

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 : 9.00

デプロイメント リファレンス

ドキュメントのリリース日付 : 2010 年 3 月
ソフトウェアのリリース日付 : 2010 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 が提供する有効なライセンスが必要です。FAR 12.211 および 12.212 に準拠し、商用コンピュータ 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 2008–2010 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。

Java™ は、Sun Microsystems, Inc の米国内での商標です。

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

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

UNIX® は、オープン グループの登録商標です。

Oracle テクノロジーの制限された権限に関する通知

DOD FAR 補足規定に従って供給されたプログラムは、「商用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、該当する Oracle 使用許諾契約に記載されている使用許諾の制限に従うものとします。そうでなければ、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 USA, 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>)

この製品には、The Legion Of The Bouncy Castle によって開発されたソフトウェアが含まれています。
(<http://www.bouncycastle.org>)

この製品には、Trantor Standard Systems Inc. が開発したソフトウェアが組み込まれています。
(<http://www.trantor.ca>)

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—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 システムごとに入手できます。
- *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—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、以下の URL で行ってください。

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

または、HP Passport ログイン ページの [新規ユーザー - 登録してください] 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 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 Software Support Online 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、HP ソフトウェア サポート サイトで、以下の機能を利用できます。

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

大部分のサポートには、HP Passport へのユーザー登録とログインが必要です。また、サポート契約が必要な場合もあります。HP Passport ID のご登録は、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	21
ガイドの説明	21
このドキュメントで使用する環境変数	22
改訂履歴	23
NNMi の詳細	24
準備	27
ハードウェアとソフトウェアの要件	29
対応ハードウェアとソフトウェア	29
システム設定 (UNIX)	30
NNMi と HP Performance Insight の共存	31
NNMi と HP Operations Manager エージェントの共存	31
設定	33
設定の一般概念	35
タスク フロー モデル	35
ベストプラクティス : 既存の設定を保存	36
ベストプラクティス : 作成者属性を使用する	36
ユーザー インタフェース モデル	36
順序	36
ノード グループ	37
グループの重複	38
ノード グループのメンバーシップ	39
階層 / コンテインメント	39
デバイス フィルタ	40
追加フィルタ	40
追加ノード	40
ノード グループのステータス	41
インタフェース グループ	41
ノード / インタフェース / アドレス階層	41
すべてを停止して再度やり直す	42
NNMi 通信	43
通信の概念	44
通信の設定レベル	44
ネットワーク待ち時間とタイムアウト	44
SNMP アクセス制御	45
SNMP バージョンの優先	46

管理アドレスの優先	47
ポーリング プロトコル	47
通信の計画作成	48
デフォルトの通信設定	48
通信設定領域	48
特定のノードの設定	49
再試行とタイムアウトの値	50
アクティブなプロトコル	50
複数のコミュニティ文字列または認証プロファイル	50
通信の設定	51
通信の評価	51
すべてのノードが SNMP 用に設定されましたか?	51
デバイスについて SNMP アクセスは現在利用できますか?	52
管理 IP アドレスは正しいですか?	52
NNMi は正しい通信設定を使っていますか?	52
State Poller 設定は通信設定と一致していますか?	52
通信の調整	53
NNMi 検出	55
検出の概念	55
NNMi はデバイス プロファイルから属性を導き出す	56
検出の計画	57
基本的な検出方法を選択する	57
リストベース検出	57
ルールベースの検出	57
自動検出ルール	58
自動検出ルールの順序	58
デバイスを検出から除外	58
Ping スweep	59
自動検出ルールの検出シード	59
自動検出ルールのベスト プラクティス	59
例	59
ノード名の解決	60
サブネット接続ルール	60
検出シード	61
再検出の間隔	61
オブジェクトを検出しない	62
検出の設定	62
自動検出ルールを設定する場合のヒント	62
シードを設定する場合のヒント	63
検出の評価	64
初期検出の進行状況をたどる	64
すべてのシードが検出されているか?	64
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?	65
すべてのノードが正しく検出されたか?	65
自動検出ルール	65
IP アドレス範囲	65
システム オブジェクト ID の範囲	66

すべての接続と VLAN は正しいか？	66
デバイスを再検出する	66
検出の調整	66
NNMi 状態ポーリング	67
状態ポーリングの概念	67
状態ポーリングの計画を作成	68
ポーリング チェックリスト	68
NNMi で何を監視できますか？	69
モニタリングされないノードへのインタフェース	70
モニタリングの停止	71
グループの計画作成	71
インタフェース グループ	72
ノード グループ	72
ポーリング間隔の計画作成	73
どのデータを収集するか	74
状態ポーリングの設定	74
インタフェース グループとノード グループの設定	74
インタフェースの監視の設定	75
ノードの監視の設定	75
デフォルト設定の確認	76
状態ポーリングの評価	76
ネットワーク監視の設定を確認します	76
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？	76
どの設定が適用されていますか？	77
どのデータが収集されていますか？	77
ステータス ポーリングのパフォーマンスの評価	77
State Poller は最新の状態に付いていっていますか？	78
状態ポーリングの調整	78
NNMi インシデント	81
インシデントの概念	81
インシデント ライフサイクル	82
トラップおよびインシデント転送	83
受信済み SNMP トラップ	84
MIB	85
カスタムインシデント属性	86
インシデント数の削減	86
インシデントの抑制、強化、およびダンプニング	86
インシデントの計画	88
NNMi が処理するデバイス トラップ	88
NNMi で表示するインシデント	88
インシデントに対する NNMi の対応方法	88
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	88
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	88
インシデントの設定	89
インシデントの評価	89
インシデントの調整	89

NNMi での証明書の使用	93
すべてをまとめる.....	94
認証機関証明書を生成する.....	95
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.....	97
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.....	98
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.....	99
自己署名証明書を使用するように高可用性を設定する.....	99
新規証明書を使用するように高可用性を設定する.....	100
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.....	100
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.....	102
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.....	103
ディレクトリ サービスへの SSL 接続を設定する.....	104
NNMi とシングル サインオンの使用	107
NNMi への SSO アクセス.....	107
NNMi と iSPI の SSO アクセス.....	108
HP NNMi-HP BAC My BSM 統合のシングル サインオンの設定.....	109
SSO の無効化.....	110
SSO セキュリティに関する注意.....	110
NNMi と LDAP によるディレクトリ サービスの統合	113
NNMi ユーザーのアクセス情報と設定オプション.....	113
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.....	114
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、一部のユーザー情報をディレクトリ サービスに保存.....	115
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.....	116
ディレクトリ サービスにアクセスする NNMi の設定.....	117
ディレクトリ サービスのクエリ.....	122
ディレクトリ サービス アクセス.....	122
ディレクトリ サービスの情報.....	123
ディレクトリ サービス管理者が所有する情報.....	126
ユーザー識別.....	127
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).....	128
ロール識別.....	129
Active Directory でのロール識別.....	130
他のディレクトリ サービスでのロール識別.....	130
ディレクトリ サービスからの NNMi ロール取得の設定 (詳細な方法).....	131
NNMi ロールを保存するディレクトリ サービスの設定.....	133
ディレクトリ サービス統合のトラブルシューティング.....	133
ldap.properties 設定ファイル リファレンス.....	134
例.....	138
グローバル ネットワーク管理	139
グローバル ネットワーク管理の利点.....	139
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.....	140
マルチサイト ネットワークを継続的にモニタリングする必要がありますか?.....	140
重要デバイスを表示できるか?.....	140
ライセンスの考慮事項.....	140

実践的なグローバル ネットワーク管理の例	141
要件のレビュー	142
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	142
初期準備	144
ポート可用性: ファイアウォールの設定	144
自己署名証明書の設定	144
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	144
NNMi 管理サーバー規模の考慮事項	144
システム クロックの同期化	145
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	145
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	145
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	145
モニタリングする重要な機器の一覧作成	145
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	146
NNMi ヘルプ トピックの確認	146
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	147
リージョナル マネージャでの転送フィルタの設定	149
転送されるノードを制限する転送フィルタの設定	149
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	157
global1 から regional1 と regional2 への 接続ステータスの判定	161
global1 インベントリの確認	162
global1 と regional1 との通信の切断	163
追加情報	166
検出とデータの同期化	166
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	168
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	168
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	169
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	169
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	171
NNMi ヘルプのトラブルシューティング情報	171
クロック同期	171
グローバル ネットワーク管理システム情報	171
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	172
破損した global1 上のデータベースの修復	172
グローバル ネットワーク管理と NNM iSPI またはサードパーティの統合	172
アプリケーション フェイルオーバー構成の NNMi の設定	173
アプリケーション フェイルオーバーの概要	173
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	174
アプリケーション フェイルオーバー構成の NNMi の設定	175
アプリケーション フェイルオーバー機能の使用	177
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	178
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	179
アプリケーション フェイルオーバーの例	179
その他の ovstart および ovstop オプション	180
アプリケーション フェイルオーバーのインシデント	180

iSPI およびアプリケーション フェイルオーバー	180
NNM iSPI のインストールに関する情報	181
統合アプリケーション	182
アプリケーション フェイルオーバーの無効化	183
管理タスクおよびアプリケーション フェイルオーバー	184
アプリケーション フェイルオーバーおよび NNMi パッチ	185
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	186
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)	186
ネットワーク レイテンシ/帯域に関する考慮	187
高可用性クラスタに NNMi を設定する	189
サポート対象の HA 製品	190
HA 用に NNMi を設定するための前提条件	190
HA の概念	191
HA 用語集	192
NNMi HA クラスタのシナリオ	193
マンページ	196
HA の設定	197
HA 用の NNMi の設定	197
NNMiHA 設定情報	197
プライマリ クラスタ ノードでの NNMi の設定	199
セカンダリ クラスタ ノードでの NNMi の設定	201
HA 用の NNM iSPI の設定	202
NNM iSPI for Metrics、NNM iSPI for QA、および NNM iSPI for Traffic	202
NNM iSPI for MPLS、NNM iSPI for IP Multicast、および NNM iSPI for IP Telephony	203
HA 下で実行中の 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 と NNMi	203
Oracle 環境での HA 用の NNMi の設定	203
Oracle を使っている NNMi の HA 設定情報	204
Oracle を使っている NNMi に HA を設定する	204
共有 NNMi データ	205
NNMi の共有ディスク内のデータ	205
設定ファイルの複製	206
共有ディスクの設定	206
Windows Server での共有ディスク設定についての注記	206
HA クラスタ内の NNMi のライセンス契約	207
HA 設定のメンテナンス	208
メンテナンス モード	208
HA リソース グループをメンテナンス モードにする	208
HA リソース グループのメンテナンス モードを解除する	208
HA クラスタ内の NNMi のメンテナンス	208
NNMi の起動と停止	208
クラスタ環境で NNMi のホスト名や IP アドレスを変更する	208
フェイルオーバーを行わせないように NNMi を停止する	211
メンテナンス後に NNMi を再起動する	211
NNMi HA クラスタ内のアドオン NNM iSPI のメンテナンス	211
HA の設定解除	212
HA クラスタ内の NNMi の設定を解除する	212
HA 下の NNMi のパッチ	216

HA 下の NNMi を NNMi 8.1x から NNMi 9.00 にアップグレードする	217
HA 設定のトラブルシューティング	221
一般的な HA のトラブルシューティング	221
エラー : Wrong Number of Arguments (引き数の数が間違っています)	221
製品スタートアップのタイムアウト (Solaris)	221
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	221
HA リソース グループが特定のクラスタ ノードでは起動できない	222
NNMi 固有の HA のトラブルシューティング	223
すべてのクラスタ ノードの設定解除後に、HA 用の NNMi を再び有効にする	223
NNMi を HA 下で正常に起動できない	223
HA の設定後、nmsdbmgr を起動できない	224
HA の設定後、pmd を起動できない	224
ディスク フェイルオーバーが行われない	224
フェイルオーバー後にセカンダリ ノードで共有ディスク ファイルが見つからない	224
NNM iSPI 固有の HA のトラブルシューティング	225
HA 設定リファレンス	226
NNMi HA 設定ファイル	226
NNMi に付属している HA 設定スクリプト	226
NNMi HA 設定のログ ファイル	228
IPv6 用 NNMi Advanced の設定	231
機能説明	231
必要条件	232
ライセンス	233
サポートされる設定	233
管理サーバー	233
IPv6 をサポートしている SNMP MIB	234
NNMi のインストール	235
IPv6 機能のアクティブ化	235
IPv6 機能の非アクティブ化	237
非アクティブ化後の IPv6 モニタリング	237
非アクティブ化後の IPv6 インベントリ	237
IPv6 インベントリ クリーンアップ時の既知の問題点	238
NNMi のメンテナンス	241
NNMi のバックアップおよびリストア ツール	243
バックアップ コマンドとリストア コマンド	243
NNMi データのバックアップ	244
バックアップ タイプ	244
バックアップ領域	244
NNMi データのリストア	246
同じシステムでのリストア	247
異なるシステムでのリストア	247
バックアップとリストアの方針	248
すべてのデータを定期的にバックアップする	248
設定変更前のデータのバックアップ	248
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	249

ファイルシステムのファイルのみのリストア	249
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	249
NNMi の保守	251
カスタム ポーラー収集のエクスポートの管理	251
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	251
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	252
カスタム ポーラー メトリックスの累積周期の変更	252
インシデント アクションの管理	253
同時アクション数の設定	253
Jython アクションのスレッド数の設定	254
アクション サーバー名のパラメータの設定	254
アクション サーバーのキュー サイズを変更する	255
NNMi 正規化プロパティの変更	255
初期検出後の正規化プロパティの変更	256
NNMi コンソールとの HTTPS のみ通信を設定する	257
NNMi 自己監視	257
NNMi で使用する Telnet および SSH プロトコルを設定する	259
Telnet メニュー項目の無効化	259
ssh プロトコルを使用する新規メニュー項目の設定	260
Windows 上のブラウザへの Telnet または SSH クライアントの設定	260
Windows オペレーティング システム提供の Telnet クライアント	262
サードパーティ Telnet クライアント (標準 Windows)	263
サードパーティ Telnet クライアント (Windows 上のウィンドウ)	264
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)	265
Linux で Telnet または SSH を使用する Firefox の設定	267
Linux 上の Telnet	267
Linux 上のセキュア シェル	268
Windows レジストリを変更するファイル例	268
nmmtelnet.reg の例	269
nmmputtytelnet.reg の例	269
nmmtelnet32on64.reg の例	269
nmmssh.reg の例	269
NNMi 管理サーバーの変更	271
NNMi 設定移動の準備のベストプラクティス	271
NNMi 設定および組み込みデータベースの移動	272
NNMi 設定の移動	272
NNMi パブリック キー証明書のリストア	273
NNMi 管理サーバーの IP アドレスを変更する	276
NNMi 管理サーバーのホスト名またはドメイン名の変更	277
Oracle データベース インスタンス接続情報の変更	280
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	281

NNMi 9.00 へのアップグレード	283
NNMi 管理サーバーを適切にアップグレードする	285
NNMi 8.0x からの起動	285
既存の NNMi 管理サーバー を NNMi 9.00 にアップグレード	285
別の NNMi 管理サーバーにアップグレードする	287
NNMi 8.0x からの起動	287
別の NNMi 管理サーバーへのアップグレード	287
Red Hat Linux 4.6 から 5.2 または 5.3 への NNMi の移行	289
Red Hat Linux 4.6 から Red Hat Linux 5.2 または 5.3 への NNMi の変更	289
NNMi Oracle データの移行	293
NNMi Oracle データの以降	293
追加アップグレード情報	295
設定面の相違点	295
機能面の相違点	296
NNM 6.x/7.x からのアップグレード	299
製品の比較	301
ネットワーク検出	301
検出の重要概念	303
ステータス モニタリング	304
ステータス モニタリングの重要概念	306
イベント モニタリングのカスタマイズ	306
イベント モニタリングの重要概念	308
NNM 6.x/7.x からのアップグレード	309
アップグレード オプション	310
新たな始まり	310
フェーズ別アップグレード	310
フェーズ 1: NNM 管理ステーションからのデータ収集	313
フェーズ 2: SNMP 情報のアップグレード	315
SNMP アクセスの設定	315
名前解決の制限	319
デバイス プロファイルのカスタマイズ	320
フェーズ 3: 検出のアップグレード	321
検出のスケジュール	322
自分の検出方法の選択	323
自動検出ルールの設定	324
スパイラル検出の設定	324
検出からのアドレスの除外	328
シード検出のためにシードを NNMi に追加します	329
接続のカスタマイズ	330

フェーズ 4: ステータス モニタリングのアップグレード	331
ポーリング間隔の設定	331
ポーリング プロトコルの選択	333
危険域にあるノードの設定	335
ステータス ポーリングからオブジェクトを除外します。	336
フェーズ 5: イベント設定とイベント削減のアップグレード	337
デバイスからのトラップの表示	337
NNMi で生成された管理イベント表示のカスタマイズ	339
トラップのブロック / 無視 / 無効化	339
ライフサイクル移行アクションの設定	340
追加 (手動) 処理の設定	341
イベント関連処理: イベントの繰り返し	341
イベント関連処理: レート計算	342
イベント関連処理: Pairwise のキャンセル	343
イベント関連処理: スケジュールされたメンテナンス	343
フェーズ 6: グラフィカルな視覚化のアップグレード (OVW)	344
フェーズ 6: グラフィカルな視覚化のアップグレード (ホーム ベース)	346
フェーズ 7: カスタム スクリプトのアップグレード	347
アップグレード ツール リファレンス	348
データ収集ツール	348
NNM 設定データ ファイル	349
アップグレード用データ インポート ツール	350

NNM 6.x または NNM 7.x と NNMi との統合 353

イベント転送の設定	354
ステップ 1: NNM 6.x/7.x を、NNMi 管理サーバーにイベントを転送するように設定する	354
推奨およびサポートされる手順: [イベント設定] ウィンドウを使用する	354
任意: 転送先リスト ファイル	355
別の手順: trapd.conf を手順で編集する	356
Step 2: (任意) ノード レベルのフィルタリングを使用してイベント数をさらに削減する	356
ステップ 3: NNM 6.x/7.x 管理ステーションを NNMi トポロジに追加する	356
ステップ 4: (任意) 管理ステーション設定を保存する	357
ステップ 5: NNM 6.x/7.x インシデント設定を NNMi コンソールで確認する	357
カテゴリのマッピング	357
リモート ビュー起動の設定	358
ステップ 1: Java プラグインのインストール	358
ステップ 2: NNMi で NNM 6.x/7.x 管理ステーション エンティティを作成する	359
ステップ 3: (オプション) その他の NNM 6.x/7.x ビューを設定する	360
選択を必要としない URL	360
選択を必要とする URL	361
統合をテストする	361
テスト 1: イベント転送の確認	361
テスト用のインタフェース停止、インタフェース開始イベントの生成	362
sendMsg.ovpl	363
NNM 6.x/7.x システムへのトラップをテストする	363
テスト 2: NNMi からの NNM 6.x/7.x 動的ビューの起動	364
イベント転送のトラブルシューティング	364

AlarmPoint	369
HP NNMi-AlarmPoint 統合	370
HP NNMi-AlarmPoint 統合について	370
値	370
サポートされるバージョン	371
ドキュメント	371
HP NNMi-AlarmPoint 統合の有効化	371
HP NNMi-AlarmPoint 統合の使用法	372
HP NNMi-AlarmPoint 統合の無効化	373
HP NNMi-AlarmPoint 統合のトラブルシューティング	373
HP NNMi-AlarmPoint Mobile Gateway 統合	373
HP NNMi-AlarmPoint Mobile Gateway 統合について	373
値	373
サポートされるバージョン	373
ドキュメント	374
HP NNMi-AlarmPoint Mobile Gateway 統合の有効化	374
HP NNMi-AlarmPoint Mobile Gateway 統合の使用法	374
HP NNMi-AlarmPoint Mobile Gateway 統合の無効化	375
HP NNMi-AlarmPoint Mobile Gateway 統合のトラブルシューティング	375
CiscoWorks LAN Management Solution	377
HP NNMi-CiscoWorks LMS の統合	377
値	377
サポートされるバージョン	378
ドキュメント	378
HP NNMi-CiscoWorks LMS 統合の有効化	378
HP NNMi-CiscoWorks LMS 統合の使用法	379
HP NNMi-CiscoWorks LMS の統合設定の変更	380
HP NNMi-CiscoWorks LMS 統合の無効化	380
HP NNMi-CiscoWorks LMS 統合のトラブルシューティング	380
CiscoWorks LMS アクションが機能しない	380
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	380
[HP NNMi-CiscoWorks LMS の統合設定] フォームのリファレンス	381
NNMi 管理サーバー接続	381
CiscoWorks LMS サーバー接続	382
Clarus Systems ClarusIPC Plus+	383
HP NNMi-Clarus Systems ClarusIPC Plus+ 統合	383
HP NNMi-Clarus Systems ClarusIPC Plus+ 統合について	383
値	384
サポートされるバージョン	384
ドキュメント	384
HP NNMi-Clarus Systems ClarusIPC Plus+ 統合の有効化	384
HP NNMi-Clarus Systems ClarusIPC Plus+ 統合の使用法	384
HP NNMi-Clarus Systems ClarusIPC Plus+ 統合の無効化	384

HP NNMi-Clarus Systems ClarusIPC Plus+ 統合のトラブルシューティング	385
HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合	385
HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合について	385
値	385
サポートされるバージョン	386
ドキュメント	386
HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合の有効化	386
HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合の使用法	387
HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合の無効化	387
HP NNM iSPI for IP Telephony-Clarus Systems ClarusIPC Plus+ 統合のトラブルシューティング	387
HP Asset Manager	389
HP NNMi-HP Asset Manager 統合	389
値	389
サポートされるバージョン	390
ドキュメント	390
HP NNMi-HP Asset Manager 統合の使用法	390
HP Business Availability Center My BSM	391
HP NNMi-HP BAC My BSM 統合	391
値	392
サポートされるバージョン	392
ドキュメント	392
My BSM のデフォルト NNMi モジュール	392
デモ ポートレットの設定	394
カスタム NNMi ポートレットの作成	395
ポートレット URL の特定	395
ポートレットの定義 HTML リファレンス	396
HP NNMi-HP BAC My BSM 統合のシングル サインオンの設定	398
HP NNMi-HP BAC My BSM 統合のトラブルシューティング	398
NNMi ポートレットがサインイン ページとして表示される	398
NNMi ポートレットが正しくロードしない	399
NNM iSPI for Performance ポートレットが正しくロードしない	399
NNM iSPI for Performance ポートレットに AsynchWait_Requests エラーが表示される	399
シングル サインオンが正しく機能しない	399
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	399
HP NNMi-HP BAC My BSM 設定フォームのリファレンス	400
HP Business Service Management トポロジ	403
HP NNMi-HP BSM トポロジ統合	403
値	403
サポートされるバージョン	404
ドキュメント	404
HP NNMi-HP BSM トポロジ統合の有効化	404
HP NNMi-HP BSM トポロジ統合の使用	405
HP NNMi-HP BSM トポロジ統合の設定の変更	405
HP NNMi-HP BSM トポロジ統合の無効化	406

HP NNMi-HP BSM トポロジ統合のトラブルシューティング	406
HP NNMi-HP BSM トポロジ統合設定フォームのリファレンス	406
NNMi 管理サーバー接続	407
BSM サーバー接続	407
BSM トポロジフィルタ	408
HP Network Automation	411
HP NNMi-HP NA 統合	411
値	412
サポートされるバージョン	412
ドキュメント	413
HP NNMi-HP NA 統合の有効化	413
HP NNMi-HP NA 統合の使用	415
統合が提供する NNMi 機能	415
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	416
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	417
不整合な状態のレイヤー 2 接続の特定 (NNM iSPI NET)	417
統合により提供される NA 機能	418
デバイス設定中のネットワーク管理の無効化	418
デバイス コミュニティ文字列の変更の伝播	419
NA インベントリへの NNMi 8.10 デバイスのインポート	419
HP NNMi-HP NA 統合の変更	420
HP NNMi-HP NA 統合の無効化	420
HP NNMi-HP NA 統合のトラブルシューティング	420
HP NNMi-HP NA 統合設定フォームのリファレンス	423
NNMi 管理サーバー接続	423
NA サーバー接続	424
統合動作	424
HP ProCurve Manager Plus	425
HP NNMi-HP ProCurve Manager Plus 統合	425
値	426
サポートされるバージョン	426
ドキュメント	426
HP NNMi-HP ProCurve Manager Plus 統合の使用法	426
HP RAMS MPLS WAN	427
HP NNMi-HP RAMS MPLS WAN 統合	427
値	427
サポートされるバージョン	427
ドキュメント	428
HP NNMi-HP RAMS MPLS WAN 統合の使用法	428
HP Systems Insight Manager	429
HP NNMi-HP SIM 統合	430
値	430
サポートされるバージョン	430
ドキュメント	430
HP NNMi-HP SIM 統合の有効化	430

HP NNMi-HP SIM 統合の使用法	432
HP NNMi-HP SIM 統合設定の変更	432
HP NNMi-HP SIM 統合の無効化	432
HP NNMi-HP SIM 統合のトラブルシューティング	433
SIM アクションが機能しない	433
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	433
[HP NNMi-HP SIM 統合設定] フォームのリファレンス	433
NNMi 管理サーバー接続	434
SIM サーバー接続	434
HP Universal CMDB	437
HP NNMi-HP UCMDB 統合	437
値	437
サポートされるバージョン	438
ドキュメント	438
HP NNMi-HP UCMDB 統合の使用法	438
nGenius Performance Manager	439
HP NNMi-nGenius Performance Manager 統合	440
値	440
サポートされるバージョン	441
ドキュメント	441
HP NNMi-nGenius Performance Manager 統合の有効化	441
HP NNMi-nGenius Performance Manager 統合の使用法	442
HP NNMi-nGenius Performance Manager 統合の無効化	442
HP NNMi-nGenius Performance Manager 統合のトラブルシューティング	442
NNMi ノースバウンド インタフェース	443
NNMi ノースバウンド インタフェース	444
値	444
サポートされるバージョン	444
用語	444
ドキュメント	445
NNMi ノースバウンド インタフェースの有効化	445
NNMi 8.1x からアップグレードした NNMi ノースバウンド インタフェース	445
新規 NNMi Northbound インタフェース設定	446
NNMi ノースバウンド インタフェースの使用法	447
インシデント転送	447
インシデント ライフサイクル状態変化通知	448
インシデント関連処理通知	449
インシデント削除通知	449
イベント転送フィルタ	450
NNMi ノースバウンド インタフェースの変更	450
NNMi ノースバウンド インタフェースの無効化	451
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	451
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	453
ローカル Northbound アプリケーション	453
リモート Northbound アプリケーション	453

