用し、状態ポーリング障害が二次的問題の現象であるか調べます。ルーターが根本原因インシデントであることを報告し、根本原因ルーター障害が解決されるまでダウンストリーム ノードで発生している問題の現象を報告することは差し控えます。

し

シード

ネットワーク検出プロセスの開始点として機能することによって、NNMi のネットワーク検出を補助するネットワーク ノードのことです。たとえば、管理環境内のコア ルーターなどがシードになることができます。各シードは、IP アドレスやホスト名によって識別されます。ルールベースの検出が設定されていない場合、NNMi の検出プロセスは指定シードのリストに基づいた検出に制限されます。

シード済み検出

リストに基づいた検出を参照してください。

システム オブジェクト ID

NNMi で、ネットワーク要素のモデルまたは種類を識別する SNMP オブジェクト識別子の専門化された用語。システム オブジェクト ID は、ネットワーク要素の MIB オブジェクトの一部です。このオブジェクトは、検出の間に個別のノードから NNMi がクエリーします。システム オブジェクト ID によって分類できるネットワーク要素の種類の例には、HP ProCurve スイッチ ファミリ、HP J8715A ProCurve Switch、HP IPF システム用の HP SNMP エージェントがあります。他のベンダーのネットワーク要素も同じようにシステム オブジェクト ID に従って分類できます。システム オブジェクト ID の重要な使用法は NNMi デバイス プロファイルの定義にあります。デバイス プロファイルは、ネットワーク要素の種類が分かると、削減できるネットワーク要素の特徴を指定します。

システムアカウント

NNMi では、NNMi のインストール時に使うために備わっている特別なアカウントです。NNMi システム アカウントは、インストール終了後は、コマンド ラインのセキュリティや復旧目的のみに使用されます。ユーザー アカウントと比べてください。

障害ポーリング

主要な NNMi 監視アクティビティ。このアクティビティでは、NNMi は、管理対象の各オブジェクトの状態を調べるために、管理対象インタフェース、IP アドレス、SNMP エージェントすべてに関し、ステータス MIB の SNMP 読み取り専用クエリか ICMP ping、またはその両方を発行します。ユーザーは、NNMi コンソール の **[設定]** ワークスペースの **[監視の設定]** で、さまざまなインタフェース グループ、ノード グループ、ノードすべてについて実行された障害ポーリングの種類をカスタマイズできます。障害ポーリングは状態ポーリングのサブセットです。

自動検出

ルールベースの検出を参照してください。

状態

NNMi では、一般的に、MIB II `ifAdminStatus`、MIB II `ifOperStatus`、パフォーマンス、または可用性に関連する自己報告された管理対象オブジェクト応答について**状態**という用語を使用します。ステータスと比べてください。

状態ポーリング

NNMi の State Poller が実行する指令された監視。障害、パフォーマンス、コンポーネント稼働状態、管理対象オブジェクトの可用性データを取得するために ICMP ping と SNMP クエリーを使います。「障害ポーリング」も参照。

す

スパイラル検出

NNMi の管理するネットワークのインベントリ、コンテインメント、リレーションシップ、接続についての情報などのネットワーク トポロジ情報を NNMi が常時更新する処理のことです。「検出プロセス」、「ルールベースの検出」、および「リストに基づいた検出」も参照してください。

ステータス

NNMi では、全般的な稼働状態を示す管理対象オブジェクトの属性。ステータスは、管理対象オブジェクトの未解決結論から Causal Engine が計算します。状態と比べてください。

と

トポロジ (ネットワーク)

ネットワークのノードや接続などが、通信ネットワーク上でどのように配置されているのかを示す図のことです。

トラップ

SNMP トラップを参照してください。

の

ノード

ネットワーク関係で、ネットワークに接続されているコンピュータ システムやデバイス (プリンター、ルーター、ブリッジなど) のことです。SNMP クエリーに応答できるノードは最も包括的な情報を NNMi に提供しますが、NNMi は非 SNMP ノードの制限された管理も実行できます。

ノード グループ

NNMi の主要なフィルタ テクニックの 1 つ。ただし、グループごとに、グループまたはフィルタの視覚化に設定を適用する目的で、ノードはグループにまとめられます。ノード グループは、監視の設定、テーブル ビューのフィルタ、マップ ビューのカスタマイズのいずれか、またはすべてに使用できます。「インタフェース グループ」も参照。