[NNMi ノースバウンド インタフェースの転送先] フォームのリファレンス	454
Northbound アプリケーションの接続パラメータ	455
統合コンテンツ	456
Northbound 転送先のステータス情報	458
HP Operations Manager	459
HP NNMi-HPOM 統合 (HPOM エージェント実装)	459
HP NNMi-HPOM 統合について (HPOM エージェント実装)	460
値	460
サポートされるバージョン	461
ドキュメント	461
HP NNMi-HPOM 統合の有効化 (HPOM エージェント実装)	461
NNMi 8.1x からアップグレードされた統合設定	461
新規統合設定	462
HP NNMi-HPOM 統合の使用法 (HPOM エージェント実装)	465
HP NNMi-HPOM 統合設定の変更 (HPOM エージェント実装)	466
新規 NNMi トラップの HPOM ポリシーの更新	466
設定パラメータの変更	467
HP NNMi-HPOM 統合の無効化 (HPOM エージェント実装)	467
HP NNMi-HPOM 統合のトラブルシューティング (HPOM エージェント実装)	468
HPOM は転送されたインシデントを受信しない	468
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	470
[HP NNMi-HPOM エージェント転送先] フォーム リファレンス (HPOM エージェント実装)	471
HPOM エージェント接続	471
統合コンテンツ	472
転送先ステータス情報	474
HP NNMi-HPOM 統合 (Web サービス実装)	475
HP NNMi-HPOM 統合について (Web サービス実装)	475
値	476
サポートされるバージョン	477
ドキュメント	477
HP NNMi-HPOM 統合の有効化 (Web サービス実装)	477
Windows 用 HPOM	477
UNIX 用 HPOM または Linux 用 HPOM	479
HP NNMi-HPOM 統合の使用法 (Web サービス実装)	481
使用例	481
正常な状況: 不明な MSI 条件	482
詳細情報	482
HP NNMi-HPOM 統合設定の変更 (Web サービス実装)	482
HP NNMi-HPOM 統合の無効化 (Web サービス実装)	483
すべての HPOM 管理サーバーについて	483
1 つの HPOM 管理サーバーについて	483
HP NNMi-HPOM 統合のトラブルシューティング (Web サービス実装)	483
HPOM は転送されたインシデントを受信しない	483
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	486
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	486
NNMi と HPOM が同期されない	486
統合がファイアウォールを経由して動作しない	487

[HP NNMi-HPOM Web サービス統合設定] フォーム リファレンス	488
NNMi 管理サーバー接続	488
HPOM Management Server Connection(HPOM 管理サーバー接続)	489
統合動作	490
Incident Filter(インシデント フィルタ)	491
インシデント フィルタの例	492
インシデント フィルタの制限	493
Netcool ソフトウェア用 HP NNMi 統合モジュール	495
Netcool ソフトウェア用 HP NNMi 統合モジュール	495
値	496
サポートされるバージョン	496
ドキュメント	497
Netcool ソフトウェア用 HP NNMi 統合モジュールの有効化	497
NNMi 8.1x からアップグレードした Netcool ソフトウェア用 NNMi 統合モジュール	497
新規 Netcool ソフトウェア用 NNMi 統合モジュール設定	498
Netcool ソフトウェア用 HP NNMi 統合モジュールの使用法	500
Netcool ソフトウェア用 HP NNMi 統合モジュールの変更	501
Netcool ソフトウェア用 HP NNMi 統合モジュールの無効化	501
Netcool ソフトウェア用 HP NNMi 統合モジュール のトラブルシューティング	502
Netcool/OMNIbus は転送された NNMi 管理イベントを受信しない	502
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	503
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	503
Netcool ソフトウェア用 HP NNMi 統合モジュール 転送先フォームのリファレンス	504
Netcool/OMNIbus SNMP Probe の接続	504
統合コンテンツ	505
転送先ステータス情報	508
追加情報	509
NNMi 環境変数	511
このドキュメントで使用する環境変数	511
他の使用可能な環境変数	512
NNMi 8.00 からの Windows パスおよび環境変数	515
NNMi 9.00 およびウェルノウン ポート	517
設定変更の提案	521
用語集	523
索引	531

このガイドについて



(1) 最初のインストール
またはテスト ベッド

NNMi インストール
ガイドの手順に従っ
てください



(2) 製品の導入および前バージ
ョンからの移行

NNMi 導入リファレンス
をご覧ください (このマ
ニュアル)



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環境変数
- 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ミュニティ文字列の設定、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 BTO Software

- %NnmDataDir%: <drive>%ProgramData%HP BTO Software

- **Windows Server 2003:**

- %NnmInstallDir%: <drive>%Program Files%HP BTO Software

- %NnmDataDir%: <drive>%Documents and Settings%All Users%Application Data%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、515 ページの「NNMi 8.00 からの Windows パスおよび環境変数」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、512 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
NNMi バージョン 9.0x:	
2010 年 4 月 (9.00)	<ul style="list-style-type: none">英語第 3 版。完全に更新。日本語第 2 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 ドキュメントと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。詳細については、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』のダウンロード。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。 <ul style="list-style-type: none">『HP Network Node Manager i Software Windows 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 27 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 33 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 91 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 241 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から NNMi にアップグレードする。	このガイドの 283 ページの「NNMi 9.00 へのアップグレード」を参照してください。
Network Node Manager の前バージョンから NNMi にアップグレードする。	このガイドの 299 ページの「NNM 6.x/7.x からのアップグレード」を参照してください。
NNMi と統合される製品の詳細を学ぶ。	このガイドの 367 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 509 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 iSP ネットワーク エンジニアリング ツールセット (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『 <i>HP NNM iSPI Network Engineering Toolset Planning and Installation Guide</i> 』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。	『 <i>HP Network Node Manager i Software Developer's Toolkit Guide Toolkit Guide</i> 』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
- システム設定 (UNIX)
- NNMi と HP Performance Insight の共存
- NNMi と HP Operations Manager 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
	<p><i>NNMi</i> インストール ガイド</p> <ul style="list-style-type: none"> • 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]
	<p><i>NNMi</i> リリース ノート</p> <ul style="list-style-type: none"> • 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]
	<p><i>NNMi</i> システムおよびデバイスのサポート マトリックス</p> <ul style="list-style-type: none"> • 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。

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 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%\nmm\props
 - **UNIX:** \$NNM_CONF/nmm/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 と同じサーバーにインストールした NNMi をアンインストールすると、OVPI 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 以下の 2 つのコマンドを使用して、snmpmib MIB データベースを再作成します。

```
a mkdir -p /var/opt/OV/shared/nmm/conf/
```

```
b /opt/OV/lbin/nmmloadmib -load /usr/OVPI/mibs/GENMIB2IF.mib
```

上記コマンドを使用して、追加の MIB をロードします。

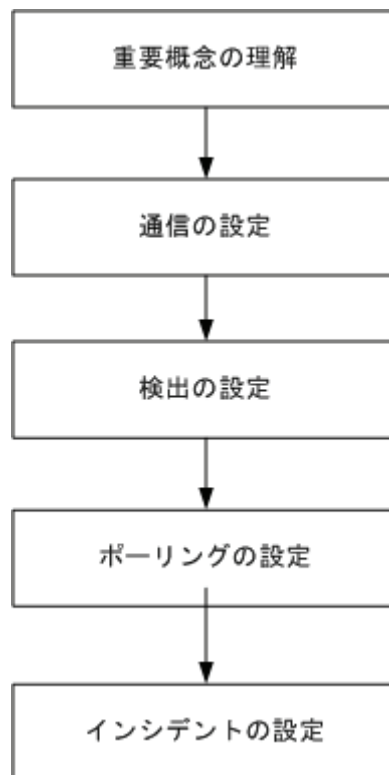
NNMi と HP Operations Manager エージェントの共存

NNMi 管理サーバーに HP Operations Manager (HPOM) をインストールする場合は、HPOM 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。

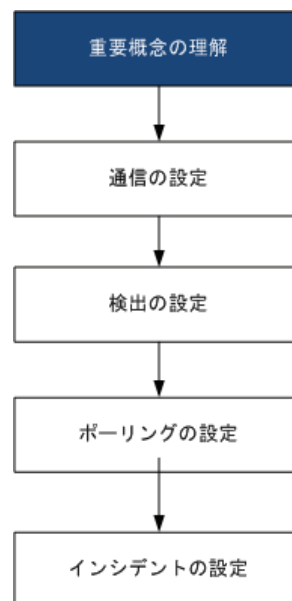
設定

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



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** 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
- 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** — 一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** — 一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** — プッシュン。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

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。

- モニタリング設定
- 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

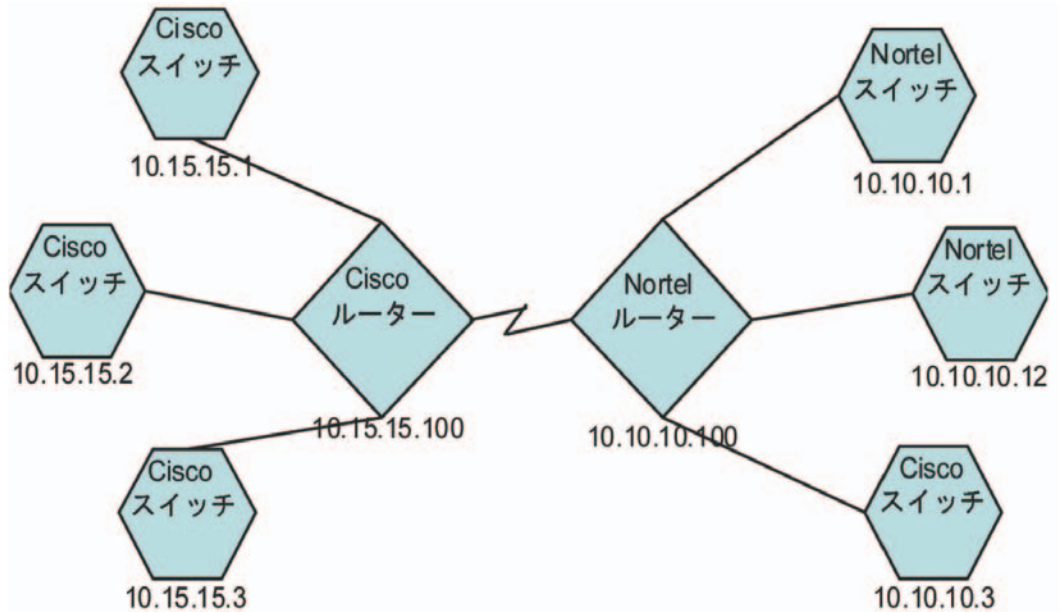
インタフェース グループは、以下のいずれかまたは両方の目的に使用できます。

- 検出からのインタフェース除外
- モニタリング設定
- 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または監視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。



- モニタリングを目的とした場合、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

ノードグループのメンバーシップは、検出した各ノードを設定した各々のグループと比較することにより評価されます。次の 4 種類の情報を使用して、適したノードをフィルタリングできます。

- 明示的に指定する追加ノード

以下の情報で OR を適用

- 子グループを含むこと

以下の情報で OR を適用

- システム オブジェクト ID から導き出される機能に基づいたデバイス フィルタ

以下の情報で AND を適用

- 他の属性に基づいた追加フィルタ

追加するノードは、グループのメンバーになります。子グループのメンバーは、このグループのメンバーとしての資格を得ます。その他のノードの場合は、[**デバイス フィルター**] タブ AND [**追加のフィルター**] タブを適用した条件と一致する必要があります。[**追加のフィルター**] タブ内では、AND、OR、および括弧評価の複合論理を作成できます。

階層 / コンテンメント

単純で再利用可能な原子グループを作成し、これらをモニタリング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。

- モニタリング 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モニタリング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、56 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、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

フィルタを使用して制限するには難しすぎる重大デバイスがネットワークに含まれている場合、これらのデバイスをホスト名別でグループに追加できます。

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ンツも継承しませんが、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 はモニタリング設定を、以下の方式で割り当てます。

- 1 インタフェース設定—NNMi によって、最初に一致するインタフェース設定定義に基づき、各ノードのインタフェースと IP アドレスが監視されます。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モニタリング設定は子ノードグループ内のノードにも適用されます。親ノードグループモニタリング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。

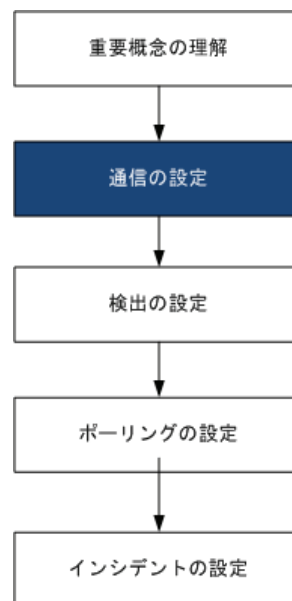
```
ovstart -c
```

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 は、Simple Network Management Protocol (SNMP) と Internet Control Message Protocol (ICMP ping) 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稼動状態を監視します。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ー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) のいずれかを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、プライバシーなし]**—認証もプライバシー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シーがないユーザー、次に、認証とプライバシーがあるユーザーを試みます。
- **[認証、プライバシーなし]**—認証はあるがプライバシー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ーのあるユーザーを試みます。
- **[認証、プライバシー]**—認証もプライバシー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 アドレス再検出を有効にする]** フィールドの設定により **NNMi** の動作が制御されます。

- **[SNMP アドレス再検出を有効にする]** 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 アドレス再検出を有効にする]** チェック ボックスがオフになっている場合、**NNMi** はデバイスは「停止中」とであると報告し、そのデバイスについて別の通信設定を試みません。



[SNMP アドレス再検出を有効にする] 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になります。

- オプションの自動検出ルール **ping** スワイプ機能は、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、さまざまな **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する必要があります。

- 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。
- 「NoSNMP」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

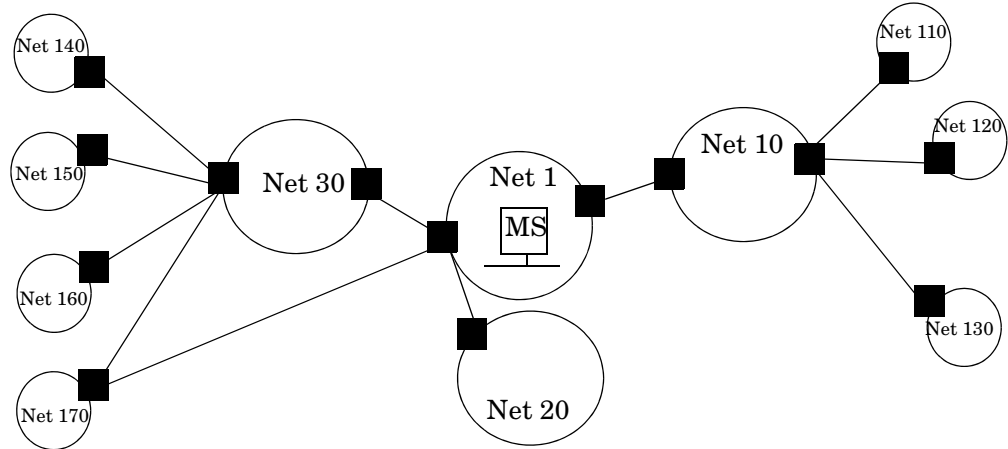
NNMi は、該当する領域や特定のノードで指定しなかった設定をデフォルト値を使用して完成させるため、大半のネットワークで妥当なものになるようデフォルトを設定します。

- **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 (rtrn`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
- ほか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。ネットワークの各エリア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モニタリングします。

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 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 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 사용되는固有の認証資格証明（ある場合）を決定します。

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、36 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。

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 【デバイスのプロファイル】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]>[設定のポーリング]**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ますし、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ある場合もあります。

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エリアへのプロトコルトラフィックが許容される場合でも、その種類のトラフィックはモニタリング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。

モニタリング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。

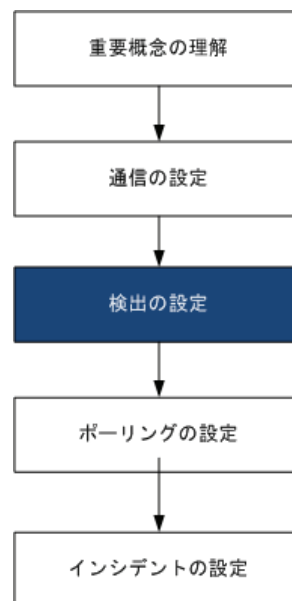
タイムアウトと再試行の調整

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、**[通信設定]** フォームの **[領域]** タブまたは **[特定のノードの設定]** 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、**[通信設定]** フォームの **[領域]** タブまたは **[特定のノードの設定]** 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 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投入されます。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 9.00 で検出がどのように変わったのかを知りたい方は、301 ページの「ネットワーク検出」でこの両者の違いについての高度な説明をお読みください。

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

NNMi のルーターとスイッチのみを検出するデフォルト動作では、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 では、事前設定をせずに行える検出はありません。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 モニタリングの考慮事項も、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モニタリングしません。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、67 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指定し、NNMi に各領域の開始アドレスを指定して、NNMi で定義済みデバイスを検出するようにします。

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。

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、モニタリング設定）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 では、リリース時に公開された 3600 以上のシステム 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。

リストベース検出

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。

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。
- 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weep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たい数以上のデバイスを NNMi が検出する場合、不要なデバイスを NNMi トポロジから削除しなければならなくなります。NNMi には一括削除のためのツールはありません。そのため、広範囲な検出から除去するのは非常に困難です。

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、以下のように検出範囲に影響します。

- 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。)

Ping スweep

ping sweepを使用して、設定した自動検出ルール内のIPアドレス範囲内のデバイスを検出することができます。初期検出では、すべてのルールで ping sweep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 sweep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 sweep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 sweep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 sweep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 sweepは、小さな検出範囲にのみ有効にしてください。

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 sweepをルールに対して有効にします。

自動検出ルールのベスト プラクティス

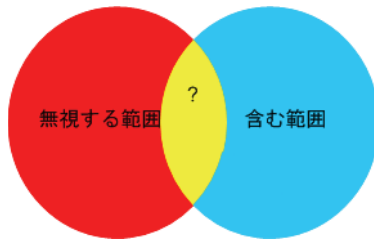
- NNMi はすべての検出対象デバイスを自動的に管理するため、管理したいネットワークの範囲に厳密に一致する IP アドレス範囲を使用してください。
 - 複数の IP アドレス範囲を1つの自動検出ルール内で使用して、検出を限定することができます。
 - 自動検出ルールに大きな IP アドレス範囲を追加した後に、そのルール内の検出からいくつかの IP アドレスを除外することができます。
- システム オブジェクト ID 範囲の指定は接頭部分であり、絶対値ではありません。たとえば、範囲 1.3.6.1.4.1.11 は 1.3.6.1.4.1.11.* と同じです。

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している場合、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 一致が見つかり、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、モニタリング/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weep 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weep 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 または SNMP 通信 (あるいはその両方) を、グローバルで、通信領域で、または特定のホスト名または IP アドレスなどさまざまな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、47 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、NNMi に特定の 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、これらのアドレスは任意のノードのアドレスリストに表示されない、またはデバイス間の接続にこれらのアドレスは使用されないため、NNMi がこれらのアドレスの稼動状態を監視することはありません。

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 read した後で、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。
- **保存して閉じる**をコンソールまでさかのぼって行う。

▶ 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、36 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。)
- シードファイルの各エントリに適切な書式を、以下に示します。

```
IP_address # node name
```

この書式は、**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勧めます。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。
- 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。)

ルールベース検出
のみ

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、動的かつ継続的で完了することはないため、「検出が完了」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「検出が完了」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、または DNS 名が解決されなかったために検出が失敗—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ます。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—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、シード済みデバイスや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、51 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 **[デバイスのプロファイル]** 列を、文字列 [No Device Profile] 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？

[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 51 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weep 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ある場合、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、62 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、このルールの設定は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を検出されない場合、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、このルールの設定は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 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。

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。

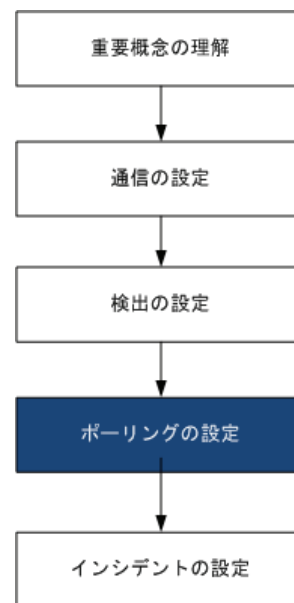
そのデバイスがシードの場合、シードを削除し、それからシードを再度追加します。

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 (またはその両方) 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。

NNMi 状態ポーリング



この章では、HP Network Node Manager i Software State Poller サービスを設定し、ネットワーク モニタリング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 9.00 でモニタリングがどのように変更されたか理解したい場合は、相違点の高レベルの概要に関する 304 ページの「ステータス モニタリング」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 モニタリング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 68 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 モニタリング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 デバイスをモニタリングするか、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。

[モニタリングの設定] 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 37 ページの「ノードグループ」と 41 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、State Poller 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、グローバルなモニタリング設定 ([**モニタリングの設定**] フォームの [**デフォルト設定**] タブ) によってモニタリング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。モニタリング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？
- モニタリング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？ 次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 iSPI Performance 製品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** モニタリングは要求しません。

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、55 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のが適切であることは明らかです。デバイスのインタフェース (**SNMP**) モニタリング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** 障害のモニタリングを有効にし、**SNMP** 障害およびポーリングのモニタリングを無効にします。グループについての **SNMP** 障害モニタリングがない場合、コンポーネント稼働状態モニタリングは適用されません。

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。

- 69 ページの「**NNMi で何を監視できますか？**」
- 71 ページの「**グループの計画作成**」
- 73 ページの「**ポーリング間隔の計画作成**」
- 74 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 StatePoller** 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。モニタリング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。

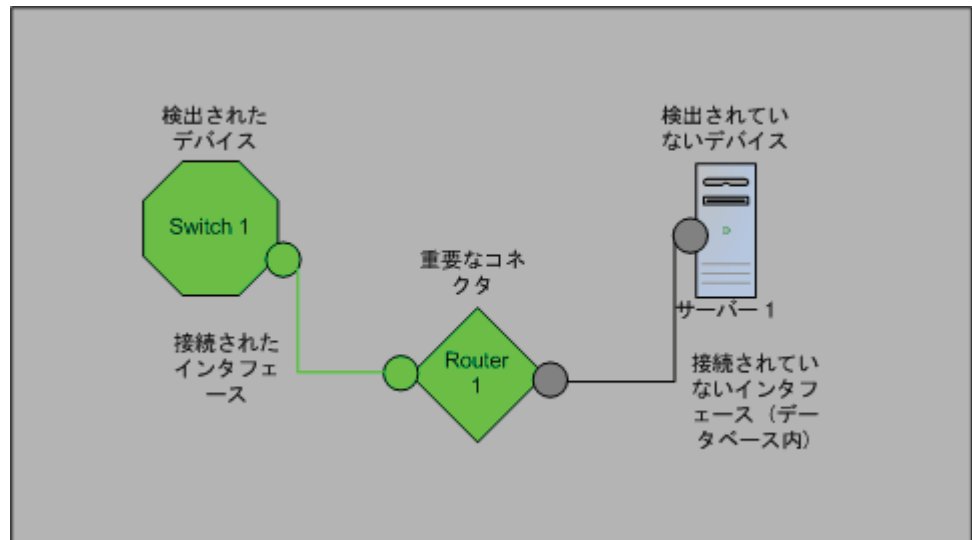
モニタリングの拡張

モニタリングを拡張して、以下が含まれるようにできます。

- 未接続インターフェース。デフォルトでは、NNMi がモニタリングする未接続インターフェースは 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ーフェースとして未接続インターフェースを定義します。



- ルーター インターフェースのように、IP アドレスのあるインターフェース。
- 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。

モニタリングされないノードへのインターフェース

直接管理していないデバイスに接続されているインター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ーフェースを未接続と見なします。

モニタリング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モニタリングする方法には次の2つがあります。

- モニタリングされていないノードの検出。

モニタリング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、モニタリング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 にモニタリングさせたくない、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関係なく、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。

モニタリングの停止

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、種類に関係なく、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またはインタフェースの中には、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、モニタリング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モニタリング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）。

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。モニタリング設定用にノード 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。

[モニタリングの設定] 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、インタフェースまたはデバイス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 (67 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、設定作業を簡単に行きます。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 つの種類の種類があります。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。モニタリング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、ファミリー
- MIB II sysName、sysContact、sysLocation

ベストプラクティス

簡単に再使用可能な極小のグループを作成し、モニタリング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、ファミリー、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、モニタリング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、ベンダーに無関係に、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、ネットワークでモニタリング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** または **SNMP** を使って実行できます。

ICMP (ping)

ICMP アドレス モニタリングは、**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 モニタリングは、モニタリングされている各 **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、モニタリング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** モニタリングは、モニタリング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。障害モニタリングに使われる値もあります。**NNM iSPI 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

コンポーネント稼働状態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モニタリングは、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 モニタリング設定は **NNM iSPI 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モニタリングは、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

モニタリング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、36 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、**[モニタリングの設定]** 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 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 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 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、[**モニタリングの設定**] 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 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 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 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 [**モニタリングの設定**] 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、モニタリング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モニタリング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頭に入れておいてください。

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かもしれません。

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モニタリング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 に現在のモニタリング設定が表示されます。

[障害 SNMP ポーリングが有効になっています] と **[障害のポーリング周期]** 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、ノードのモニタリング設定、およびモニタリング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働状態統計をいつでもチェックできます。

表 2 StatePoller 稼働状態情報

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	<ul style="list-style-type: none">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、定期的な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。 <ul style="list-style-type: none">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。
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。 <ul style="list-style-type: none">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。
ポーリング結果のキューの長さ	<ul style="list-style-type: none">監視すべきもの：この値はほとんどの時間 0 に近いはずですが。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	<ul style="list-style-type: none">監視すべきもの：この値はほとんどの時間 0 に近いはずですが。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。
状態アップデート キュー期間	<ul style="list-style-type: none">監視すべきもの：この値はほとんどの時間 0 に近いはずですが。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

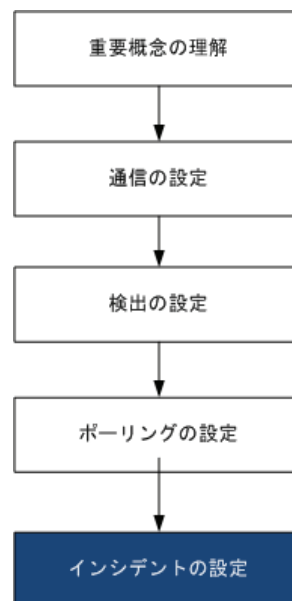
これらの変数は、ネットワーク管理のニーズによって促進されます。ステータス ポーリングについてパフォーマンス上の問題がある場合は、次の設定を考慮してください。

- 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 ([モニタリングの設定] 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、最も特定の制御を維持し、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モニタリング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モニタリングするには、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。

モニタリング設定とは無関係に、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モニタリング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。しかし、コンポーネント稼働状態モニタリングを無効にすると、State Poller が使用するメモリー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 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 インシデントと関連処理が用意されています。この章では、HP Network Node Manager i Software 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 9.00 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 306 ページの「イベント モニタリングのカスタマイズ」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関連処理が用意されています。デフォルトのインシデント関連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関連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 NNMi 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。

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	<ul style="list-style-type: none"> • 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関連処理待ちです。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、86 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	<ul style="list-style-type: none"> • 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。	<ul style="list-style-type: none"> • 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
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	<ul style="list-style-type: none"> • 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 (続き)

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
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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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

	トラップ転送	NNMi ノースバウンドインタフェース	NNMi リモート マネージャ
転送対象	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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。	リモート 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。
設定先	[設定] ワークスペースの [トラップ転送設定]	[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 トラップ設定] フォームまたは [リモート NNM 6.x/7.x イベント設定] フォームの [グローバル マネージャへ転送] タブ

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 (続き)

	トラップ転送	NNMi ノースバウンドインタフェース	NNMi リモートマネージャ
注		<p>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。</p> <ul style="list-style-type: none"> • 443 ページの「NNMi ノースバウンドインタフェース」 • 459 ページの「HP NNMi-HPOM 統合 (HPOM エージェント実装)」 • 495 ページの「Netcool ソフトウェア用 HP NNMi 統合モジュール」 	<p>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 マネージャ上での関連処理に参加します。</p>
詳細情報	<p>NNMi ヘルプに トラップ転送を設定する</p>	<p>447 ページの「NNMi ノースバウンドインタフェースの使用法」</p>	<ul style="list-style-type: none"> • 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

受信済み SNMP トラップ

NNMi が管理デバイスから受信する SNMP トラップをノースバウンド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、456 ページの表 36 のインシデントを参照してください。

以下の理由により、NNMi SNMP トラップ転送メカニズムが推奨されています。

- **トラップのフィルタリング**
 - NNMi SNMP トラップ転送メカニズムを設定し、ノースバウンドアプリケーションに転送するタイプを制限することができます。
 - NNMi ノースバウンドインタフェースによって、受信した SNMP トラップがすべてフィルタリングしないで転送されます。
- **トラップ ID**
 - *Windows* (すべて) および *UNIX* (元のトラップ転送なし)

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、ノースバウンドアプリケーションへ転送する前に各 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。)

ノースバウンド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ノースバウンドアプリケーションに直接送信したように表示されるため、ノースバウンド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 ノースバウンドインタフェースは各 **SNMP** トラップを強化してから、ノースバウンドアプリケーションに転送します。トラップは **NNMi** 管理サーバーからのものと考えられます。**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
- ノースバウンド宛先に転送するすべての **SNMP** トラップ
- **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 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
- (**NNM iSPI for Metrics**) しきい値監視で使用するすべての **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。

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 — 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 — 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ウが再開始されます。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 — 一定時間ウィンドウ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)。

設定時の注：

- 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。

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 read した後で、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、**36** 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。

- 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い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]>[インシデントの設定レポート]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。

詳細設定

この項では以下の章について説明します。

- NNMi での証明書の使用
- NNMi とシングルサインオンの使用
- NNMi と LDAP によるディレクトリ サービスの統合
- グローバル ネットワーク管理
- 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
- IPv6 用 NNMi Advanced の設定

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、通信するその他のパーティの証明書、またはその他のパーティを識別するときに信頼する認証機関の証明書が含まれます。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

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、95 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。
- グローバルまたはリージョナル 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。97 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](#)」で説明したように、各クラスタの NNMi 管理サーバーの `nnm.keystore` と `nnm.truststore` ファイルをマージしてから、グローバル ネットワーク管理を設定します。
- 認証機関を使用する必要がある、グローバルまたはリージョナル NNMi 管理サーバーでアプリケーション フェイル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、95 ページの「[認証機関証明書を生成する](#)」で説明した手順に従い、次に、各クラスタの NNMi 管理サーバーの `nnm.keystore` と `nnm.truststore` ファイルをマージしてから、98 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](#)」で説明したようにグローバル ネットワーク管理を設定します。
- グローバルまたはリージョナル NNMi 管理サーバーで高可用性 (HA) を使用するように設定されている場合は、99 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、仮想ホスト名の `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後、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て、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。103 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 管理サーバーが 95 ページの「[認証機関証明書を生成する](#)」の手順で生成した 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のはこれらの CA 証明書のみです。
- グローバル ネットワーク管理構成で NNMi 管理サーバーを設定し、その後でリージョナルまたはグローバル ノードをアプリケーション フェイルオーバー クラスタに含めることにした場合は、97 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 ネットワーク管理構成で NNMi 管理サーバーを設定し、その後でリージョナルまたはグローバル ノードで HA を使用することにした場合は、99 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、104 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.exe -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。

b 必要な情報を入力します。

▶ 姓名の入力を求められたら、システムの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 の場合:** /opt/OV/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、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。

5 CA 署名機関に CSR を送信します。CA 署名機関から、myserver.crt という名前の署名付き証明書が発行されます。myserver.crt ファイルには、サーバー証明書と CA (認証機関) 証明書の両方が含まれています。CA 証明書は、サーバー証明書をインポートするときに使用します。

- 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、署名付き証明書および 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 -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。

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
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 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 -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 トランスタアのパスワードの入力を求められたら、**ovpass** 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



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`

トランス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`

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

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、`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。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。

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>
```

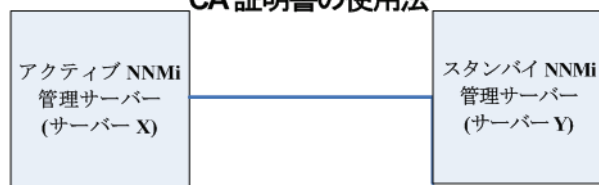
- 4 マージした nnm.keystore および nnm.truststore ファイルを server X から server Y にコピーし、どちらのノードにもマージ済みファイルがあるようにします。これらのファイル保存場所は、以下のとおりです。
 - Windows: %NNM_DATA%\%shared%\nnm\certificates
 - UNIX: \$NNM_DATA/shared/nnm/certificates
- 5 176 ページの **手順 6** からアプリケーション フェイルオーバー機能の設定を続行します。



アプリケーション フェイルオーバー機能を起動すると、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 NNMi_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

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、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。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。

- 1 NNMi_standby については、95 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、NNMi_standby 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 および nnm.truststore ファイルを Server Y から Server X の一時ファイル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。

- 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:

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

UNIX:

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

- 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\%nm%\certificates
- UNIX: \$NNM_DATA/shared/nm/certificates

- 176 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。



アプリケーション フェイルオーバー機能を起動すると、NNMi によってマージしたキーストアとトラストストア情報がサーバー X からサーバー Y に自動的に複製されます。

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

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

以下の手順を実行し、上の図に基づいて自己署名証明書を使用するように HA を設定します。

- NNMi_HA1 で nnmhaconfigure.ovpl スクリプトを実行します。このスクリプトでは、新しい仮想ホスト名 (この例では NNMi_virtual) を作成します。

nnmhaconfigure.ovpl スクリプトは、NNMi_virtual の新しい自己署名証明書を使用して、NNMi_HA1 の nnm.keystore および nnm.truststore ファイルを更新します。

- NNMi_HA2 で nnmhaconfigure.ovpl スクリプトを実行します。

このスクリプトを実行すると、NNMi_HA2 は仮想ホスト名 NNMi_virtual を継承します。失敗した場合、NNMi_HA2 は、NNMi_virtual ホスト名を含むキーストアとトラストストアを取得します。

- HA の設定を続行します。

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。

- 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
- 以下のコマンドを実行して、newcert を NNMi_HA1 の 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
- 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
- NNMi_HA1 と NNMi_HA2 の nms-local.properties ファイルに以下の行を追加します。

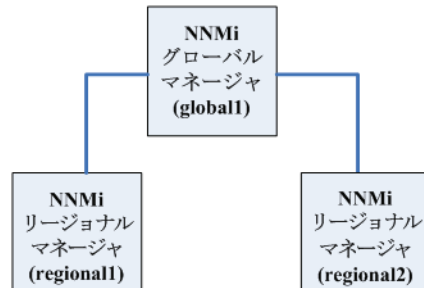
```
com.hp.ov.nms.ssl.KEY_ALIAS = newcert
```
- 変更を保存します。
- HA の設定を続行します。

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 ネットワーク管理で、以下の図に示すモデルを実現するとします。

グローバル ネットワーク管理での 自己署名証明書の使用法



以下の手順を実行し、上の図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、上の regional1 および regional2 の場所から、global1 のいずれかの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 の場合

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

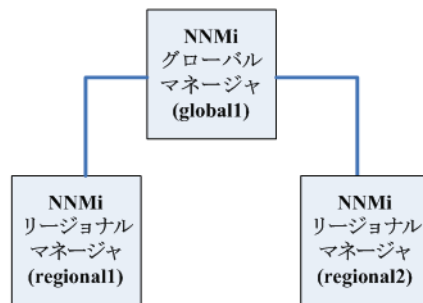
- 4 global1 で、以下のコマンドを以下の順序で実行します。
 - a `ovstop ovjboss`
 - b `ovstart ovjboss`

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 ネットワーク管理で、以下の図に示すモデルを実現するとします。

グローバル ネットワーク管理での CA 証明書の使用法



- 1 regional1 および regional2 については、95 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、上の regional1 および regional2 の場所から、`global1` のいずれかの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 の場合

- 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。

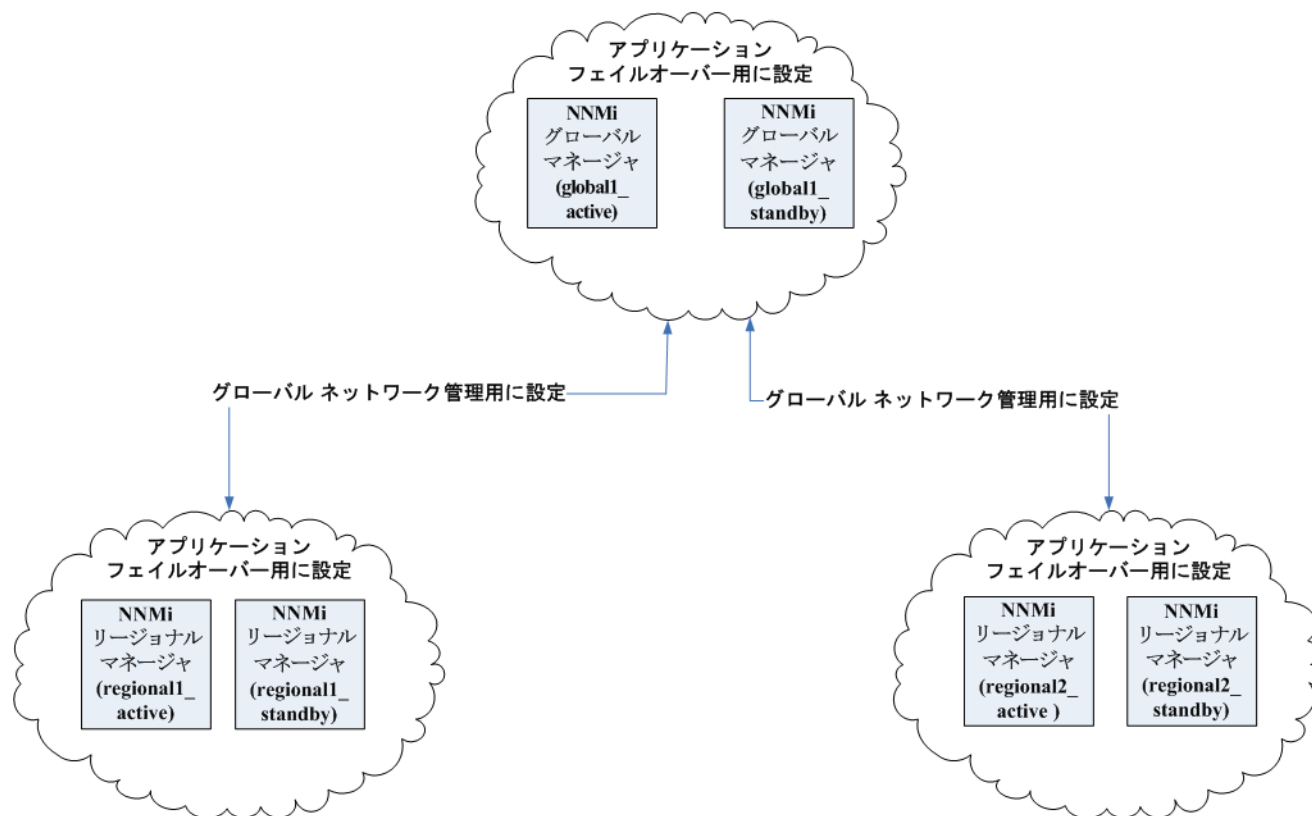
- a `ovstop ovjboss`
- b `ovstart ovjboss`

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 ネットワーク管理で、以下の図に示すモデルのアプリケーション フェイルオーバー機能を実現するとします。

グローバル ネットワーク管理 (アプリケーション フェイルオーバー)



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、97 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。
- 2 174 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。
- 3 100 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 および 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\%nm%\certificates
- **UNIX:** \$NNM_DATA/shared/nm/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 nnm_i_ldap -keystore nnm.truststore %  
-file <Directory_Server_Certificate.txt>
```

— **UNIX:**

```
$NnmInstallDir/nonOV/jdk/b/bin/keytool -import % -alias  
nnm_i_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。

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

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
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 -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、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。

NNMi とシングル サインオンの 使用

HP Network Node Manager i Software 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 を使用すると、NNMi コンソールにサインインするときに、再びサインインせずにほかの NNM iSPI にアクセスできます。SSO は、安全な NNM iSPI アクセス レベルを維持しながら、より簡単に NNM iSPI 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した後に NNMi コンソールとは異なる NNM iSPI URL にアクセスするには、サインイン資格情報を再入力する必要があります。

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。

- `lwssofmconf.xml` ファイルを編集して、複数の NNMi 管理サーバーで、パラメータ `initString` と `domain` を同じにします。
- `lwssofmconf.xml` file を編集し、SSO を無効にします。

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。詳細については、[lwssofmconf.xml](#) 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 管理サーバーのドメイン名が、`mycompany` のように短くてピリオドがない場合、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、「.」が少なくとも 1 つ付いているドメイン名が必要です。これを補修するには、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_SHARED_CONF%/lwssofmconf.xml`
 - **UNIX:** `$(NNM_SHARED_CONF)/lwssofmconf.xml`

- この例では、以下の文字列を検索します。

```
<domain>mycompany</domain>
```

これを以下の文字列で置き換えます。

```
domain>myhost.mycompany<domain>
```

- ovjboss を再起動します。

a **ovstop ovjboss**

b **ovstart ovjboss**

NNMi と iSPI の SSO アクセス

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。
http://<fully_qualified_domain_name>:<port_number>/nnmi/
<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 のインストール中に割り当てられたポート番号です。
- 有効なアカウントを使用して NNMi にサインインします。

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、次に NNM iSPI にアクセスするときにもう一度サインイ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 コンソールにサインオンできます。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。
- NNMi コンソールにアクセスできない場合は、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：`http://server:port/nnm/launch?cmd=showMain`。

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。

あるユーザーが、NNMi と 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 My BSM ポータルにログオンし、NNMi にサインインすることなく 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。My BSM と NNMi のサインイ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、BAC では普通の権限、NNMi では管理者権限を有する場合があります。

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、ほかのアプリケーションや NNMi iSPI の初期化ストリング設定も更新します。

BAC 初期化スト リング

以下のようにして、BAC 初期化ストリングを特定します。

- 1 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://<BAC_hostname>:<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:** `;%$NNM_SHARED_CONF%/lwsofmconf.xml`
- **UNIX:** `$NNM_SHARED_CONF/lwsofmconf.xml`

- 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、`lwsofmconf.xml` 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、`ovjboss` を再起動します。

```
a ovstop ovjboss
```

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_SHARED_CONF%\lwssofmconf.xml
 - **UNIX:** \$NNM_SHARED_CONF/lwssofmconf.xml
- 2 そのファイルから、以下のようなセクションを特定します。


```
<enableLWSSO enableLWSSOFramework="true"
enableCookieCreation="true" enableAutoCookieCreation="true"
cookieCreationType="LWSSO" enableSAML2Support="false"/>
```

 これを以下のように変更します。


```
<enableLWSSO enableLWSSOFramework="false"
enableCookieCreation="true" enableAutoCookieCreation="true"
cookieCreationType="LWSSO" enableSAML2Support="false"/>
```
- 3 以下のコマンドを実行し、ovjboss を再起動します。
 - a **ovstop ovjboss**
 - b **ovstart ovjboss**

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` を共有できません。
 - `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 マッピング s (同期)

SSO では、統合アプリケーション間のユーザー マッピングが確実に維持されないため、統合アプリケーションがユーザー マッピング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。

ユーザーのマッピングが失敗すると、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、実際には異なるユーザーに、複数のアプリケーションで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 (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 (アプリケーション B) にアクセスするとします。ユーザーのマッピングが失敗すると、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、ユーザー名を入力することになります。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、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。

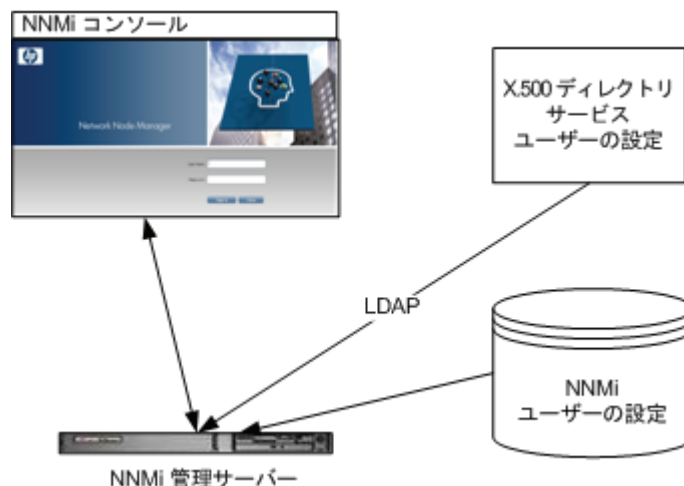
6 認証に Identity Manager が使用される

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 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 ロール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。

- 113 ページの「NNMi ユーザーのアクセス情報と設定オプション」
- 117 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」
- 104 ページの「ディレクトリ サービスへの SSL 接続を設定する」
- 122 ページの「ディレクトリ サービスのクエリ」
- 133 ページの「NNMi ロールを保存するディレクトリ サービスの設定」
- 133 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」
- 134 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 ロール**の割り当てにより、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。ロールの割り当てに従って、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5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5 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	ロール マッピング
1	NNMi	NNMi	NNMi
2	両方	ディレクトリ サービス	NNMi
3	ディレクトリ サービス	ディレクトリ サービス	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]タブのサインインおよびロール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

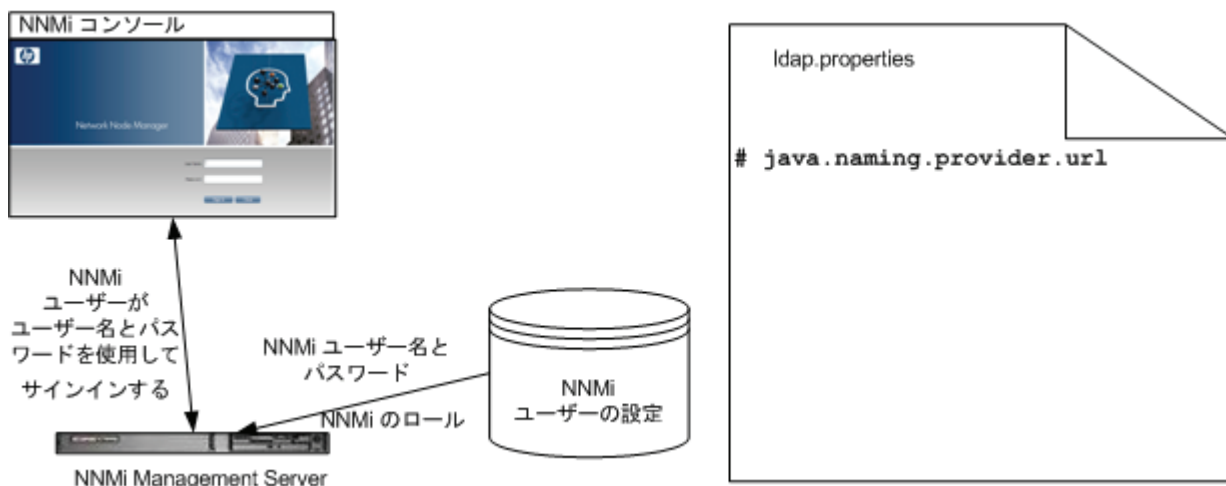
NNMiは、すべてのユーザーアクセス情報を取得するためにNNMiデータベースにアクセスします。それらの情報は、NNMi管理者がNNMiコンソールで定義およびメンテナンスします。ユーザーアクセス情報は、NNMiにとってローカルの情報となります。NNMiはディレクトリサービスにアクセスせず、NNMiは(図2のコメント行に示されている)ldap.propertiesファイルを無視します。

図2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2 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、一部のユーザー情報をディレクトリ サービスに保存

NNMi は、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 ロールへのマッピングは、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) ユーザー名と NNMi ロールのマッピングを 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 3 のコマンドラインは、NNMi が NNMi ロール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)。

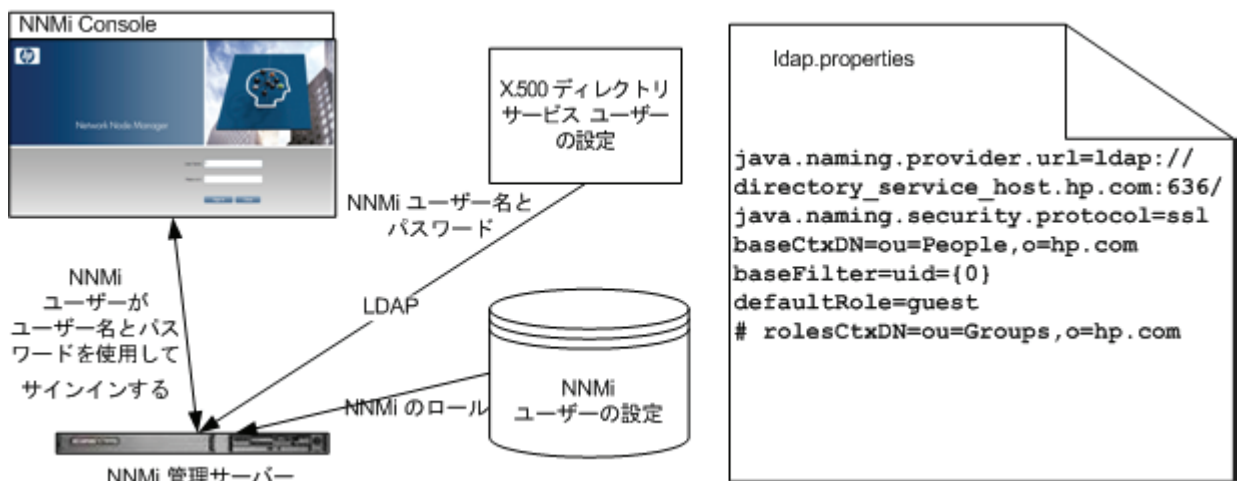
ユーザー名は、2 か所で入力する必要があるため、両方の場所でユーザー名のメンテナンスを行う必要があります。

図 3 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。
- ロール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 ロールを管理する。
- 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 3 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

NNMi は、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 ロールが決まります (NNMi ロールを定義する複数のグループでメンバーシップを持っているユーザーには、その中で最も高い権限のロールが付与されます)。

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およびグループ情報をメンテナンスします。ディレクトリ サービス管理者は、NNMi ロールごとに 1 つのグループとして、ディレクトリ サービス内でグループを設定します。

NNMi 管理者は、NNMi に対するユーザー名、ユーザー グループ、およびロールのディレクトリ 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。

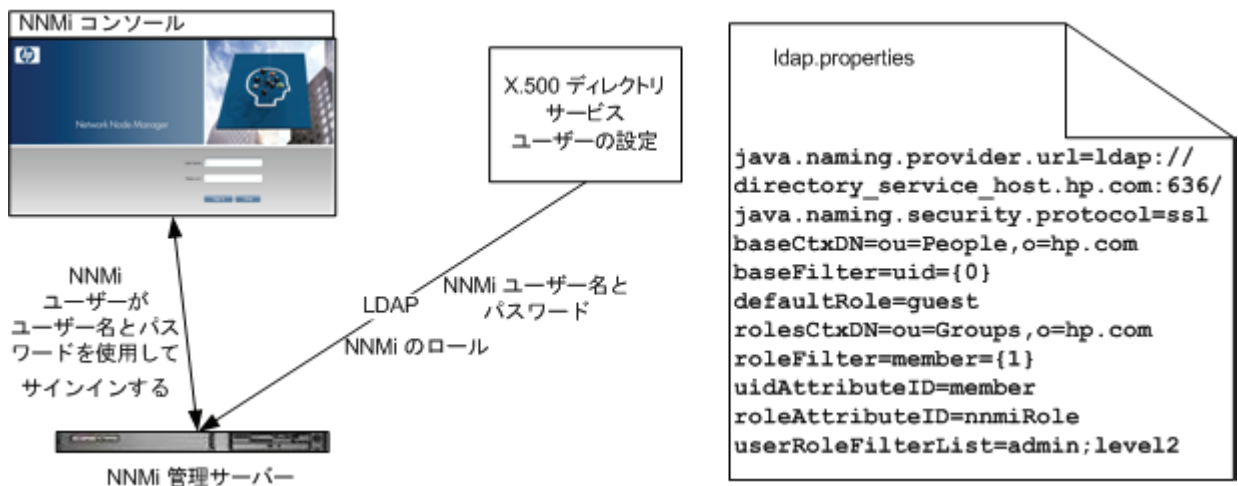
図 4 に、このオプションでの情報フローを示します。これは、NNMi にアクセスする必要があるユーザーで構成されるユーザー グループを含めるようにディレクトリ サービスを変更することが可能な環境に適しています。現在の設定に関係なく、このオプションでは、ディレクトリ サービスのグループ定義を変更する必要があります。

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 ロール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「ディレクトリ サービスを使用したアクセス制御」を参照してください。

図 4 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、134 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。138 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、122 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 NNMi 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 8:** 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

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 NNMi 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:** ディレクトリ サービスからの NNMi ロールの取得を設定する



ディレクトリ サービスに NNMi ロールを保存する場合は、NNMi ロール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、133 ページの「[NNMi ロール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:** NNMi ロール設定をテストする
- **タスク 7:** インシデント割り当ての NNMi ロールを設定する
- **タスク 8:** 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 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。

- **Windows:** `nmmconfigexport.ovpl -c account -u <user> ¥
-p <password> -f NNMi_database_accounts.xml`
- **UNIX:** `nmmconfigexport.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、104 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 NNMi 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

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
roleAttributeIsDN=true
roleNameAttributeID=info
roleAttributeID=memberOf
userRoleFilterList=admin;level2;level1
```

- 3 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 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 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 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 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 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。

```
nnmlldap.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 コンソールにサインインします。



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、ユーザー名とロール (`guest`) を確認します。

正常にユーザー サインインできない場合は、設定を確認し、期待どおりの結果になるまで手順 1 から手順 5 までの操作を繰り返してください。

- a 118 ページのタスク 3 が正常に完了したことを確認します。
- b 127 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。



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 サインインできたら、設定方法を選択します。
 - ロール割り当てを **NNMi** データベースに保存する (設定オプション 2) 場合は、121 ページの **タスク 8** に進みます。
 - ロール割り当てをディレクトリ サービスに保存する (設定オプション 3) 場合は、**タスク 5** に進みます。

タスク 5:ディレクトリ サービスからの NNMi ロールの取得を設定する

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

Microsoft Active Directory の場合の簡単な方法

- 1 任意のテキスト エディタで `ldap.properties` ファイルを開きます。
- 2 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`)。

他のディレクトリ サービスの場合の簡単な方法

- 1 任意のテキスト エディタで `ldap.properties` ファイルを開きます。
- 2 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 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:NNMi ロール設定をテストする

- 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。