は

パブリック キー証明書

ネットワーク セキュリティおよび暗号化で使用されます。デジタル署名を組み込み、パブリック キーと識別情報を結合するファイルです。証明書は、パブリック キーが個人または組織に属することの確認に使われます。NNMi は SSL 証明書を使います。これにはクライアントとサーバーの通信の認証と暗号化のために、パブリック キーおよびプライベート キーが含まれています。

ほ

ポート

ネットワーク ハードウェアの関係において、ネットワーク デバイスを経由して情報の受け渡しを行うコネクタです。

ボリューム グループ

コンピュータ ストレージ仮想化の用語。1 つの大規模ストレージ エリアを形成するよう設定された 1 つまたは複数のディスク ドライブ。NNMi がサポートするいくつかの高可用性製品は、共有ファイル システムにおいてボリューム グループを使用します。

み

未接続インタフェース

NNMi の観点からは、未接続インタフェースは NNMi が検出した他のデバイスに接続されていないインタフェースのことです。デフォルトでは、NNMi が監視する未接続インタフェースは IP アドレスのあるもののみであり、**[ルーター]** ノード グループのノードに含まれます。

ゆ

ユーザー アカウント

NNMi では、ユーザーまたはユーザー グループのために NNMi にアクセスする方法を提供します。NNMi ユーザー アカウントは NNMi コンソール にセット

アップされ、事前定義されたユーザー ロールを実装します。システムアカウントおよびユーザーロールを参照してください。

ユーザーロール

NNMi 管理者は、ユーザー アクセス設定の一環として、NNMi の各ユーザー アカウントに定義済みのユーザーロールを割り当てます。ユーザー ロールにより、NNMi コンソールにアクセス可能なユーザー アカウント、および各ユーザー アカウントで使用可能なワークスペースとアクションが決まります。NNMi には、*管理者*、*Web サービスクライアント*、*オペレータレベル 2*、*オペレータレベル 1*、*ゲスト*など、プログラムによってあらかじめ定義され、変更することのできない階層型ユーザーロールがあります。「ユーザー アカウント」も参照。

り

領域

NNMi において、タイムアウト値やアクセス資格認定のような通信設定を行うためにグループにまとめられたデバイス。

リージョナル マネージャ

デバイスの検出、ポーリング、およびトラップ受信を行い、情報をグローバル マネージャに転送する、グローバル ネットワーク管理配備内の NNMi 管理サーバーです。

リストに基づいた検出

シードのリストに基づいたプロセス。*シードとして指定するノードのみに関する*詳細ネットワーク情報を検出し、返します。リストに基づいた検出は、特定したクエリーとタスクのネットワーク インベントリのみを保守します。ルールベースの検出と比べてください。「検出プロセス」と「スパイラル検出」も参照。

る

ルール

検出ルールを参照してください。

ルールベースの検出

*自動検出*と呼ばれることがよくあります。NNMi は、ルールベースの検出を使い、ユーザー指定検出ルールに従って、NNMi がデータベースに追加する必要のあるノードを探し出します。NNMi は、検出されたノードのデータ内で検出のヒントを探してから、指定の検出ルールに照らしてこれら候補をチェックします。検出ルールは、NNMi コンソールの **[自動検出ルール]** の **[検出の設定]** 部分に設定します。リストに基づいた検出と比べてください。

れ

レイヤー 2

階層化通信モデルである Open Systems Interconnection (OSI) のデータ リンク層です。データ リンク層では、ネットワークの物理リンクを介してデータの伝送を行います。NNMi レイヤー 2 ビューは、デバイスの物理接続に関する情報を提供します。

レイヤー 3

階層化通信モデルである Open Systems Interconnection (OSI) のネットワーク層です。ネットワーク層は、ネットワーク上の隣接するノードのアドレスの取得、データ伝送経路の選択、サービス品質などに関与します。NNMi レイヤー 3 ビューは、ルーティングの観点から接続に関する情報を提供します。

ろ

論理ボリューム

個別のファイル システムまたはデバイス スワップ空間として使えるボリューム グループ内の任意のサイズの容量を指すコンピュータ ストレージ仮想化の用語。NNMi がサポートするいくつかの高可用性製品は共有ファイル システムで論理ボリュームを使います。

ロール

ユーザーロールを参照してください。

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 9.10

ドキュメント タイトル : NNMi デプロイメント リファレンス

フィードバック :

Java™
COMPATIBLE