```
nmldap.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 コンソールにサインインします。



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。

- 4 NNMi コンソールのタイトル バーで、ユーザー名とロール (ディレクトリ サービスで設定) を確認します。

正常にユーザー サインインできない場合は、設定を確認し、期待どおりの結果になるまで手順 1 から手順 4 までの操作を繰り返してください。

- a 120 ページのタスク 5 が正常に完了したことを確認します。
- b 129 ページの「ロール識別」の詳細な設定プロセスに従います。



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。

タスク 7: インシデント割り当ての NNMi ロールを設定する

- 1 任意のテキスト エディタで ldap.properties ファイルを開きます。
- 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。
- 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。
nmldap.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 コンソールにサインインします。
- 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 設定した各ロール タイプ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 8: 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 NNMi データベースでユーザー アクセス情報をリセットします。
 - NNMi データベースにロール割り当てを保存する (設定オプション 2) には、NNMi コンソールで以下の手順を実行します。
 - 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 インタフェースの設定] フォームの [ユーザー アカウント] タブと [ユーザー プリンシパル] タブにあるすべてのオブジェクトを削除します)。
 - ディレクトリ サービスのユーザー名のロール割り当てを作成します。(NNMi ユーザーごとに、(ディレクトリ サービスで定義されている) ユーザー名を NNMi ロールと関連付ける [ユーザー インタフェースの設定] フォームの [ユーザー アカウント] タブで、新規オブジェクトを作成します。
 - 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「*Control Access Using Both Directory Service and NNMi*」を参照してください。

- ディレクトリ サービスからのロール割り当てを設定した (設定オプション 3) 場合は、NNMi コンソールで以下の手順を実行します。
 - 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 インタフェースの設定] フォームの [ユーザー アカウント] タブと [ユーザー プリンシパル] タブにあるすべてのオブジェクトを削除します)。
 - 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「*ディレクトリ サービスを使用したアクセス制御*」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
- ロール識別

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、市販されている LDAP ブラウザを使用して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-NMi-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。
- それぞれの例には、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図も含まれています。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。

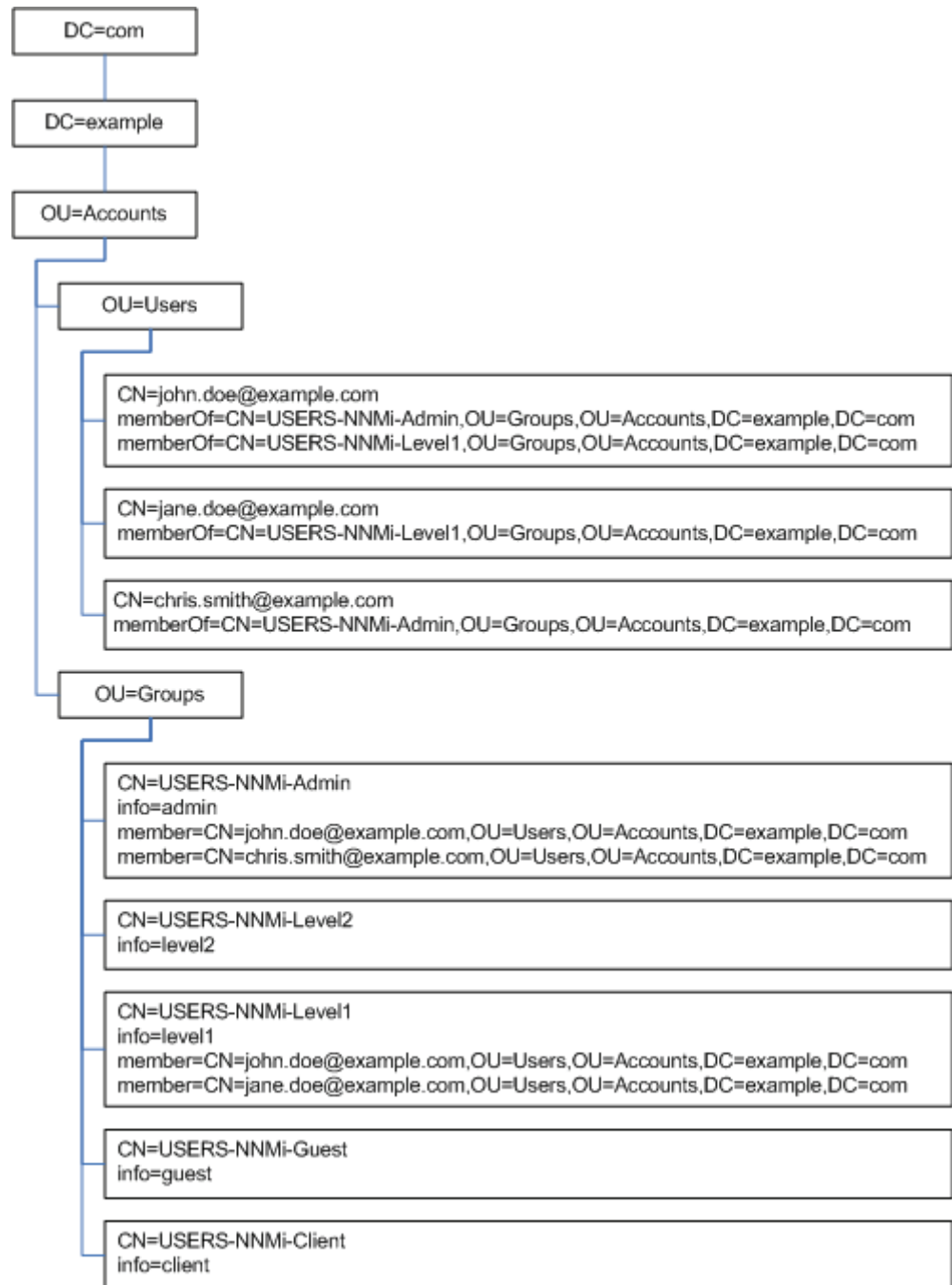
- ユーザー John Doe の識別名 :
CN=john.doe@example.com,OU=Users,OU=Accounts,DC=example,DC=com
- USERS-NMi-Admin グループの識別名 :
CN=USERS-NMi-Admin,OU=Groups,OU=Accounts,DC=example,DC=com
- ディレクトリ サービス ユーザー ID を保存するグループ属性 : member
- NNMi ロールを保存するグループ属性 : info
info 属性は、NNMi ロールを保存することを目的に再び指定されました。

LDIF ファイルの引用例 :

```
groups |USERS-NMi-Admin
dn: CN=USERS-NMi-Admin,OU=Groups,OU=Accounts,DC=example,DC=com
info: admin
cn: USERS-NMi-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
```

124 ページの図 5 に、このディレクトリ サービス ドメインを例示します。

図 5 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

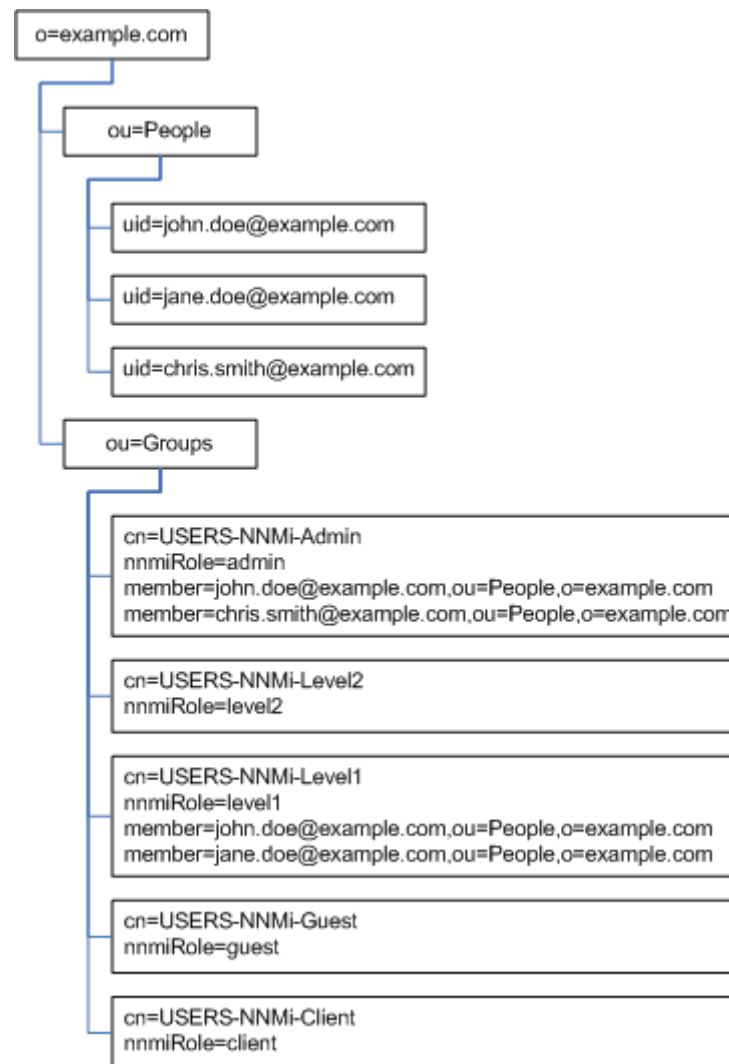
この例での関心の対象は以下の項目です。

- 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-NMi-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
- **NNMi** ロールを保存するグループ属性：nnmiRole
nnmiRole 属性は、特にこの目的のために作成されました。

LDIF ファイルの引用例：

```
groups |USERS-NMi-Admin
dn: cn=USERS-NMi-Admin,ou=Groups,o=example.com
nnmiRole: admin
cn: USERS-NMi-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 6 他のディレクトリ サービスのドメイン例



ディレクトリ サービス管理者が所有する情報

表 6 および表 7 に、LDAP を使用してディレクトリ サービスに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入手する情報を示します。

- ユーザー名とパスワードについてのみディレクトリ サービスを使用する場合（設定オプション 2）は、表 6 の情報を収集します。
- すべての NNMi アクセス情報についてディレクトリ サービスを使用する場合（設定オプション 3）は、表 6 と表 7 の情報を収集します。

表 6 ディレクトリ サービスからユーザー名とパスワードを取得する場合の情報

情報	Active Directory 例	他のディレクトリ サービス例
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	<ul style="list-style-type: none"> • 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	必要な場合は、自社のトラストストア証明書のコピーを入手し、104 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。	
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 7 ディレクトリ サービスから NNMi ロールを取得する場合の情報

情報	Active Directory 例	他のディレクトリ サービス例
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。	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • CN=john.doe@example.com, OU=Users,OU=Accounts, DC=example,DC=com • CN=john.doe@example.com 	<ul style="list-style-type: none"> • 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7 ディレクトリ サービスから NNMi ロールを取得する場合の情報 (続き)

情報	Active Directory 例	他のディレクトリ サービス例
ユーザーを NNMi ロールにマッピングするためにディレクトリ サービス管理者が作成したグループの名前	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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
NNMi ロールを保存する新規グループそれぞれの属性の名前	info	nnmiRole

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、ディレクトリ サービス内で 1 人のユーザーを検出する完全修飾方式による名前です。NNMi は、LDAP 要求でユーザー識別名をディレクトリ 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 コンソールでユーザーが入力したサインイン パスワードと一致すると、ユーザー サインインの処理が続行されます。

設定オプション 2 の場合、NNMi は以下の情報を調べ、より特権の多いロールをユーザーに付与します。

- ldap.properties ファイルの defaultRole パラメータの値
- NNMi コンソールでこのユーザーに割り当てられたロール

設定オプション 3 の場合、NNMi は、129 ページの「ロール識別」の説明に従ってユーザー ロールを判断します。

Active Directory でのユーザー識別例

baseFilter が CN={0} に、baseCtxDN が OU=Users, OU=Accounts, DC=example, DC=com に設定されている場合、ユーザーが NNMi に john.doe としてサインインすると、以下の文字列がディレクトリ サービスに渡されます。

```
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 が uid={0}@example.com に、baseCtxDN が ou=People, o=example.com に設定されている場合、ユーザーが NNMi に john.doe としてサインインすると、以下の文字列がディレクトリ サービスに渡されます。

```
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)

118 ページのタスク 3 の説明にある簡単な方法では正常に機能しない場合は、以下の手順を実行します。

- 1 ディレクトリ サービス管理者から、126 ページの表 6 に示す情報を入手します。
- 2 以下の該当する手順を実行します。
 - **Active Directory** と他のディレクトリ サービスの場合に **LDAP** ブラウザを使用する方法 : 129 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 : 129 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、134 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: 129 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 `<directory_service_host>` と `<port>` 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) `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時の方法と関連するように、`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。

- 9 119 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となります。<user_search_string> の値は、識別ユーザー名です。

ロール識別

ロール識別は、設定オプション 3 に適用されます。

NNMi は、ディレクトリ サービス内のユーザーのグループ メンバーシップを調べることによって、ユーザーの NNMi ロールを判断します。ディレクトリ サービス グループと NNMi 設定ファイルでは、短いテキスト文字列によって NNMi ロールを識別します。表 8 に、NNMi コンソールに表示されるテキスト文字列とロール名のマッピングを示します。

表 8 NNMi ロール名のマッピング

NNMi コンソールでのロール名	ディレクトリ サービスのグループと NNMi 設定ファイルでのテキスト文字列
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

Active Directory でのロール識別

ディレクトリ サービス ドメインでのユーザー定義には、ユーザーが属するディレクトリ サービス グループが含まれます。各グループ名は、一般に `memberOf` と呼ばれる、特定のユーザー属性の別々のエントリによって示されます。`ldap.properties` ファイルでは、`roleAttributeID` パラメータにより、ユーザーのグループ メンバーシップを保存するユーザー属性の名前を指定します。

NNMi は、リストにあるグループごとに、そのグループ定義に **NNMi** ロールが含まれるかどうかを判断します。`ldap.properties` ファイルでは、`roleNameAttributeID` パラメータにより、(表 8 で定義される) **NNMi** ロールのテキスト文字列を保存するグループ属性の名前を指定します。**NNMi** は、その属性の値を取得して **NNMi** ユーザーに割り当てるロールを決定します(ユーザーに複数のロールが割り当てられている場合、**NNMi** は、より特権の多いロールを使用します)。

他のディレクトリ サービスでのロール識別

ディレクトリ サービス ドメインでのグループ定義には、そのグループに属するディレクトリ サービスのユーザーが含まれます。

`ldap.properties` ファイルでは、`roleFilter` 値によってグループ メンバーの識別方法を指定し、`rolesCtxDN` 値によってグループを定義するディレクトリ サービス ドメイン内の場所を指定します。たとえば、`roleFilter` が `member={1}` に、`rolesCtxDN` が `ou=Groups,o=example.com` に設定され、認証されたユーザー識別名が `john.doe@example.com` の場合、**NNMi** は、完全修飾識別名が `ou=Groups,o=example.com` で終わるすべてのグループについてディレクトリ サービスに対してクエリを実行します。

NNMi は、ディレクトリ サービスによって返されたグループのリストを解析し、以下の指定値を含むグループを判断します。

```
member=uid=john.doe@example.com,ou=People,o=example.com
```

最後に **NNMi** は、適切な `member` 指定のグループのリストを解析し、いずれかのグループに **NNMi** ロールに対応する属性があるかどうかを判断します。


`ldap.properties` ファイルにおいて、`roleAttributeID` の値は、(表 8 で定義される) **NNMi** ロールのテキスト文字列を保存するグループ属性です。**NNMi** は、その属性の値を取得して **NNMi** ユーザーに割り当てるロールを決定します(ユーザーに複数のロールが割り当てられている場合、**NNMi** は、より特権の多いロールを使用します)。

`ldap.properties` ファイルにおいて、`uidAttributeID` の値は、ユーザー名を保存するグループ属性の名前です。**NNMi** は、その属性の値を取得して設定を照合します。

ディレクトリ サービスからの NNMi ロール取得の設定 (詳細な方法)

120 ページのタスク 5 の説明にある簡単な方法では正常に機能しない場合は、以下の手順を実行します。

- 1 ディレクトリ サービス管理者から、126 ページの表 7 に示す情報を入手します。
- 2 以下の該当する手順を実行します。
 - *Active Directory* の場合に **LDAP** ブラウザを使用する方法 : 132 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 : 132 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 : 132 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、134 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 `roleAttributeID` パラメータを以下のように設定します。
 - *Active Directory* の場合は、ユーザーが属するグループを示す *user* 属性の名前を指定します。
 - 他のディレクトリ サービスの場合は、NNMi ロール テキスト文字列 (129 ページの表 8 の 2 列目にある値のいずれか) を保存する *group* 属性の名前を指定します。
- 8 `roleAttributeIsDN` パラメータを以下のように設定します。
 - *Active Directory* の場合は、このパラメータを `true` に設定します。
 - 他のディレクトリ サービスの場合は、このパラメータを `false` に設定します。
- 9 (*Active Directory*) `roleNameAttributeID` パラメータを、NNMi ロール テキスト文字列 (129 ページの表 8 の 2 列目にある値のいずれか) を保存する *group* 属性の名前に設定します。
- 10 120 ページのタスク 6 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 ロール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 ロール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となります。
- 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ているユーザーの名前の形式を判断してください。

NNMi ロールを保存するディレクトリ サービスの設定

NNMi ロールをディレクトリ サービスに保存する場合 (設定オプション 3) は、NNMi ロール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 ロール割り当て用の新規ユーザー グループを作成できます。どちらの場合でも、ディレクトリ サービス管理者は、NNMi ロールのグループ属性をメンテナンスする必要があります。この新規属性は、`ldap.properties` ファイルの `roleNameAttributeID` パラメータ (Active Directory の場合) または `roleAttributeID` パラメータ (他のディレクトリ サービスの場合) に対応します。129 ページの表 8 に、ディレクトリ サービスで考えられるロール属性の値を示します。

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。

```
nnmlldap.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。

```
nnmlldap.ovpl -reload
```

- 3 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
```

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。
- バックスラッシュ文字 (\) を指定するには、バックスラッシュを 1 つ追加して (\\) バックスラッシュ文字をエスケープします。

▶ 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。

```
nnmlldap.ovpl -reload
```

表 9 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 9 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 9 ldap.properties ファイルのパラメータ

パラメータ	説明
java.naming.provider.url	<p>ディレクトリ サービスにアクセスするときの URL。</p> <p>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。例： 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。</p> <ul style="list-style-type: none">• 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。 <p>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。例：</p> <pre>java.naming.provider.url=ldap://ldap1.example.com/ ldap:// ldap2.example.com/</pre> <p>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。</p>
java.naming.security.protocol	<p>接続プロトコル指定。</p> <ul style="list-style-type: none">• 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。例： 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。 <p>詳細については、104 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。</p>

表9 ldap.properties ファイルのパラメータ (続き)

パラメータ	説明
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。 例： 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。例： 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識別します。 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。例： <ul style="list-style-type: none"> • baseCtxDN=CN=Users,DC=ldapserver,DC=example,DC=com • baseCtxDN=ou=People,o=example.com 詳細については、127 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を識別します。 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。 <ul style="list-style-type: none"> • 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。例： <ul style="list-style-type: none"> - 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。例： <ul style="list-style-type: none"> - baseFilter=CN={0}@example.com - baseFilter=uid={0}@example.com 詳細については、127 ページの「ユーザー識別」を参照してください。
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) ロールマッピングの保存場所に関係なく適用されます。ユーザーが 1 つの NNMi ロールで設定されている場合、NNMi は、より特権の多いロールを使用します。有効な値は、admin、level2、level1、または guest です。 例： 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。

表9 ldap.properties ファイルのパラメータ (続き)

パラメータ	説明
rolesCtxDN	<p>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識別します。</p> <p>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。例：</p> <ul style="list-style-type: none"> rolesCtxDN=CN=Users,DC=ldapserver,DC=example,DC=com rolesCtxDN=ou=Groups,o=example.com <p>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 ロール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。</p> <p>rolesCtxDN=cn=USERS-NNMi-*,ou=Groups,o=example.com</p> <p>このパラメータを設定すると、LDAP を介した NNMi ロール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 ロール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ロール関連の値を無視します。</p> <p>詳細については、129 ページの「ロール識別」を参照してください。</p>
roleFilter	<p>ディレクトリ サービスがグループ メンバー名を保存するときと同じ形式になっている、NNMi にサインインするユーザーを識別します。</p> <p>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。</p> <ul style="list-style-type: none"> 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} <p>詳細については、129 ページの「ロール識別」を参照してください。</p>
uidAttributeID	<p>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識別します。</p> <p>例： uidAttributeID=member</p> <p>詳細については、129 ページの「ロール識別」を参照してください。</p>

表9 ldap.properties ファイルのパラメータ (続き)

パラメータ	説明
roleAttributeID	<ul style="list-style-type: none"> • Active Directory の場合は、ユーザーのグループ メンバーシップを保存するユーザー属性の名前を識別します。例： roleAttributeID=memberOf • 他のディレクトリ サービスの場合は、ディレクトリ サービス グループのメンバーに適用される NNMi ロールを保存するグループ属性の名前を識別します。例： roleAttributeID=nnmiRole <p>詳細については、129 ページの「ロール識別」を参照してください。</p>
roleAttributeIsDN	<p>ディレクトリ サービスでのユーザーのロール属性の形式を示します。</p> <ul style="list-style-type: none"> • Active Directory の場合は、以下を使用します。 roleAttributeIsDN=true グループのロール属性 (roleNameAttributeID によって指定) はロール オブジェクトの識別名を表し、ロール名は、対応するユーザー オブジェクトの roleAttributeID 属性の値から取得します。 • 他のディレクトリ サービスの場合は、以下を使用します。 roleAttributeIsDN=false ロール名は、グループのロール属性の値 (roleAttributeID) から直接取得します。 <p>詳細については、129 ページの「ロール識別」を参照してください。</p>
roleNameAttributeID	<p>(Active Directory) roleAttributeIsDN=true の場合は、NNMi ロールを保存するディレクトリ サービス内のグループ属性を識別します。使用例は以下のとおりです。 roleNameAttributeID=info</p>
userRoleFilterList	<p>オプション。関連付けられたユーザーを NNMi コンソールでインシデントに割り当てることができる NNMi ロールを制限します。</p> <p>このリストのロールは、LDAP によって認証されたディレクトリ サービスのユーザー名にのみ適用されます。このパラメータにより、NNMi が NNMi コンソールで割り当てられ、NNMi データベースに保存する場合には使用できない機能を提供します。</p> <p>形式は、(129 ページの表 8 で定義される) 1 つ以上の NNMi ロール名で構成されるセミコロンで区切ったリストです。例： userRoleFilterList=admin;level2;level1</p>
searchTimeLimit	<p>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。</p> <p>例： searchTimeLimit=10000</p>

例

Active Directory の場
合の ldap.properties
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。

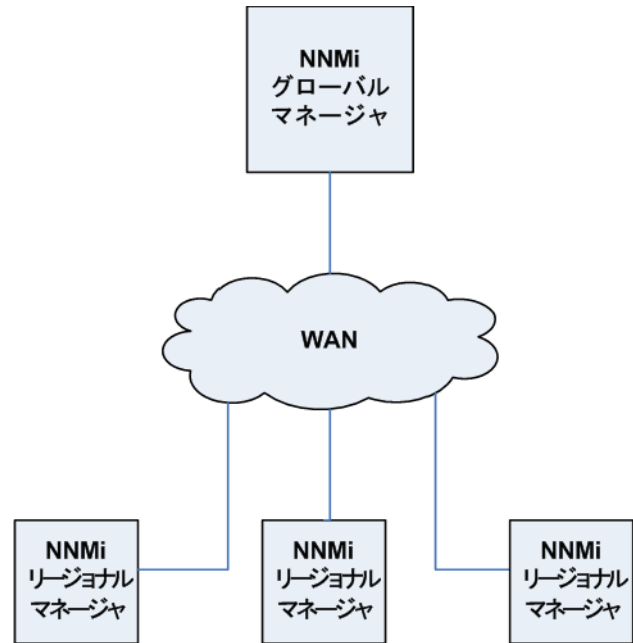
```
java.naming.provider.url=ldap://MYldapserver.example.com:389/  
bindDN=MYdomain\MYusername  
bindCredential=MYpassword  
baseCtxDN=CN=Users,DC=MYldapserver,DC=EXAMPLE,DC=com  
baseFilter=CN={0}  
defaultRole=guest  
rolesCtxDN=CN=Users,DC=MYldapserver,DC=EXAMPLE,DC=com  
roleFilter=member={1}  
uidAttributeID=member  
roleAttributeIsDN=true  
roleNameAttributeID=info  
roleAttributeID=memberOf  
userRoleFilterList=admin;level2;level1
```

他のディレクトリ
サービスの場合の
ldap.properties 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  
roleAttributeID=MYnmiRole  
userRoleFilterList=admin;level2;level1
```

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 またはサードパーティの統合

グローバル ネットワーク管理の利点

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、検出とモニタリングのニーズに合うように、ネットワークの検出およびモニタリングを行っています。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モニタリング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 のグローバル 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モニタリング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、モニタリング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

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。

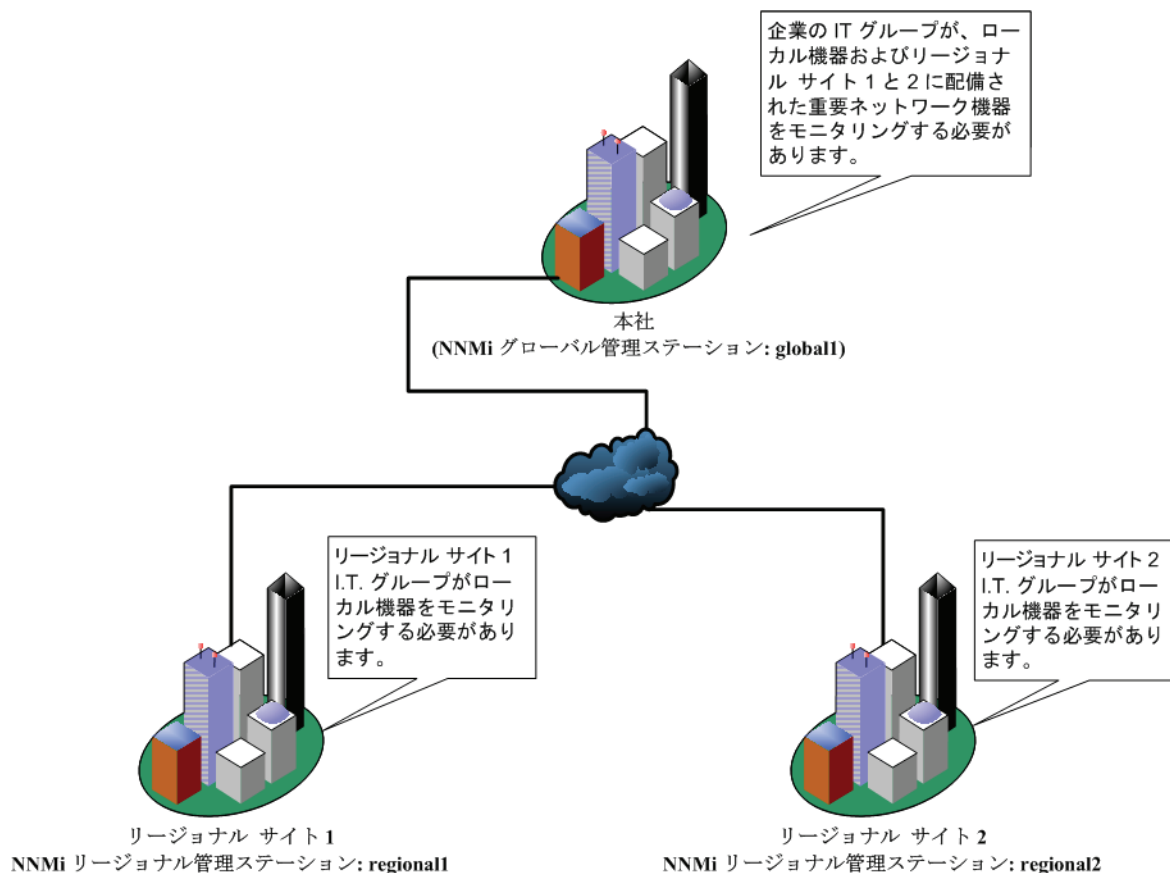
グローバルマネージャ、リージョナルマネージャ両方についてNNMi Advancedライセンスが必要ですか？グローバルマネージャとして使用するNNMi管理サーバーには、NNMi Advancedライセンスを購入してインストールする必要があります。NNMi管理サーバーをリージョナルマネージャとして使用する場合は、NNMi Advancedライセンスは必要ありません。

実践的なグローバルネットワーク管理の例

141 ページの図7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管理ステーションが機能しています。

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モニタリング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、それ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モニタリングする必要があります。

図7 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モニタリングを行うように NNMi 管理サーバーを設定します。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 管理サーバーへの接続を試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。バックアップ データを、ある NNMi 管理サーバー から 2 番目の NNMi 管理サーバー に配置することは、どちらのサーバーのデータベース UUID も同じであることを意味します。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モニタリングを行い、ほかのデバイスの管理はしない予定です。以下の表に、モニタリングのニーズをまとめます。

表 1 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 が本社をモニタリングし、NNMi 管理サーバー regional1 と regional2 が、各リージョナル サイトをモニタリングしています。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、次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。現在の値を確認したり値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 2 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

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に、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。97 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に、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。103 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 ネットワーク管理構成で既存の 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 をインストールするサーバーのサイズに関する特別な情報については、『NNMi 9.0 インストール ガイド』、『HP Network Node Manager i 9.0 Software リリース ノート』および『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。

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 ネットワーク管理構成に接続する前に、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 171 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。103 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。97 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」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。102 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。

モニタリングする重要な機器の一覧作成

global1 からモニタリングする、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 が現在モニタリングしている機器を確認します。機器を確認しておくで、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 が現在モニタリング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 がモニタリングしているノードを確認し、global1 でモニタリング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 がモニタリングしているノードを確認し、global1 でモニタリング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

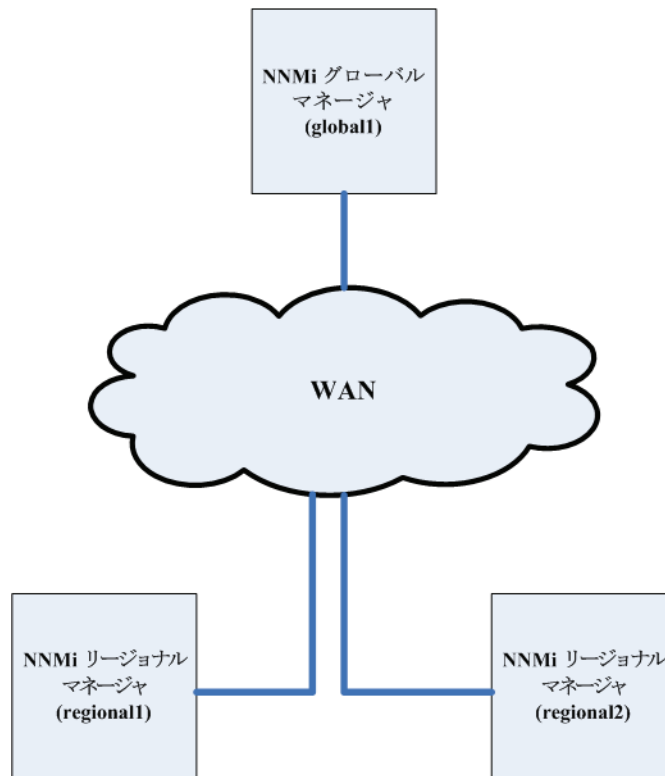
グローバル ネットワーク管理に関するすべてのヘルプ トピックを確認するには、以下の手順を実行します。

- 1 NNMi ヘルプで、**[検索]** をクリックします。
- 2 **[検索]** フィールドに「**グローバル ネットワーク管理**」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。

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

SSO (HP Network Node Manager i Software single sign-on) 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、107 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、148 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、次の手順に従って SSO を正しく設定するか、110 ページの「SSO の無効化」に示したように 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 の SSO NNMi 初期化文字列を探します。以下の場所を探してください。
 - **Windows:** %NNM_SHARED_CONF%/lwssofmconf.xml
 - **UNIX:** \$NNM_SHARED_CONF/lwssofmconf.xml
- 2 global1 の lwssofmconf.xml を開き、ファイルの中から以下のようなセクションを探します。

```
<lwssValidation id="ID000001">
```



```

<domain>cnd.hp.com</domain>
<crypto cipherType="symmetricBlockCipher"
engineName="AES" paddingModeName="CBC" keySize="256"
encodingMode="Base64Url"
initString=Initialization String></crypto>
</lwssofmvalidation>

```

- 3 global1 の lwssofmconf.xml ファイルにある *Initialization String* の実際の値を、regional1 と regional2 の lwssofmconf.xml 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、110 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、lwssofmconf.xml ファイルの中から以下のようなセクションを探します。

```

<protectedDomains>
  <url>xxx.hp.com</url>
</protectedDomains>

```

- a global1 は country1.hp.com に、regional1 は country2.hp.com に、そして、regional2 は country3.hp.com にあるとします。global1、regional1 および regional2 にある lwssofmconf.xml ファイルの protectedDomains セクションを、以下のように変更します。

```

<protectedDomains>
  <url>hp.com</url>
</protectedDomains>

```

変更を保存します。

- b global1 は colorado.hp.com に、regional1 は california.mycompany.com に、そして regional2 は hawaii.yourcompany.com にあるとします。global1、regional1 および regional2 にある lwssofmconf.xml ファイルの protectedDomains セクションを、以下のように変更します。

```

<protectedDomains>
  <url>colorado.hp.com</url>
  <url>california.mycompany.com</url>
  <url>hawaii.yourcompany.com</url>
</protectedDomains>

```


変更を保存します。

- 5 サーバー A、B、C 上で、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`



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。

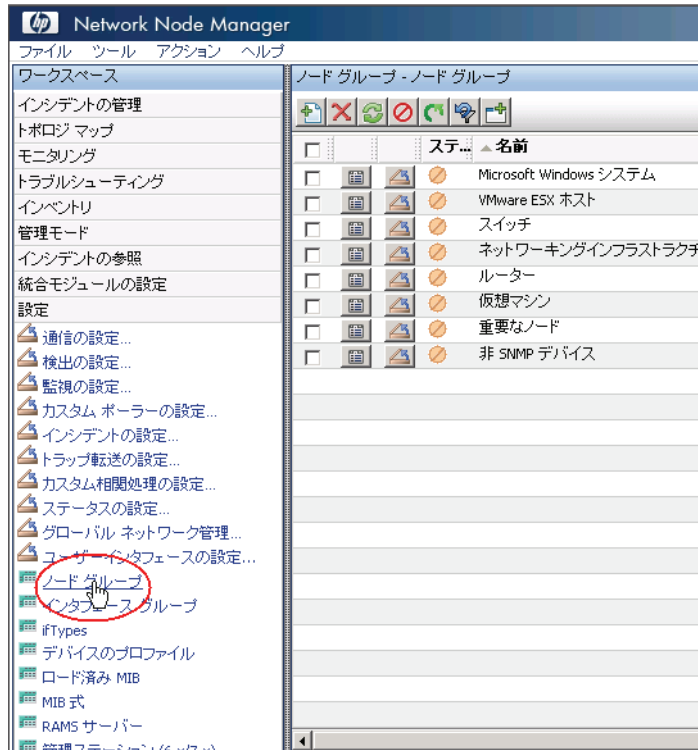
リージョナル マネージャでの転送フィルタの設定

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。

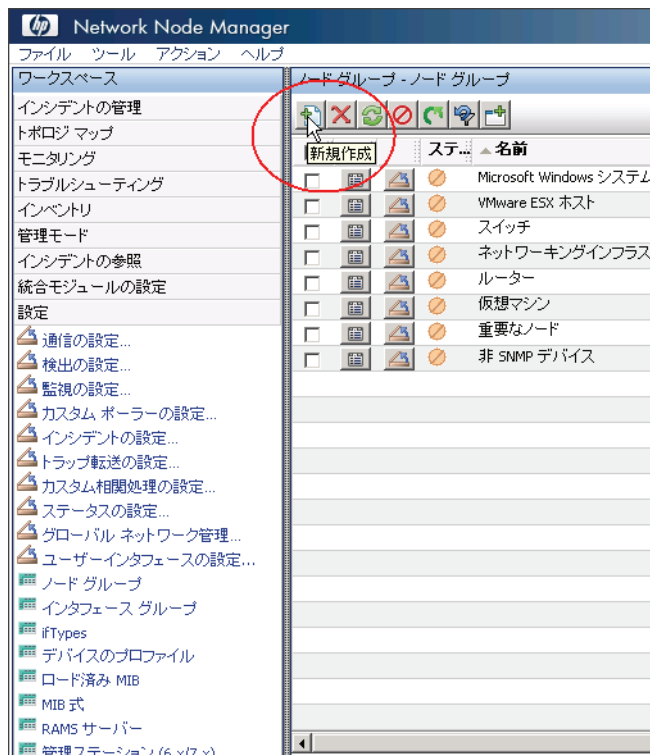
転送されるノードを制限する転送フィルタの設定

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。



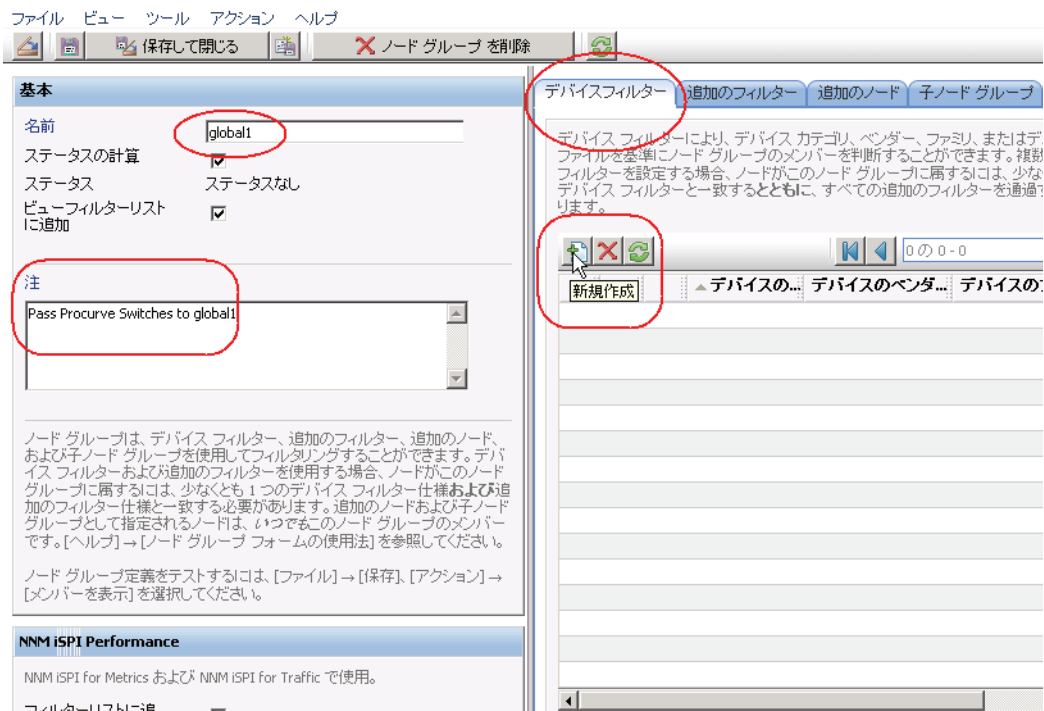
▶ この例では、ノードフィルタの新規作成し、そのフィルタを使用して **regional1** と **regional2** の転送フィルタを作成する方法を説明していますが、既存のフィルタを使用して、リージョナル NNMi 管理サーバーからグローバル NNMi 管理サーバーへの転送フィルタを設定することもできます。

▶ 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。

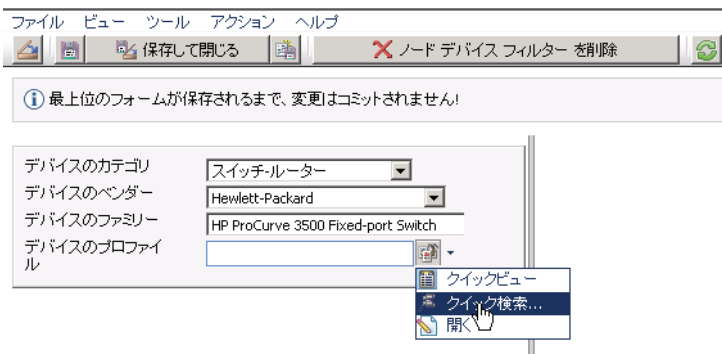
3 **【デバイスフィルタ】** タブをクリックします。フィルタ名に **global1** と入力し、**【注】** フィールドに作成するフィルタの説明を入力します。

The screenshot shows the NNMi configuration interface. The 'Device Filter' tab is selected and highlighted with a red circle. The 'Name' field is set to 'global1', and the 'Note' field contains 'Procure Switches を global1 に渡す'. The 'Device Filter' tab is highlighted with a red circle, and the 'Note' field is also circled in red. The interface includes a menu bar (File, View, Tools, Action, Help), a toolbar with icons for saving and deleting, and a main content area with various tabs and a list of filters.

- 4 **[新規作成]** アイコンをクリックして、[ノード デバイス フィルター] 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ます。

クイック検索 - デバイスのプロファイル

空にする

以下の 1 つを入力してください。

- [閉じる] アイコンをクリックして変更を行わず、前のフォームに戻ります。
- [空にする] アイコンをクリックして、オブジェクト インスタンスへの関連付けを削除します。
- [選択] をクリックします。この項目アイコン (テーブル行内) は、オブジェクト インスタンスとの関連付けを確立します。
- [クイックビュー] アイコン (テーブル行内) をクリックして、オブジェクト アイコンに関する詳細を表示します。

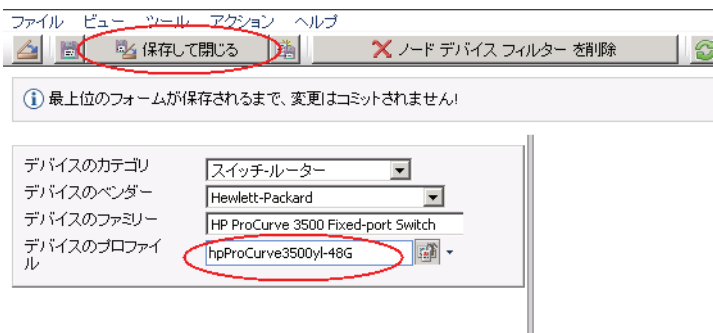
5315 の 3824 - 3835

デバイスのモデル	SNMP のオブジェクト ID	OUI	デバイスのファミリー	デバイスのベンダ...	デバイスのカ...
hpProCurve3500yl-48G	.1.3.6.1.4.1.11.2.3.7.11.59		3500 HP ProCurve 3500...	Hewlett-Packard	スイッチ...
クイックビューのツールチップ					
hpProCurve3500yl-48G					
SNMP のオブジェクト ID: .1.3.6.1.4.1.11.2.3.7.11.59					
デバイスのファミリー: HP ProCurve 3500 Fixed-port Switch					
デバイスのベンダー: Hewlett-Packard					
デバイスのカテゴリ: スイッチ-ルーター					
説明: HP ProCurve 3500yl-48G Switch (J8693A)					
			3500 HP ProCurve 3500...	Hewlett-Packard	スイッチ...
			3500 HP ProCurve 3500...	Hewlett-Packard	スイッチ...
			4100 HP ProCurve 4100...	Hewlett-Packard	スイッチ...
			4100 HP ProCurve 4100...	Hewlett-Packard	スイッチ...
			4200 HP ProCurve 4200...	Hewlett-Packard	スイッチ...
			4200 HP ProCurve 4200...	Hewlett-Packard	スイッチ...
			4200 HP ProCurve 4200...	Hewlett-Packard	スイッチ...
			4200 HP ProCurve 4200...	Hewlett-Packard	スイッチ...
			4200 HP ProCurve 4200...	Hewlett-Packard	スイッチ...
			4200 HP ProCurve 4200...	Hewlett-Packard	スイッチ...
			5300 HP ProCurve 5300...	Hewlett-Packard	スイッチ...
			5300 HP ProCurve 5300...	Hewlett-Packard	スイッチ...

8 3500yl HP ProCurve Switch のプロファイルを選択します。

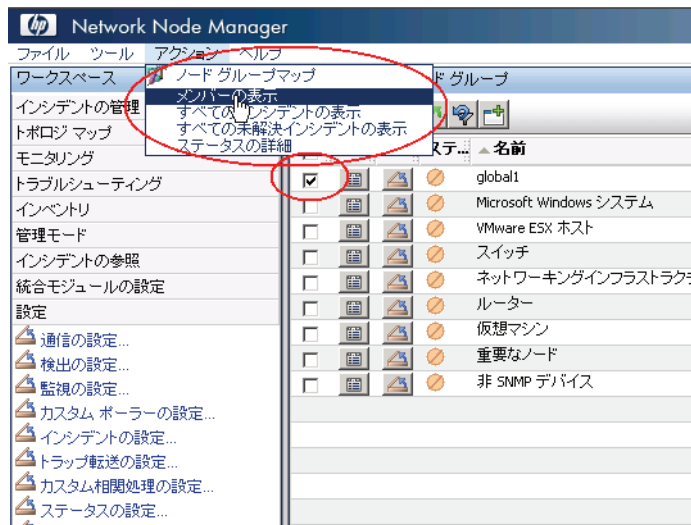


9 [保存して閉じる] を 2 回クリックします。



10 このフィルタをテストするため、[global1] を選択します。

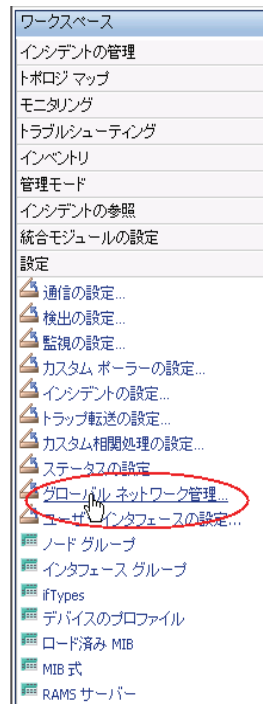
11 プルダウンメニューから、[メンバーの表示]をクリックします。



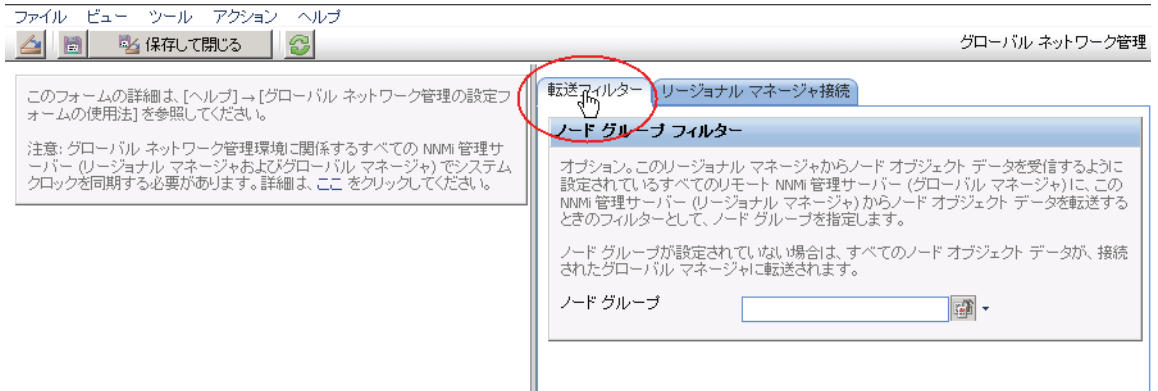
12 NNMi ではすでに HP 3500yl スイッチが 1 つ検出されています。これは、作成したフィルタが、設定した特定のスイッチ モデルを検索していることを示しています。次のステップでは、今作成したこのノードフィルタを使用して転送フィルタを設定します。



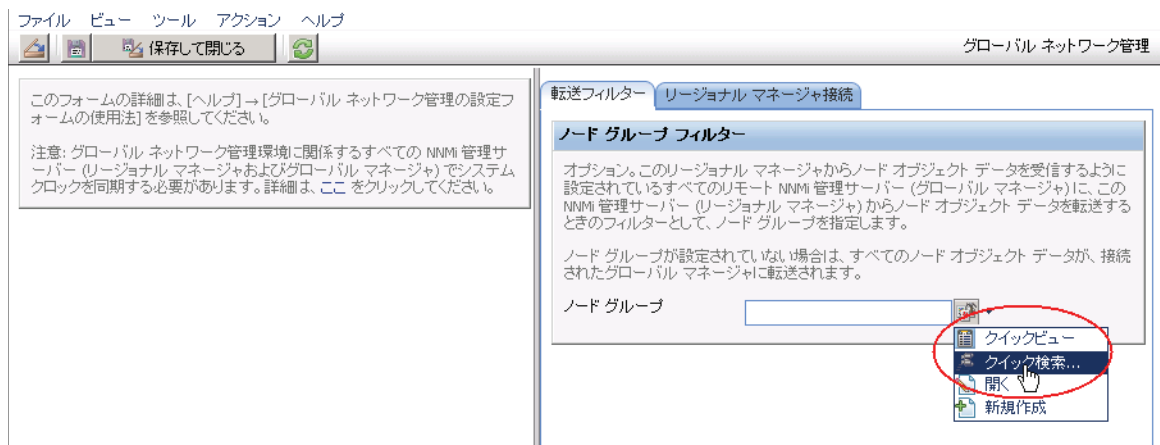
13 NNMi コンソールの regional1 の [設定] ワークスペースから、[グローバル ネットワーク管理] をクリックします。



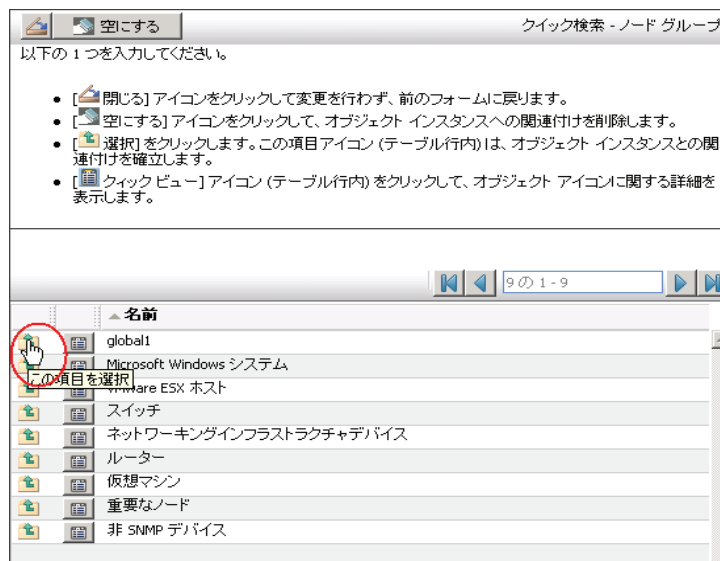
14 [転送フィルタ] タブをクリックします。



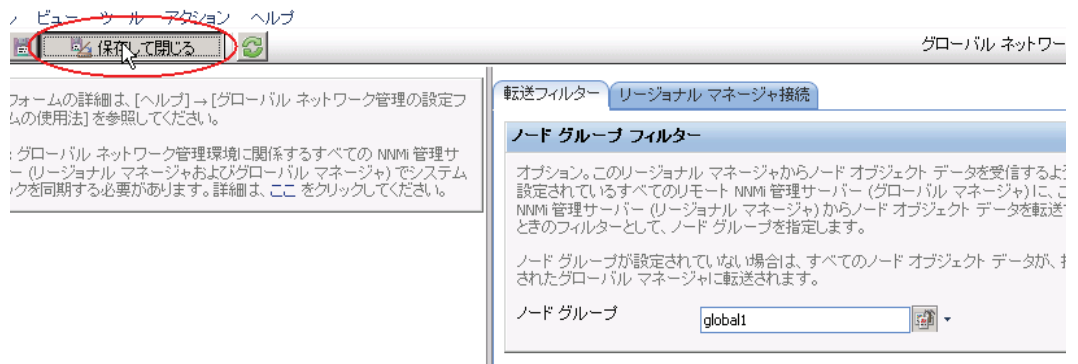
15 [クイック検索] をクリックします。



16 [global1] フィルタをクリックします。



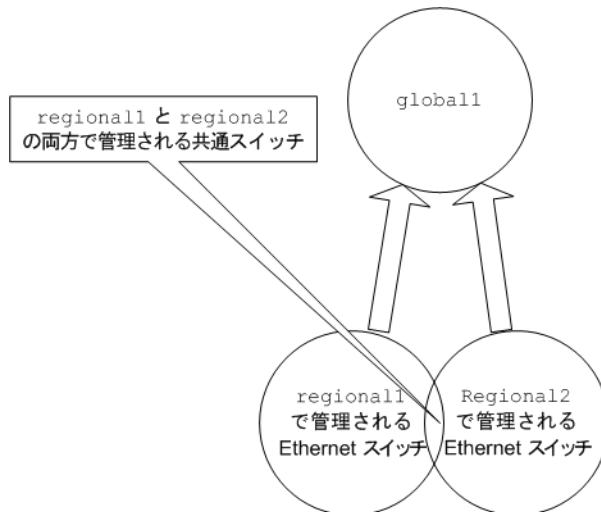
17 [保存して閉じる] をクリックします。



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 17 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モニタリングを行う 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 ネットワーク管理構成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。

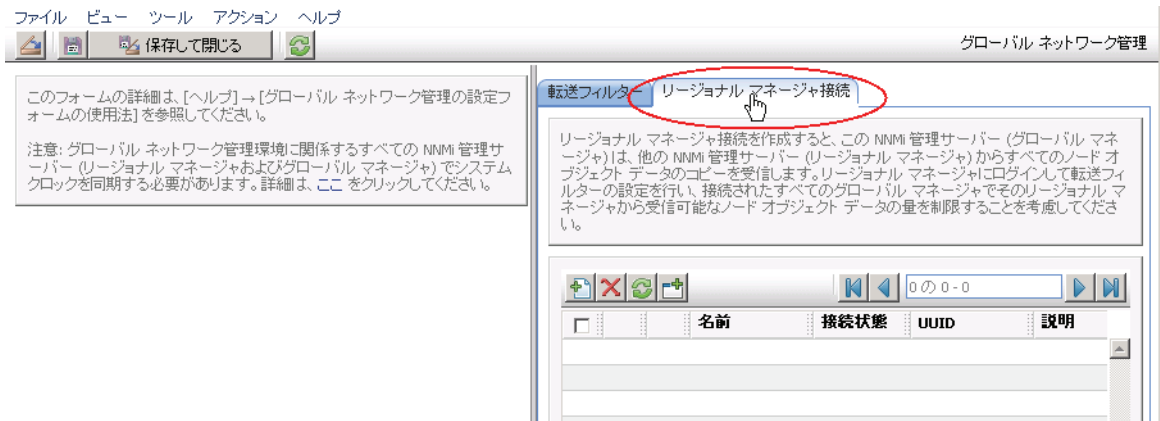



サーバー クロック同期の問題など、リージョナル マネージャとの接続に問題がある場合は、NNMi では警告メッセージが表示されます。

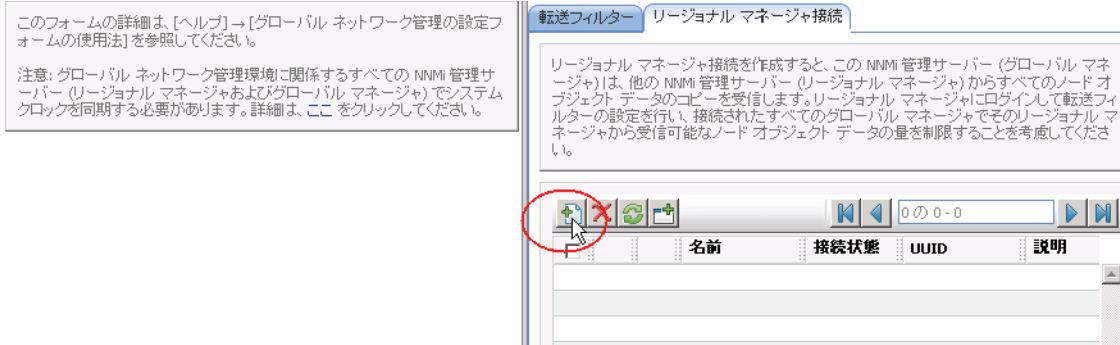
- 2 global1 から regional1 への接続を設定します。
 - a global1 の NNMi コンソールで、[設定] ワークスペースの [**グローバル ネットワーク管理**] をクリックします。




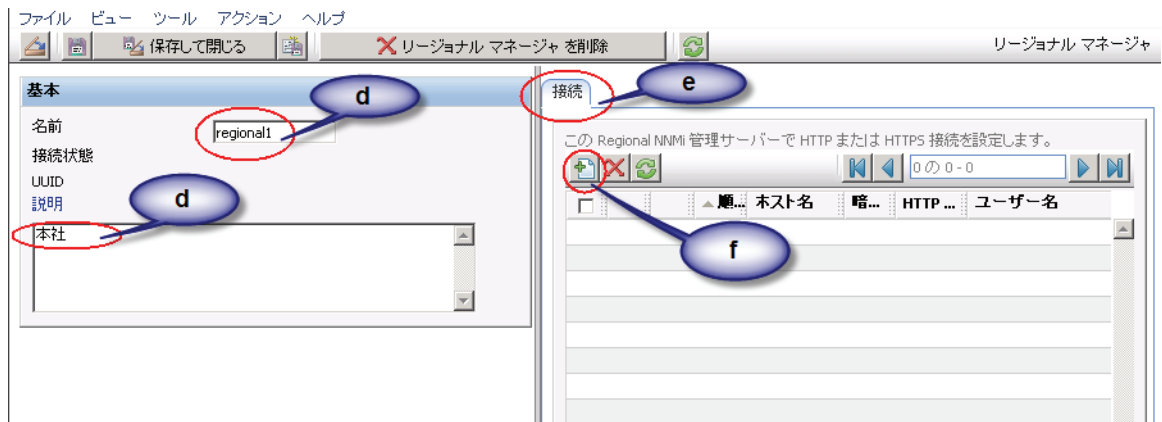
- b [**リージョナル マネージャ接続**] をクリックします。



- 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。

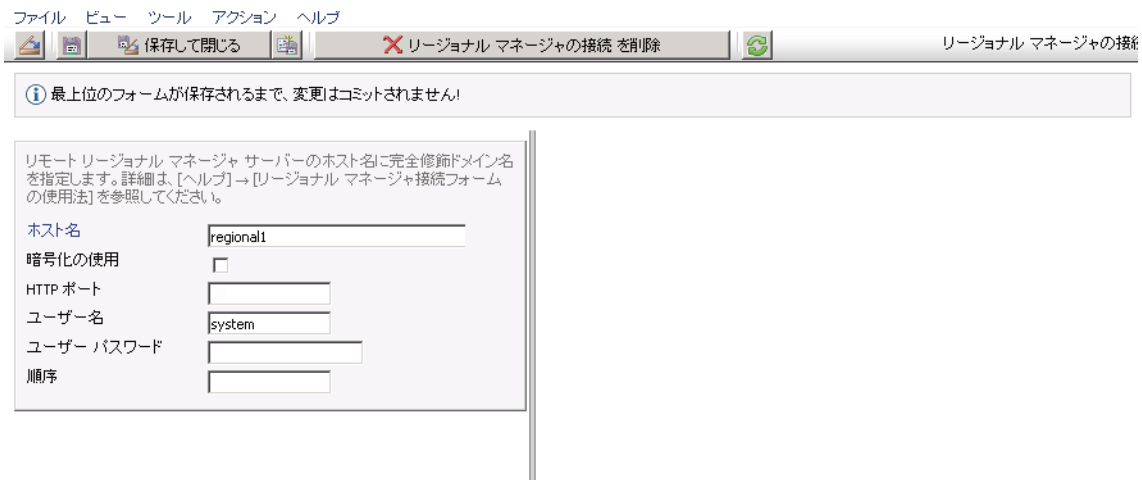


- d regional1 の名前と説明情報を追加します。
- e **[接続]** タブをクリックします。
- f  アイコンをクリックします。



- 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트리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 マネージャの接続 フォームの使用法**」を参照してください。



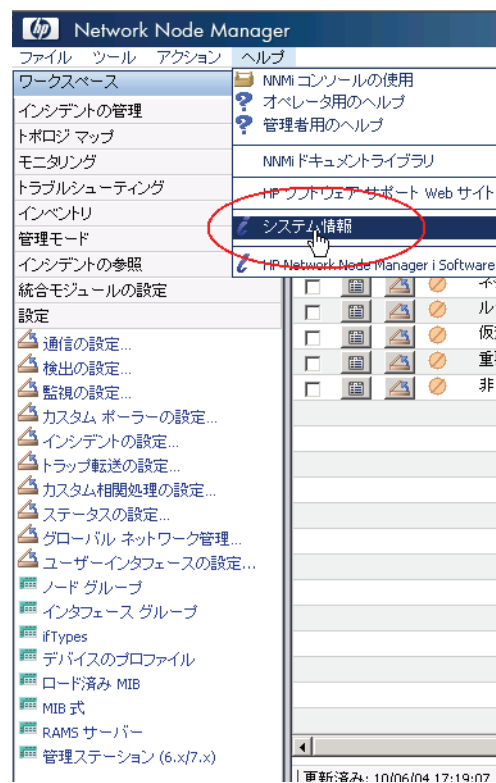
h [保存して閉じる] を 2 回クリックして作業を保存します。

- 3 global1 から regional2 への接続を確立するため、158 ページの手順 a から 159 ページの手順 g までを実行します。

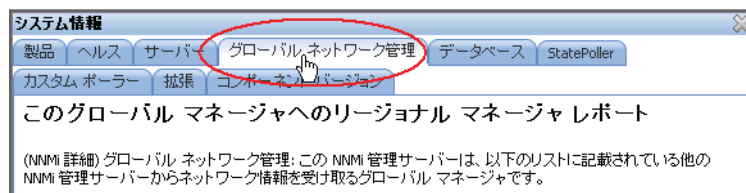
global1 から regional1 と regional2 への接続ステータスの判定

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 コンソールから、[ヘルプ]>[システム情報]をクリックします。



- 2 [グローバル ネットワーク管理] 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。[Connected] 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。

システム情報

製品 ヘルス サーバー グローバル ネットワーク管理 データベース StatePoller

カスタム ポーラー 拡張 コンポーネント バージョン

このグローバル マネージャへのリージョナル マネージャレポート

(NNMi 詳細) グローバル ネットワーク管理: この NNMi 管理サーバーは、以下のリストに記載されている他の NNMi 管理サーバーからネットワーク情報を受け取るグローバル マネージャです。

名前	接続状態	ノード カウント
regional1	Connected	28
regional2	Connected	28

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 global1 の NNMi コンソールで、[インベントリ] ワークスペースの [管理サーバーのノード] フォームに移動します。

hp Network Node Manager ユーザー名: system ユー...

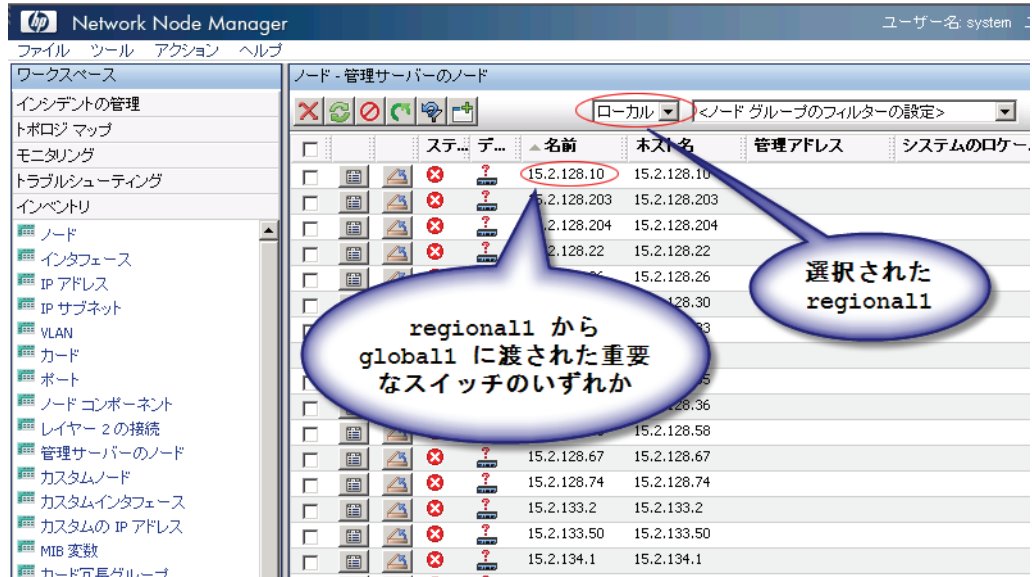
ワークスペース

インベントリ

ノード - 管理サーバーのノード

ステ...	デ...	名前	ホスト名	管理アドレス	システム
<input type="checkbox"/>		15.2.128.10	15.2.128.10		
<input type="checkbox"/>		15.2.128.203	15.2.128.203		
<input type="checkbox"/>		15.2.128.204	15.2.128.204		
<input type="checkbox"/>		15.2.128.22	15.2.128.22		
<input type="checkbox"/>		15.2.128.26	15.2.128.26		
<input type="checkbox"/>		15.2.128.30	15.2.128.30		
<input type="checkbox"/>		15.2.128.33	15.2.128.33		
<input type="checkbox"/>		15.2.128.34	15.2.128.34		
<input type="checkbox"/>		15.2.128.35	15.2.128.35		
<input type="checkbox"/>		15.2.128.36	15.2.128.36		
<input type="checkbox"/>		15.2.128.58	15.2.128.58		
<input type="checkbox"/>		15.2.128.67	15.2.128.67		
<input type="checkbox"/>		15.2.128.74	15.2.128.74		
<input type="checkbox"/>		15.2.133.2	15.2.133.2		
<input type="checkbox"/>		15.2.133.50	15.2.133.50		
<input type="checkbox"/>		15.2.134.1	15.2.134.1		
<input type="checkbox"/>		15.2.134.10	15.2.134.10		
<input type="checkbox"/>		15.2.134.11	15.2.134.11		
<input type="checkbox"/>		15.2.134.12	15.2.134.12		

- 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。

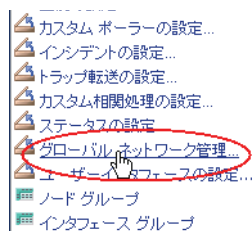


手順 1 から手順 2 を実行して、`global1` に接続されている他のリージョナルマネージャから `global1` に転送されたデバイス インベントリも表示します。

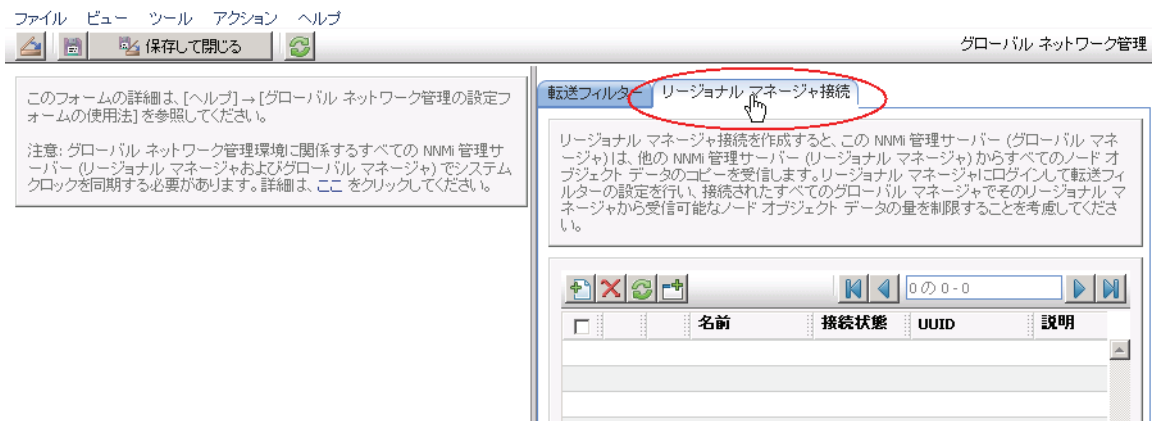
global1 と regional1 との通信の切断

`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。

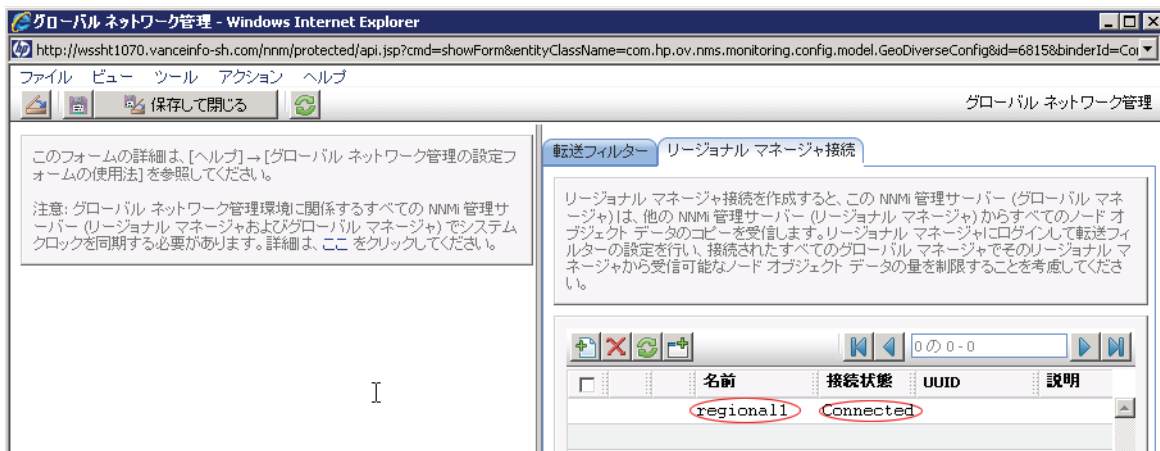
- 1 `global1` の NNMi コンソールで、[設定] ワークスペースの [グローバルネットワーク管理] をクリックします。



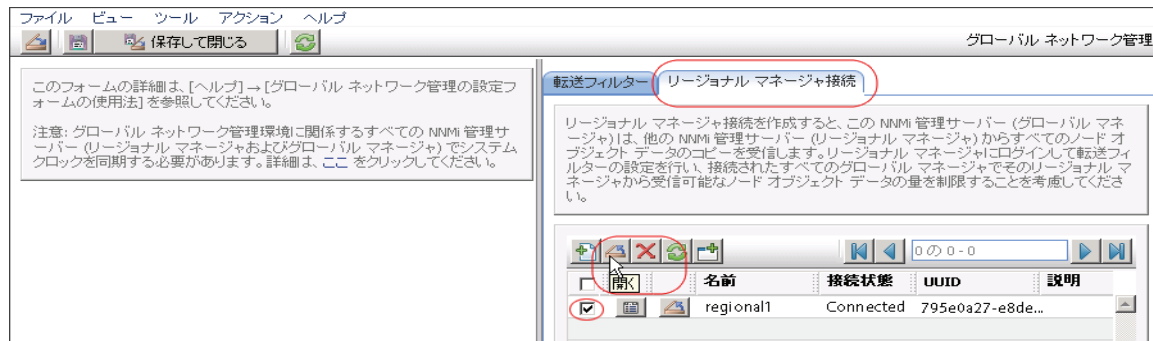
2 [リージョナル マネージャの接続] をクリックします。



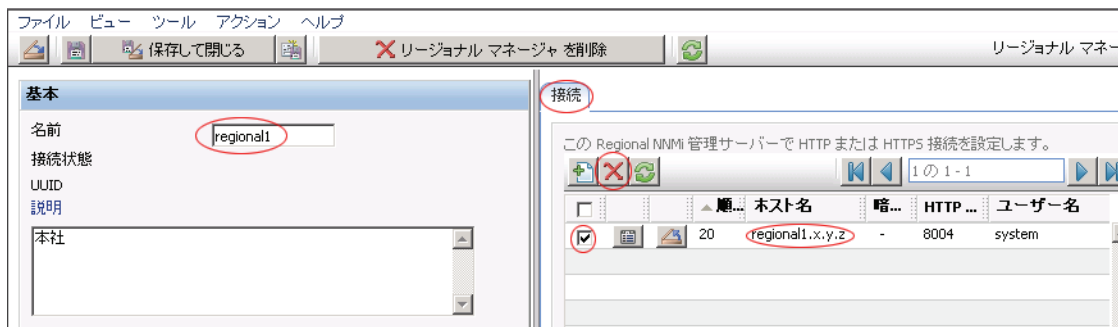
3 ステータスが [Connected] であることを確認します。ステータスが [Connected] ではない場合、処理を続行する前に、NNMi ヘルプの「グローバル ネットワーク管理のトラブルシューティング」を参照して問題を診断します。



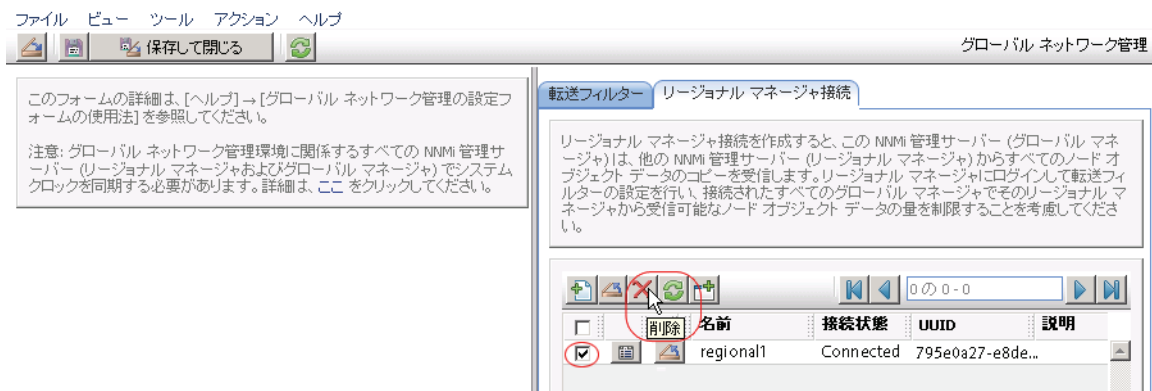
4 regional1 を選択して [開く] アイコンをクリックします。



- 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 マネージャの接続] タブでは、regional1 の [Name] 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。
- ワークスペース ナビゲーション パネルで、[設定] ワークスペースをクリックします。
  - [グローバル ネットワーク管理] フォームを選択します。
  - [リージョナル マネージャ接続] タブを選択します。
  - regional1 を選択して [削除] アイコンをクリックします。



- [保存して閉じる] をクリックして削除を保存します。
- 12 regional12 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。

### 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。ノードが `regional1` か `regional2` のいずれかにより管理されている場合、`global1` からのノード情報の要求による検出プロセスの複製は導入していません。

`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、同期することに大きく異なります。同期では、以下のような重要な計算と更新が行われます。

- `NNMi` は、**FDB**、**DOT1DPORT**、**IFACE\_STACK**、および **VLAN** データを更新します。
- `NNMi` は、レイヤ 2 **FDB** 接続分析を行います。

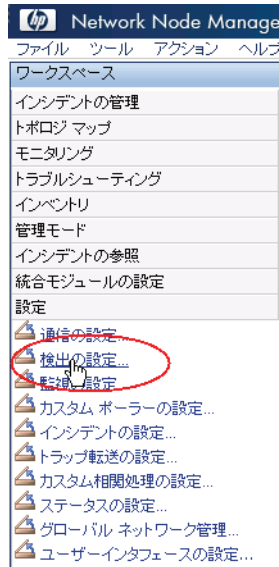
上記のリストは完全なリストではありませんが、`NNMi` が同期中に更新する主なデータのいくつかを示しています。



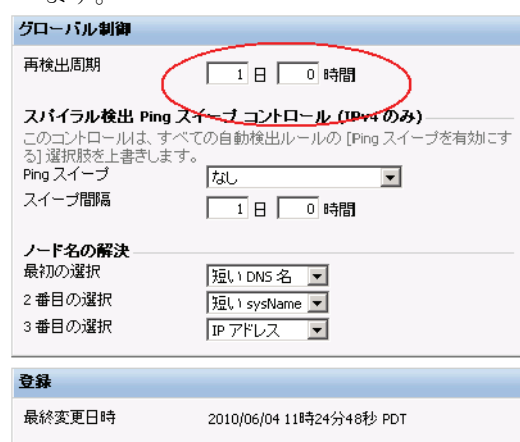
ユーザーが修正した属性やアプリケーションが修正した属性に対する変更は、グローバル サーバーでは同期中に更新されません。

再検出周期 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。[再検出周期] 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。[再検出周期] 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。[再検出周期] を設定するには、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 [ 検出の設定 ] をクリックします。



- 2 グローバルとリージョナルの再同期を行う頻度に従って [ 再検出間隔 ] 時間を調整します。



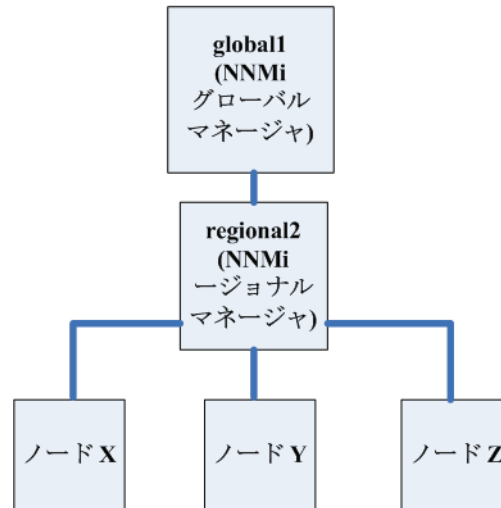
- 3 [ 保存して閉じる ] をクリックします。

## 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 regional2 が Node X を検出して管理し、グローバル NNMi 管理 global1 がリージョナル NNMi 管理 regional2 に接続すると想定します。

図 8 ノードのステータス ポーリングまたは設定ポーリング

### グローバル ネットワーク管理



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、モニタリング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は、トポロジに違いがある場合には、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。

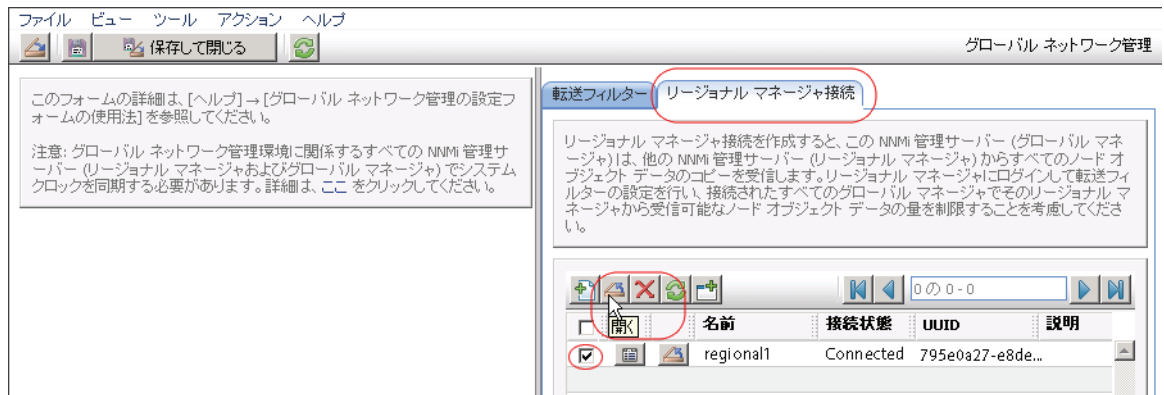
- 1 global1 の NNMi コンソールで、[設定] ワークスペースの [グローバル ネットワーク管理] をクリックします。



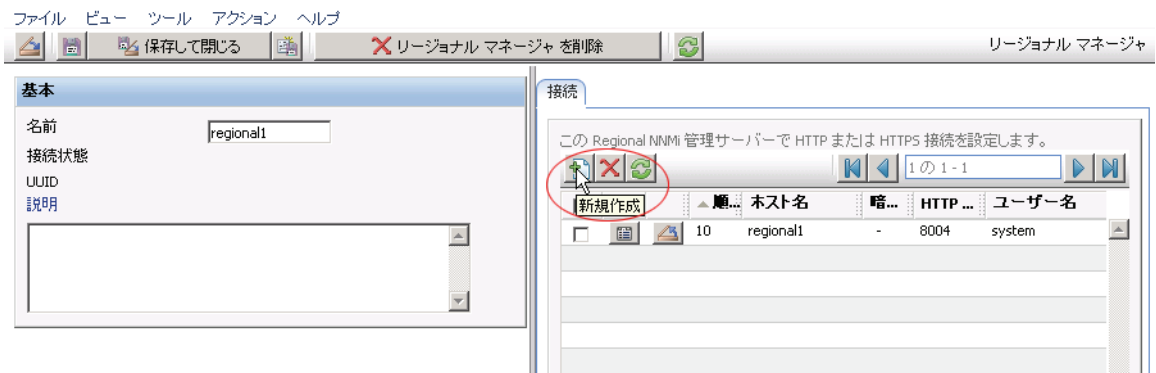
regional1 をアプリケーション フェイルオーバー用に設定し、セカンダリ サーバーとして regional1\_backup を設定したと想定します。

2 [リージョナル マネージャ接続] をクリックします。

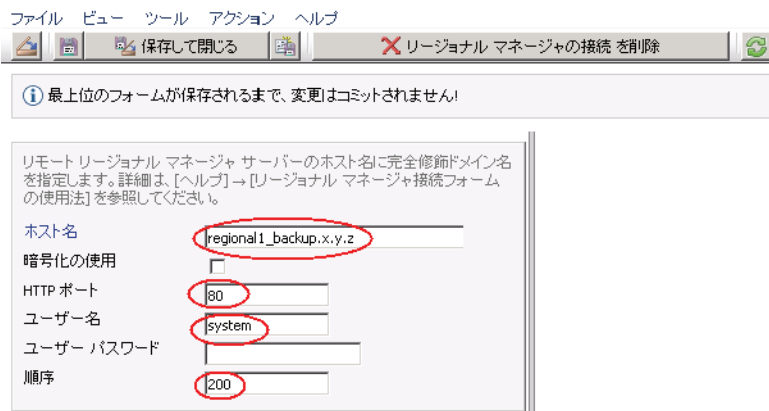
3 regional1 を選択して [開く] アイコンをクリックします。



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 `nnmnodediscover.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。

168 ページの図 8 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：  
**`nnmnodediscover.ovpl -u username -p password -rm regional2`** 詳細については、`nnmnodediscover.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 は正常に機能しません。これを解消するには、global1 で `nnmnodediscover.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。

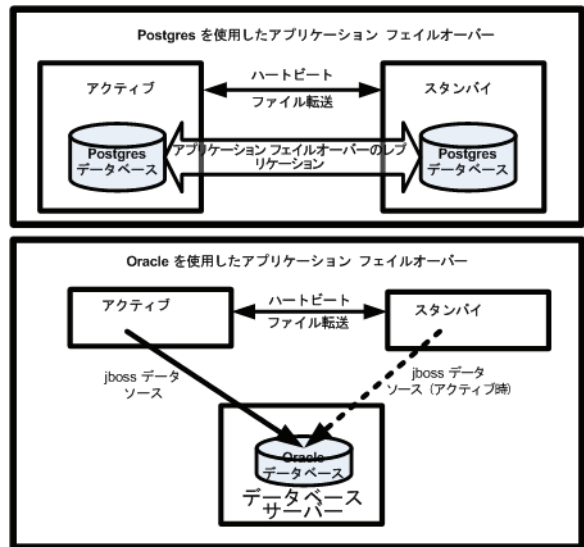
---

## グローバル ネットワーク管理と NNM iSPI またはサードパーティの統合

NNM iSPI またはサードパーティの統合は、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 regional1 と global1 の両方に配備できます。その他の NNM iSPI またはサードパーティの統合については、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 またはサードパーティの統合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 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
- 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 バージョン 9.00 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 9.00 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 管理サーバーで、同一の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、64 ページの「検出の評価」を参照してください。

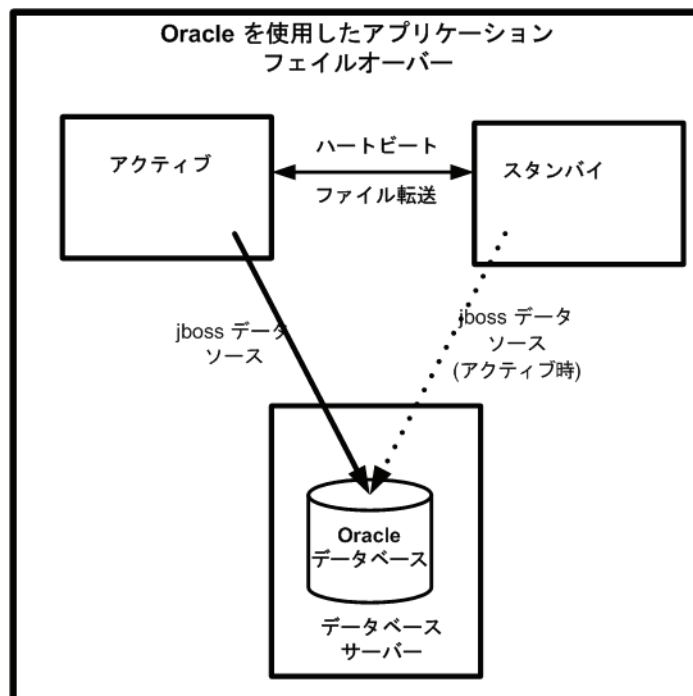
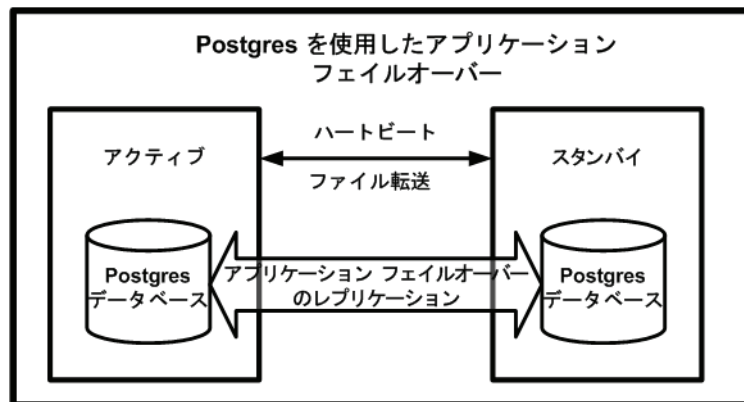
アプリケーション フェイルオーバーが正しく機能するには、アクティブ サーバーとスタンバイ サーバーは相互のネットワーク アクセスに制限のないことが必要です。この条件を満たしたら、175 ページの「アプリケーション フェイルオーバー構成の NNMi の設定」に示した手順を実行してください。詳細については、517 ページの「NNMi 9.00 および ウェルノウン ポート」を参照してください。



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 NNMi インストール ガイドの「NNMi ライセンスの取得」セクション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 アクティブおよびスタンバイ NNMi 管理サーバーが異なるサブネット内にある場合、nms-cluster.properties ファイルにさらに 2 つのパラメータを宣言する必要があります。

```
com.hp.ov.nms.cluster.protocol = TCP
```

```
com.hp.ov.nms.cluster.member.hostnames = fqdn_for_active,
fqdn_for_standby
```

- 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、97 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、102 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」に示した指示を実行します。

- 6 **UNIX**。サーバー Y が UNIX サーバーである場合、以下のコマンドを実行します。

```
chmod 400 $NnmDataDir/shared/nnm/certificates/nnm.keystore
```

- 7 **UNIX**。サーバー Y が UNIX サーバーである場合、以下のコマンドを実行します。

```
chmod 400 ¥
$NnmDataDir/shared/nnm/conf/nnmcluster/cluster.keystore
```

- 8 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
- 9 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。
  - アクティブ状態に変わります。
  - 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。
- 10 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 11 に進まないでください。
- 11 サーバー Y で NNMi クラスタ マネージャを開始します。
- nnmcluster -daemon**
- 12 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。
- 13 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。

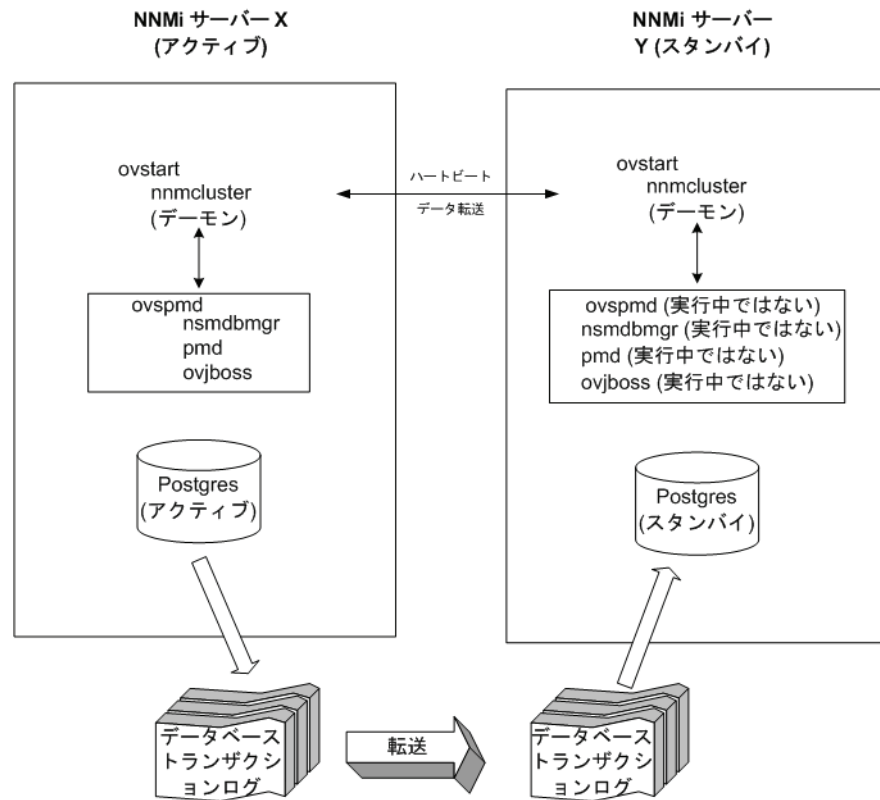
- **デーモンモード:** クラスタ マネージャのプロセスはバックグラウンドで実行し、`ovstop` および `ovstart` コマンドを使用して NNMi サービスを開始および停止します。
- **インタラクティブモード:** クラスタ マネージャは、NNMi 管理者がクラスタの属性を表示および変更できるインタラクティブセッションを実行します。たとえば、NNMi 管理者はこのセッションを使用して、アプリケーション フェイルオーバー機能を有効または無効にしたり、デーモンプロセスをシャットダウンしたりできます。
- **コマンドラインモード:** NNMi 管理者は、コマンドプロンプトでク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 9 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 9 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 ノードがプライマリ 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。

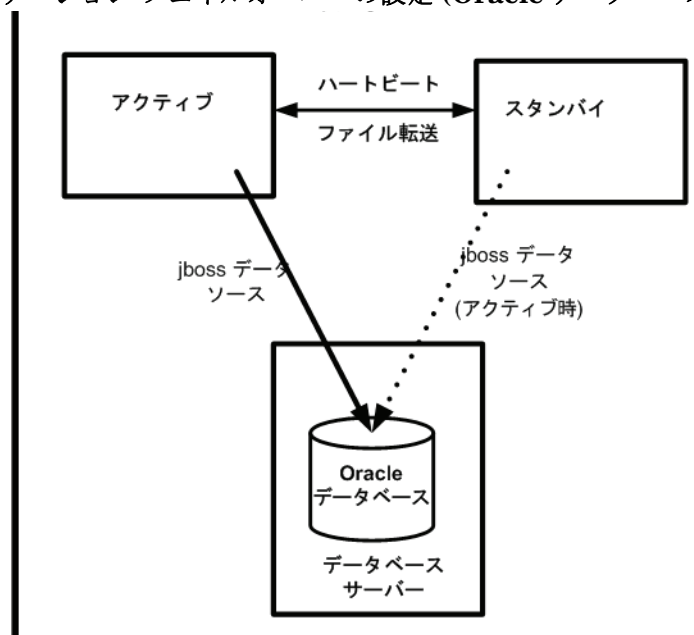
何らかの理由でアクティブ ノードが利用できなくなると、スタンバイ ノードは NNMi サービスを開始する ovstart コマンドを実行してアクティブになります。スタンバイ NNMi 管理サーバーは、残りの NNMi サービスを開始する前に、トランザクション ログをインポートします。

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 10 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 10 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働します。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 ノードとして稼働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、実際には NNMi は以下のコマンドを実行します。

- ovstart: **nmcluster -daemon**
- ovstop: **nmcluster -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 `nmcluster -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 `nmcluster -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 `nmcluster -halt` と同等です。

## アプリケーション フェイルオーバーのインシデント

`nmcluster` プロセスまたは `nmcluster` 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。

- ***NmClusterStartup***: 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。
- ***NmClusterFailover***: 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。

---

## 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 管理サーバーで実行する。
- 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 for QA、NNM iSPI for Metrics、および NNM iSPI 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 for QA、NNM iSPI for Traffic、または NNM iSPI 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 for Metrics、NNM iSPI for QA、または NNM iSPI 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` コマンドを実行します。詳細については、36 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、244 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: 万に備えて、アクティブ NNMi 管理サーバーで、`nnmcluster -syncdb` コマンドを実行し、コマンドが完了するまで待ちます。
- 4 `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。
- 5 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>
```

- 6 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

- 7 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
```

- 8 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

- 9 `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。
- 10 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、スタンバイ (クラスタに属しない) 状態の NNMi サービスが表示されます。
- 11 『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。
- 12 アクティブ NNMi 管理サーバーで `nmcluster -halt` コマンドを実行します。
- 13 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:*  
`%NmDataDir%\shared\nnm\conf\props\nms-cluster.properties`
  - *UNIX:* `$NmDataDir/shared/nnm/conf/props/nms-cluster.properties`
- 14 `com.hp.ov.nms.cluster.name` オプションをコメントアウトし、ファイルを保存します。
- 15 アクティブ NNMi 管理サーバーで `ovstart` コマンドを実行します。すると、スタンバイ (クラスタに属しない) 状態の NNMi サービスが表示されます。
- 16 『iSPI インストール ガイド』で説明されているとおりに、アクティブ NNMi 管理サーバーに NNM iSPI をインストールします。
- 17 アクティブおよびスタンバイ NNMi 管理サーバーの両方で、以下のファイルを編集します。
  - *Windows:*  
`%NmDataDir%\shared\nnm\conf\props\nms-cluster.properties`
  - *UNIX:* `$NmDataDir/shared/nnm/conf/props/nms-cluster.properties`
- 18 `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。
- 19 アクティブ NNMi 管理サーバーで `ovstart` コマンドを実行します。
- 20 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 `nmcluster -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」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 21 に進まないでください。
- 21 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。
- 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。

- 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。

- 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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
- 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。
- 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 サーバーでセカンダリ ノード 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、セカンダリ ノード 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、『**NNMi** インストールガイド』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 パッチ

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` コマンドを実行します。詳細については、36 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、244 ページの「バックアップ領域」を参照してください。
- 3 万に備えて、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、`syncdb` を入力し、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 管理サーバーは、前のメッセージで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 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。
- 7 アクティブ NNMi 管理サーバーで `ovstart` コマンドを実行します。
- 8 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。
- 9 `nnmcluster -syncdb` コマンドを実行して、新しいバックアップを作成します。
- 10 NNMi パッチをスタンバイ NNMi 管理サーバーに適用します。
- 11 スタンバイ NNMi 管理サーバーで `ovstart` コマンドを実行します。

- 12 NNM iSPI for QA、NNM iSPI for Metrics、または NNM iSPI 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。
- 13 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。スタンバイおよびアクティブ NNMi 管理サーバーを再起動する場合、プライマリ NNMi 管理サーバーを先に再起動します。

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 プライマリ NNMi 管理サーバーでデータベースを復旧します。
 - 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。246 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、クラスター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 24 時間) の間に莫大な数の 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)
```

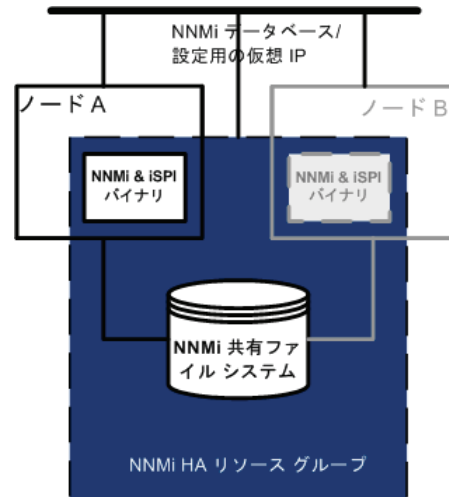
```
-----  
10 TxLogs/minute X 12 hours = 7200 TxLogs @ ~10MB = ~72GB
```

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バージニア州にあり、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。

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。(NNM iSPI for Traffic は、現在 HA では実行できません。)

この章では、HA 環境で実行する 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 の導入ガイド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。

- 190 ページの「サポート対象の HA 製品」
- 190 ページの「HA 用に NNMi を設定するための前提条件」
- 191 ページの「HA の概念」
- 197 ページの「HA の設定」
- 205 ページの「共有 NNMi データ」
- 207 ページの「HA クラスタ内の NNMi のライセンス契約」
- 208 ページの「HA 設定のメンテナンス」
- 212 ページの「HA の設定解除」
- 216 ページの「HA 下の NNMi のパッチ」
- 217 ページの「HA 下の NNMi を NNMi 8.1x から NNMi 9.00 にアップグレードする」
- 221 ページの「HA 設定のトラブルシューティング」
- 226 ページの「HA 設定リファレンス」

サポート対象の HA 製品

HA 下で NNMi を設定 / 実行するために使う、NNMi に付属しているコマンドは、各種のオペレーティング システム用の以下の HA 製品で動作します。

- **HP-UX:** HP Serviceguard バージョン 11.18 以降
- **Linux** の場合 :
 - Veritas Cluster Server (VCS) バージョン 5.0
 - HP Serviceguard バージョン 11.18
- **Solaris:** Veritas Cluster Server (VCS) バージョン 5.0
- **Windows:**
 - Windows Server 2008 対応 Microsoft フェールオーバー クラスタリング (MSFC)
 - Windows Server 2003 対応 Microsoft クラスタ サービス (MSCS)

この章で説明するテンプレートを使って、NNMi を他の HA 製品下で実行するように設定できますが、その設定に関する、クラスタ設定問題のサポートは行いません。

HA 用に NNMi を設定するための前提条件

特定のシステムを NNMi HA クラスタのノードとして追加するには、そのシステムは以下の要件を満たしている必要があります。

- 仮想 IP アドレス使用のサポート
- 共有ディスク使用のサポート
- 『HP NNMi Software システムとデバイス対応マトリックス』に記載されている NNMi のすべての要件に適合
- 以下の追加パッチのインストール
 - **Windows:**
 - 「Windows 2000 ベースのサーバー上の SMB 共有へのエイリアス名による接続が機能しない」に対する Microsoft の修正プログラムは <http://support.microsoft.com/?id=281308> からダウンロードできます。
 - **UNIX** の場合 : 追加要件はありません。
- 特定の HA 製品下で NNMi の実行を予定している場合、その製品のマニュアルに記載されている要件に適合

HA 用に NNMi を設定する前に、HA 製品のコマンドを使って、HA クラスタの設定とテストを行います。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。

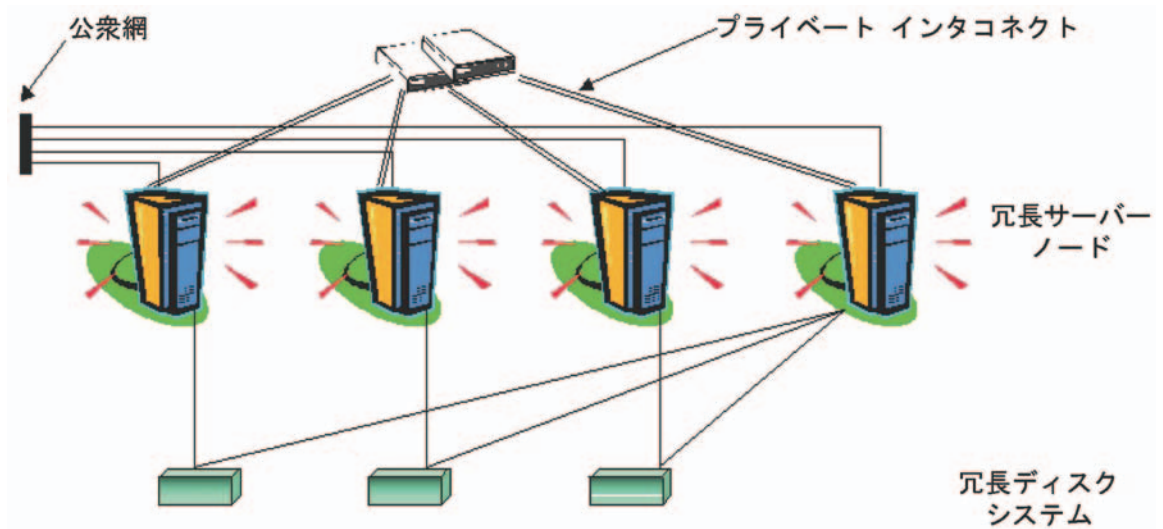
- (UNIX のみ) ssh
- (UNIX のみ) remsh
- DNS で解決可能な、HA クラスタ用の仮想 IP アドレス

- DNS で解決可能な、HA クラスタ用の仮想ホスト名

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 11 に、クラスタ アーキテクチャの例を示します。

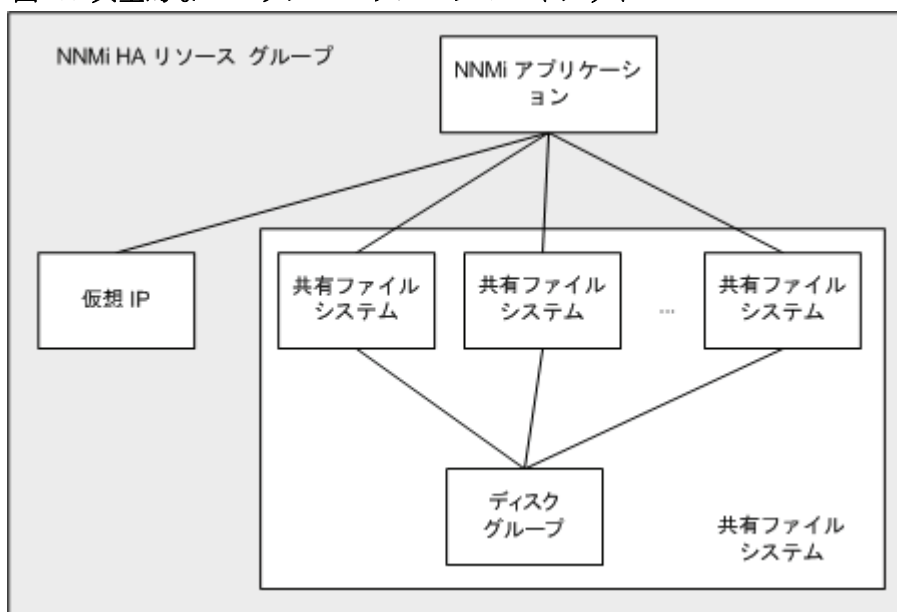
図 11 高可用性クラスタのアーキテクチャ



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ンネル)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 12 に、HA リソース グループの例を示します。

図 12 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 3 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、190 ページの「サポート対象の **HA 製品**」を参照してください。)

表 3 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
HP Serviceguard	SG	パッケージ
Veritas Cluster Server	VCS	サービス グループ
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
Microsoft Cluster Services	MSCS	リソース グループ

HA 用語集

表 4 に、一般的な **HA** 用語の定義を示します。

表 4 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 4 一般的な HA 用語 (続き)

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。

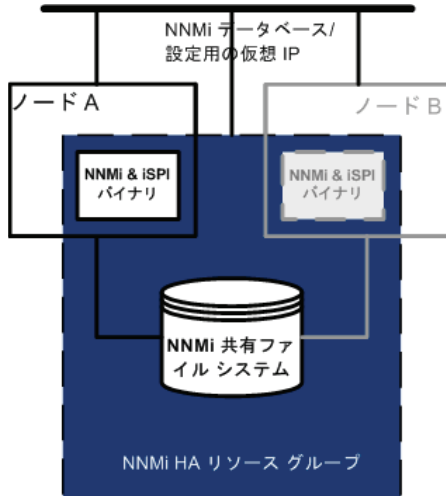
NNMi のみのシナリオ

図 13 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 13 のノード B と同様の設定を行います。

図 13 NNMi HA クラスタ用の基本的なシナリオ

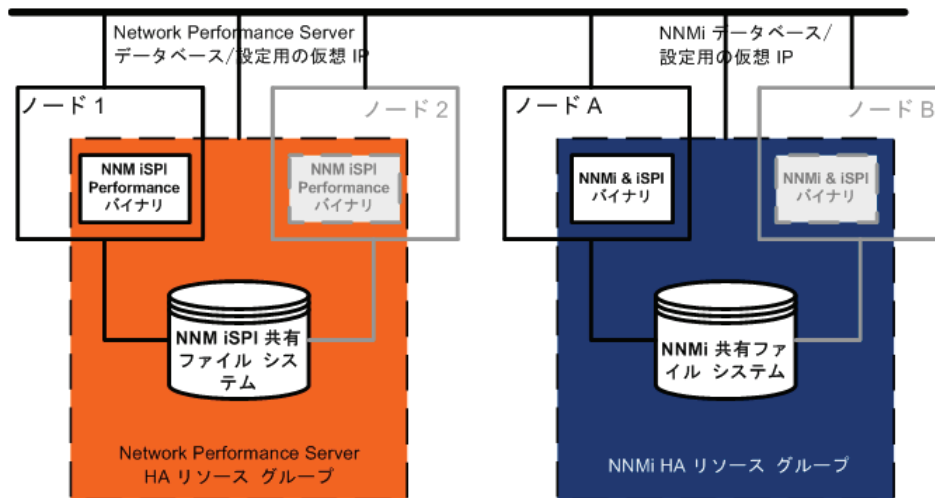


このシナリオの実装方法については、197 ページの「HA 用の NNMi の設定」と 202 ページの「HA 用の NNM iSPI の設定」を参照してください。

専用サーバーのシナリオでの NNMi と NNM iSPI Performance 製品

いずれかの NNM iSPI Performance 製品を専用サーバーで実行する場合は、図 14 のように、この NNM iSPI を NNMi HA クラスタ内で独立した HA リソース グループとして実行するように設定できます。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 14 専用サーバーでの NNMi と NNM iSPI Performance 製品用 HA



このシナリオの実装方法については、197 ページの「HA 用の NNMi の設定」と 202 ページの「HA 用の NNM iSPI の設定」を参照してください。

専用サーバーでの NNM iSPI Performance 製品のその他の選択肢は、以下のとおりです。

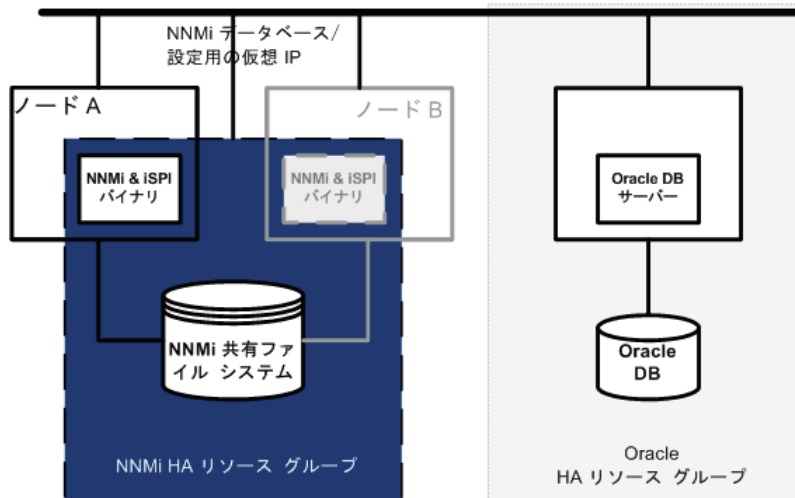
- NNM iSPI Performance 製品を HA を設定していない単一システムで実行します。このアプローチは、NNM iSPI を評価する場合、あるいは、パフォーマンス データが必ずしも必要ではない環境で使用します。
- NNM iSPI Performance 製品を NNMi 用とは異なる HA クラスタ下で実行するように設定します。この場合は、NNM iSPI Performance 製品の NNMi への依存関係を手動で管理する必要があります。

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 15](#) 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 15 Oracle データベースを使っている NNMi 用の HA

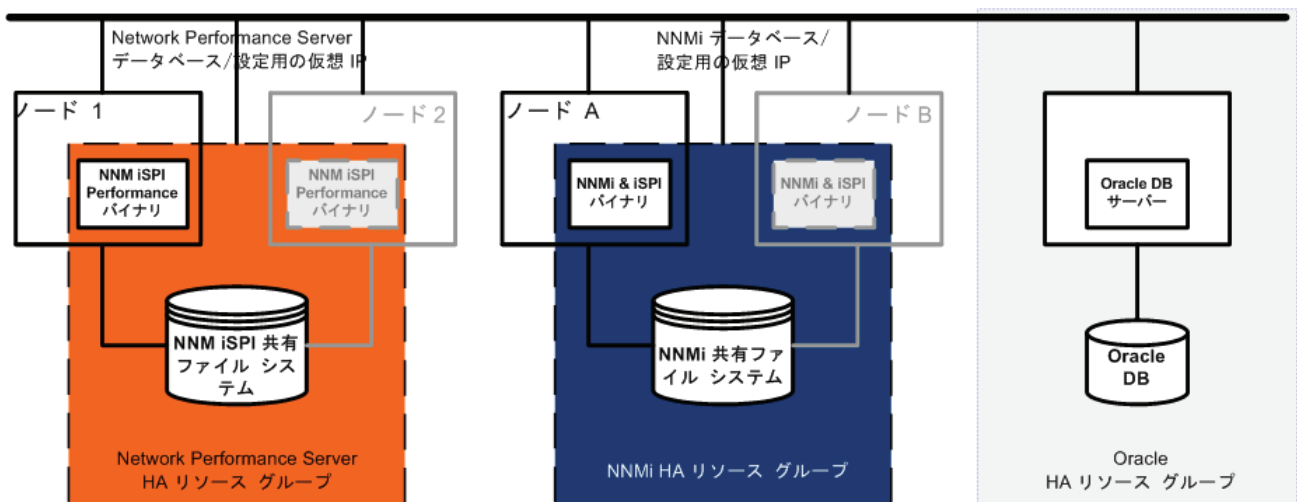


このシナリオの実装方法については、203 ページの「Oracle 環境での HA 用の NNMi の設定」と 202 ページの「HA 用の NNM iSPI の設定」を参照してください。

NNMi で Oracle データベースを使い、NNM iSPI Performance 製品を専用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い、いずれかの NNM iSPI Performance 製品を専用サーバーで実行する場合は、[図 16](#) のように、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 16 NNMi で Oracle データベースを使い、NNM iSPI Performance を専用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、203 ページの「Oracle 環境での HA 用の NNMi の設定」と 202 ページの「HA 用の NNMi 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`
- `nnmhastarttrg.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 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。

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。
 - 199 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 2 ～ 手順 12 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。
 - 199 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 13 ～ 手順 16 に従って、プライマリ ノードでこの作業を行います。
 - 201 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、セカンダリ ノードで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。

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 5 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 5 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。 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。 注記 : 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 設定スクリプトにより、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。

表 5 NNMi HA プライマリ ノードの設定情報

HA 設定項目	説明
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。例： <ul style="list-style-type: none"> • <i>Windows</i> の場合：ローカル エリア接続 • <i>HP-UX</i> の場合：lan0 • <i>Linux</i> の場合：eth0 • <i>Solaris</i> の場合：bge0
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。 <ul style="list-style-type: none"> • 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、206 ページの「共有ディスクの設定」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。 <ul style="list-style-type: none"> • <i>Windows</i> の場合：基本型 (206 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) • <i>HP-UX</i> の場合：vxfs • <i>Linux</i> の場合：HP Serviceguard には lvm2、VCS には ext2 • <i>Solaris</i> の場合：vxfs 他のフォーマットの物理的に接続されたディスクも、この HA 実装で動作すると考えています。そのため、標準のファイル システム タイプを使っている、物理的に接続されたディスクを持つ NNMi HA システムの分析についても、限定的にサポートしています。 注記: テストされていない共有ディスク フォーマットを使っている場合は、NNMi HA 設定スクリプトによって挿入された値が正しいことを確認するために、リソース グループ設定を調べてください。
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：nmmtest1-dg

表 5 NNMi HA プライマリ ノードの設定情報

HA 設定項目	説明
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。) 例 : <ul style="list-style-type: none"> • <i>Windows</i>: S:¥ • <i>UNIX</i>: /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 203 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。

- 1 システムが、190 ページの「HA 用に NNMi を設定するための前提条件」に示されているすべての要件を満たしていることを確認します。
- 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 202 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。例 :

```
nnmbackup.ovpl -type offline -scope all -target nnm_i_backups
```

このコマンドの詳細については、243 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 以下のファイルを別の場所にコピーして、NNMi のライセンス ファイルをバックアップします。
 - *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

6 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。例 :

- *MSFC* または *MSCS* の場合 : ディスクの管理を使って、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 :

次のように、**Symantec Veritas Storage Foundation** を使用します。

vxdiskadm を使って、ディスクを追加し、初期化します。

vxassist make を使って、領域ごとにディスクを割り当てます。

```
mkfs -F vxfs /dev/vx/dsk/<disk_group>/<logical_volume_group>
```

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>

7 共有ディスクのマウント ポイントになるディレクトリを作成します (たとえば、`s:¥` または `/nnmmount`):

- *Windows* の場合 : **Windows Explorer** とディスクの管理を使います。
- *UNIX* の場合 : 共有ディスクのマウント ポイントディレクトリが、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。例 :

```
ls -l /nnmmount
```

8 共有ディスクをマウントします。例 :

- *Windows* の場合 : ディスクの管理を使います。
- *Serviceguard* 用の *HP-UX* または *Linux* の場合 :

```
mount /dev/<disk_group>/<logical_volume> /nnmmount
```

- *VCS* 用の *Linux* または *Solaris* の場合 :

```
vxfs: mount /dev/vx/dsk/<disk_group>/<volume_group> /nnmmount
```

9 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。

10 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、223 ページの「すべてのクラスタノードの設定解除後に、HA 用の NNMi を再び有効にする」を参照してください。

- 11 共有ディスクをマウント解除します。
- *Windows* の場合 : *Windows Explorer* とディスクの管理を使います。
 - *UNIX*: `umount <HA_mount_point>`

- 12 (*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>
```

- 13 *NNMi* が実行中でないことを確認します。

```
ovstop -c
```

- 14 *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
```

197 ページの表 5 に、このコマンドに必要な情報を示します。

- 15 手順 14 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 (197 ページの表 5 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 16 を継続します。
- タイプ `none` を指定した場合は、206 ページの「共有ディスクの設定」に従って共有ディスクを設定し、手順 16 に進みます。

- 16 *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、221 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。

- 1 199 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 システムが、190 ページの「HA 用に *NNMi* を設定するための前提条件」に示されているすべての要件を満たしていることを確認します。

- 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。
- 4 199 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 7 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 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。

- 8 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。

- 9 オプションで、プライマリ ノードのリソース 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 for Metrics、NNM iSPI for QA、および NNM iSPI for Traffic

NNM iSPI Performance 製品 (NNM iSPI for Metrics、NNM iSPI for QA、および NNM iSPI for Traffic) は、NNMi 管理サーバーまたは専用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 iSPI Performance 製品が NNMi 管理サーバー上に置かれる場合、NNMi を HA 下で実行するよう設定する前に製品をインストールします。
- NNM iSPI Performance 製品が専用サーバー上に置かれる場合、製品をインストールする前に NNMi を HA 下で実行するよう設定します。NNM iSPI インストール プロセスの間は、NNMi 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提供します。

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 NNM iSPI の設定については、該当する NNM iSPI 導入ガイドを参照してください。

HA 下で実行中の 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 と NNMi

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 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 プロセス中は、NNMi リソース グループ仮想ホスト名を NNM サーバー ホスト名として提供します。

詳細は、『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 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、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 を使っている NNMi の HA 設定情報

Oracle と NNMi の両方を HA 下で実行する場合は、それぞれの製品を異なる HA リソースグループに設定する必要があります。Oracle リソースグループは、NNMi リソースグループを起動する前に、完全な起動状態になっている必要があります。両方の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 リソースグループでの NNMi リソースグループの依存関係を確認します。

NNMi リソースグループには、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む必要があります。

Oracle を使っている NNMi に HA を設定する

- 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、199 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、201 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、nmhadisk.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* の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` のマンページを参照してください。

共有ディスクの設定

共有ディスクがテスト済みのフォーマット (197 ページの表 5 にリスト) の場合は、HA 設定スクリプトによって共有ディスクが準備されるので、以下の手順はスキップします。

共有ディスクが、未検証の SAN や NFS 構成などを使っている場合は、共有ディスクを手動で準備する必要があります。HA の設定中にファイル システム タイプに値 `none` を指定し、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ます。例：

- **MSFC** または **MSCS** の場合：クラスタ アドミニストレータ (`cluadmin.exe`)、または `cluster.exe` コマンドを使って、リソース グループにリソースを追加します。
- **ServiceGuard** の場合：
 - **HP-UX** の場合：

```
/etc/cmcluster/<resource_group>/<resource_group>.cntl
```
 - **Linux** の場合：

```
/usr/local/cmcluster/conf/<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。

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、Microsoft Cluster Services を使っている Windows Server 2008 または Windows Server 2003 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 下で実行する場合は、NNMi の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。したがって、HA クラスタでは 1 つの NNMi ライセンスしか必要ではありません。

HA 用に NNMi ライセンスをインストールするには、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 コマンドプロンプトにて、以下のコマンドを入力します。
 - *Windows:* `%NnmInstallDir%\bin\nnmlicense.ovpl NNM -g`
 - *UNIX:* `$NnmInstallDir/bin/nnmlicense.ovpl NNM -g`
- 2 [License Password] ダイアログ ボックスで、[Request License] をクリックします。
- 3 画面の指示に従って、HA クラスタの仮想 IP アドレスに対応する、恒久ライセンスのパスワードを取得します。
- 4 コマンドプロンプトで以下のコマンドを入力し、システムをアップデートして、ライセンス データ ファイルを格納します。
 - *Windows:*
`%NnmInstallDir%\bin\nnmlicense.ovpl NNM -f <license_file>`
 - *UNIX:*
`$NnmInstallDir/bin/nnmlicense.ovpl NNM -f <license_file>`
- 5 共有ディスクの NNM ディレクトリ内のファイル licenses.txt (たとえば、S:%Nnm%\licenses.txt や /nnmount/NNM/licenses.txt) を、アクティブ ノードの次の場所にあるライセンス ファイル内の新しい情報を使ってアップデートします。
 - *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`

以下のいずれかを行います。

- このファイルが共有ディスクにある場合は、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。
- このファイルが共有ディスクにない場合は、LicFile.txt をアクティブ ノードから共有ディスクの NNM ディレクトリ内の licenses.txt にコピーします。

HA 設定のメンテナンス

メンテナンス モード

NNMi パッチを適用する必要がある場合、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 グループのモニタリングが無効になります。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

ファイルは空で構いません。

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 グループのモニタリング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、メンテナンスを開始するまでアクティブだったクラスタ ノードからメンテナンス 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って、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 アドレスが設定できますが、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。

管理サーバーのホスト名または 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 コマンド プロンプトにて、以下のコマンドを入力します。
 - **Windows:** %NnmInstallDir%\bin\nnmlicense.ovpl NNM -g
 - **UNIX:** \$NnmInstallDir/bin/nnmlicense.ovpl NNM -g
 - 2 **[License Password]** ダイアログ ボックスで、**[Request License]** をクリックします。
 - 3 画面の指示に従って、HA クラスタの新しい仮想 IP アドレスに対応する、恒久ライセンスのパスワードを取得します。
 - 4 コマンド プロンプトで以下のコマンドを入力し、システムをアップデートして、ライセンス データ ファイルを格納します。
 - **Windows:**
%NnmInstallDir%\bin\nnmlicense.ovpl NNM -f <license_file>
 - **UNIX:**
\$NnmInstallDir/bin/nnmlicense.ovpl NNM -f <license_file>
 - 5 共有ディスクの NNM ディレクトリ内のファイル licenses.txt (たとえば、S:\NNM\licenses.txt や /nmount/NNM/licenses.txt) を、アクティブ ノードの次の場所にあるライセンス ファイル内の新しい情報を使ってアップデートします。
 - **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
- 以下のいずれかを行います。
- このファイルが共有ディスクにある場合は、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。
 - このファイルが共有ディスクにない場合は、LicFile.txt をアクティブ ノードから共有ディスクの NNM ディレクトリ内の licenses.txt にコピーします。
- 6 208 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](#)」に従って、HA リソース グループをメンテナンス モードにします。

- 7 NNMi を停止します。

```
ovstop -c
```

- 8 NNMi 管理サーバーの 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

- 9 NNMi 管理サーバーのノード名を変更した場合、nnmsetofficialfqdn.ovpl コマンドでは NNMi 管理サーバーの新しい完全修飾ドメイン名を使用するよう NNMi を設定します。例:

```
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。

- 10 クラスタ設定情報を設定します。

- a 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>
```

- b 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* または *MSCS* の場合:

クラスタ アドミニストレータで、<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、<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。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。

```
HP-UX の場合: /etc/cmcluster/<resource_group>/  
<resource_group>.cntl
```

```
Linux の場合: /usr/local/cmcluster/conf/<resource_group>/  
<resource_group>.cntl
```

— *VCS* の場合:

```
$NnmInstallDir/misc/nnm/ha/nnmhargconfigure.ovpl NNM ¥  
<resource_group> -set_value <resource_group>-ip ¥  
Address <new_IP_address>
```

- c NNMi HA リソース グループを起動します。

- Windows:

- ```
%NnmInstallDir%\misc\%nm%ha%\nmhastarttrg.ovpl NNM ¥
<resource_group>
```

- UNIX:

- ```
$NnmInstallDir/misc/nm/ha/nmhastarttrg.ovpl NNM ¥  
<resource_group>
```

- 11 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。

- 12 208 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」に従って、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。

- 1 208 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」に従って、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 モニタリングを再起動します。

- 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。

- 3 208 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」に従って、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 の設定解除

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%\nmhaclusterinfo.ovpl %  
-group <resource_group> -activeNode
```

- *UNIX:*

```
$NnmInstallDir/misc/nnm/ha/nmhaclusterinfo.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 の導入ガイド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%\nmhaclusterinfo.ovpl %  
-config NNM -get NNM_ADD_ON_PRODUCTS
```

- *UNIX:*

```
$NnmInstallDir/misc/nnm/ha/nmhaclusterinfo.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。例：

```
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>
```

このコマンドによって、共有ディスクへのアクセス権は失われますが、ディスク グループやボリューム グループの設定が解除されるわけではありません。

- 5 各パッシブ ノードで、リソース グループ固有のファイルを削除します。

- *MSFC* または *MSCS* の場合:

Windows Explorer で、%NnmDataDir%\hacluster\<resource_group>\ フォルダ内のすべてのファイルを削除します。

- *Serviceguard* の場合:

- *HP-UX* の場合:

```
rm -rf /var/opt/OV/hacluster/<resource_group>/*  
rm -rf /etc/cmcluster/<resource_group>/*
```

- *Linux* の場合:

```
rm -rf /var/opt/OV/hacluster/<resource_group>/*  
rm -rf /usr/local/cmcluster/conf/<resource_group>/*
```

- *VCS* 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 の導入ガイドを参照してください。

- 7 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
```

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。

8 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。

9 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>
```

このコマンドによって、共有ディスクへのアクセス権は失われますが、ディスク グループやボリューム グループの設定が解除されるわけではありません。

10 アクティブ ノードで、リソース グループ固有のファイルを削除します。

- *MSFC* または *MSCS* の場合:

Windows Explorer で、%NnmDataDir%\hacluster\<resource_group>\ フォルダ内のすべてのファイルを削除します。

- *Serviceguard* の場合:

— *HP-UX* の場合:

```
rm -rf /var/opt/OV/hacluster/<resource_group>/*  
rm -rf /etc/cmcluster/<resource_group>/*
```

— *Linux* の場合:

```
rm -rf /var/opt/OV/hacluster/<resource_group>/*  
rm -rf /usr/local/cmcluster/conf/<resource_group>/*
```

- *VCS* の場合:

```
rm -rf /var/opt/OV/hacluster/<resource_group>/*
```

11 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も保管できます。
- 共有ディスクを別の目的で使う場合は、保管するデータをすべてコピーして（次の手順で説明）から、HA 製品のコマンドを使って、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。

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。例：

- *Windows* の場合 : Windows Explorer を使います。
- *UNIX*: `mount /dev/vgnnm/lvnm /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%\nmhadisk.ovpl NNM ¥  
-from <HA_mount_point>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhdisk.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。例：

- *Windows* の場合 : Windows Explorer を使います。
- *UNIX* の場合 : `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 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/nmhaclusterinfo.ovpl %  
-group <resource_group> -activeNode
```

- 2 アクティブ ノードで、以下の手順を実行します。

- a 208 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」に従って、HA リソース グループをメンテナンス モードにします。

- b NNMi を停止します。

```
ovstop -c
```

- c 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。

- d 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。例:

```
nnmbackup.ovpl -type offline -scope all -target nnm_i_backups
```

このコマンドの詳細については、243 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。

- e 該当する NNMi パッチをシステムに適用します。

- f NNMi を起動します。

```
ovstart -c
```

- g 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 各パッシブ ノードで、以下の手順を実行します。

- a 208 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」に従って、HA リソース グループをメンテナンス モードにします。

- b 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。

- c 208 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」に従って、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。

- 4 アクティブ ノードで、208 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」に従って、HA リソース グループをメンテナンス モードから取り出します。

HA 下の NNMi を NNMi 8.1x から NNMi 9.00 にアップグレードする

HA 下の NNMi 8.1x から NNMi 9.00 にアップグレードするには、HA の NNMi 8.1x の設定を解除して、NNMi 9.00 をインストールし、アップデートされたデータベース スキーマを取得して、HA 用に NNMi を再設定します。以下の手順に従ってください。

- 1 すべての HA ノードで、次に、それぞれのパッシブ ノードにフェイルオーバーを実行し、NNMi 8.1x の設定が同じになるようにします。
- 2 NNMi 8.1x 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%\nmhaclusterinfo.ovpl %  
-group <resource_group> -activeNode
```

- *UNIX:*

```
$NnmInstallDir/misc/nnm/ha/nmhaclusterinfo.ovpl %  
-group <resource_group> -activeNode
```

- 3 各パッシブ ノードで、NNMi 8.1x の設定を解除し、NNMi 9.00 をインストールします。

- a 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 の導入ガイドを参照してください。

- b 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%\nmhaclusterinfo.ovpl %  
-config NNM -get NNM_ADD_ON_PRODUCTS
```

- *UNIX:*

```
$NnmInstallDir/misc/nnm/ha/nmhaclusterinfo.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。例:

```
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 a を繰り返します。

- c HA クラスタの NNMi の設定を解除します。

- *Windows:*

```
%NnmInstallDir%\misc\%nnm%ha%\nmhaunconfigure.ovpl NNM %  
<resource_group>
```

- *UNIX:*

```
$NnmInstallDir/misc/nnm/ha/nmhaunconfigure.ovpl NNM %  
<resource_group>
```

このコマンドによって、共有ディスクへのアクセス権は失われますが、ディスク グループやボリューム グループの設定が解除されるわけではありません。

- d リソース グループ固有のファイルを削除します。
 - *MSFC* または *MSCS* の場合 :
Windows Explorer で、%NnmDataDir%\hacluster\<resource_group>* フォルダ内のすべてのファイルを削除します。
 - *Serviceguard* の場合 :
HP-UX の場合 :

```
rm -rf /var/opt/OV/hacluster/<resource_group>/*
```

```
rm -rf /etc/cmcluster/<resource_group>/*
```

Linux の場合 :

```
rm -rf /var/opt/OV/hacluster/<resource_group>/*
```

```
rm -rf /usr/local/cmcluster/conf/<resource_group>/*
```
 - *VCS* の場合 :

```
rm -rf /var/opt/OV/hacluster/<resource_group>/*
```
- e NNMi 9.00 と最新の NNMi 統合パッチ (がある場合) をインストールします。



この時点では、パッシブ ノードは NNMi 管理サーバーとして機能しません。アクティブ ノードも NNMi 9.00 にアップグレードされ、HA クラスタ下に再設定されるまでは、パッシブ ノードを HA クラスタに再設定しないでください。

- 4 アクティブ ノードで、NNMi 8.1x の設定を解除します。
 - 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 NNMi を停止します。

```
ovstop -c
```



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。

- c 共有ディスク上の NNMi データベースをバックアップします。

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

このコマンドの詳細は、NNMi 8.1x の『NNMi Deployment Guide (NNMi 導入ガイド)』の「NNMi 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。(nnmbackup.ovpl コマンドは、NNMi バージョン 8.13 で変更になりました。お使いのバージョンの NNMi の情報を必ず参照してください。)
- d 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\%nm%\ha\%nmhadisk.ovpl %
```

```
-from <HA_mount_point>
```
 - *UNIX*:

```
$NnmInstallDir/misc/nm/ha/nmhadisk.ovpl %
```

```
-from <HA_mount_point>
```

- e NNMi のファイルとディレクトリをすべて共有ディスクから移動します。
 - *Windows* の場合 : **Windows Explorer** を使って、共有ディスクのマウントポイント (%HA_MOUNT_POINT%、たとえば、S:¥) 下のファイルを %HA_MOUNT_POINT%¥8_10 など他の場所にすべて移動します。
 - *UNIX*:


```
cd $HA_MOUNT_POINT
mkdir 8_10
mv NNM 8_10/.
```

 NNM iSPI のディレクトリも 8_10 ディレクトリに移動します。
- f 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>
```
- g HA クラスタの NNMi の設定を解除します。
 - *Windows*:


```
%NnmInstallDir%¥misc¥nnm¥ha¥nnmhaunconfigure.ovpl ¥
<resource_group>
```
 - *UNIX*:


```
$NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl ¥
<resource_group>
```

このコマンドによって、共有ディスクへのアクセス権は失われますが、ディスクグループやボリューム グループの設定が解除されるわけではありません。
- h リソース グループ固有のファイルを削除します。
 - *MSFC* または *MSCS* の場合 :

Windows Explorer で、%NnmDataDir%¥hacluster¥<resource_group>¥ フォルダ内のすべてのファイルを削除します。
 - *Serviceguard* の場合 :

HP-UX の場合 :

```
rm -rf /var/opt/OV/hacluster/<resource_group>/*
rm -rf /etc/cmcluster/<resource_group>/*
```

Linux の場合 :

```
rm -rf /var/opt/OV/hacluster/<resource_group>/*
rm -rf /usr/local/cmcluster/conf/<resource_group>/*
```
 - *VCS* の場合 :


```
rm -rf /var/opt/OV/hacluster/<resource_group>/*
```
- i 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

- 5 HA から NNMi 8.1x の設定を解除する前はアクティブだったノードで、NNMi 9.00 を設定します。
 - a NNMi 9.00 をインストールします。

アップデートプロセスが NNMi を起動し、NNMi データベース スキーマをアップデートします。
 - b 最新の NNMi 統合パッチをインストールします。
 - c NNMi 9.00 が正しく実行中であることを確認します。
 - d NNMi 8.1x データを共有ディスクから削除します。
 - *Windows* の場合 : **Windows Explorer** を使って %HA_MOUNT_POINT%\8_10 フォルダを削除します。
 - *UNIX*:

```
cd $HA_MOUNT_POINT
rm -rf ./8_10
```
 - e 199 ページの「プライマリ クラスタ ノードでの NNMi の設定」の手順に従ってください。

以下の作業は不要です。

 - ディスク デバイス グループと論理ボリュームの定義
 - 共有ディスクのマウント ポイントの作成
 - 共有ディスクの設定
- 6 HA から NNMi 8.1x の設定を解除する前はパッシブだった各ノードで、NNMi 9.00 を設定します。
 - f 最初のセカンダリ ノードで、201 ページの「セカンダリ クラスタ ノードでの NNMi の設定」の手順を実行します。

共有ディスクのマウント ポイントの作成は不要です。

HA 設定のトラブルシューティング

一般的な HA のトラブルシューティング

ここでの内容は、すべての HP NNM i-suite Software 製品に適用されます。

エラー : Wrong Number of Arguments (引き数の数が間違っています)

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 の場合は、値 NNM を使います。
- NNM iSPI で使用する値を調べるには、NNM iSPI の該当する導入ガイドを参照してください。

製品スタートアップのタイムアウト (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。

HA リソース グループが特定のクラスタ ノードでは起動できない

nnmhangconfigure.ovpl コマンドで NNMi HA リソース グループを正常に起動 / 停止 / 切り替えできない場合は、次の情報を調べてください。

- **MSFC** または **MSCS** の場合：
 - クラスタ アドミニストレータで、リソースグループおよびそれを構成する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、システムが放置されていることです。

 - **HP-UX** の場合：`/etc/cmcluster/<resource_group>/<resource_group>.cntl.log`
 - **Linux** の場合：`/usr/local/cmcluster/conf/<resource_group>/<resource_group>.cntl.log`
- **VCS** の場合：
 - `/opt/VRTSvcs/bin/hares -state` を実行して、リソースの状態を調べます。
 - 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。

原因となっているリソースを特定できない場合は、**HA** 製品のコマンドを使って、**HA** リソース グループを手動で起動します。

- 1 共有ディスクをマウントします。
- 2 ネットワーク インタフェースに仮想ホストを割り当てます。
 - **MSFC** または **MSCS** の場合：
 - クラスタ アドミニストレータを起動します。
 - 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：
 - **HP-UX** の場合：`/usr/sbin/cmmodnet` を実行して、IP アドレスを追加します。
 - **Linux** の場合：`/usr/local/cmcluster/bin/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>`

3 HA リソース グループを起動します。例：

- *Windows:*

```
%NnmInstallDir%\misc\nnm\ha\nnmhastart.ovpl NNM ¥  
-start <resource_group>
```

- *UNIX:*

```
$NnmInstallDir/misc/nnm/ha/nnmhastart.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。

すべてのクラスタ ノードの設定解除後に、HA 用の NNMi を再び有効にする

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、226 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

以下のいずれかの状況が発生しています。

- NNMi を HA 用に設定した後、ovspmd が起動しません。(ovstatus は ovspmd が実行中でないことを示します。)
- ovstart または ovstop から、以下のメッセージが返されます。

```
ovstart: OVW クライアントで実行する場合には、名前でマネージャを指定する必要があります
```



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。

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>
- NNM_HA_CONFIGURED=YES
- HA_RESOURCE_GROUP=<resource_group>
- 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>

ov.conf ファイルの場所は、226 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、-to オプションを付けた nnmhadisk.ovpl コマンドを実行した直後に NNMi を起動した場合に発生します。(nnmhaconfigure.ovpl コマンドが実行されていません。)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。

nnmhaconfigure.ovpl を実行してから、HA 設定を完了します。

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

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などを見て、これらの製品を混在させて使うことが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。

フェイルオーバー後にセカンダリ ノードで共有ディスク ファイルが見つからない

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。

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 のトラブルシューティングについては、その NNM iSPI の導入ガイド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 6 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 6 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 7 と表 8 に、NNMi に付属している HA 設定スクリプトを示します。表 7 に示した NNMi 付属のスクリプトは、カスタム 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 7 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 7 NNMi HA 設定スクリプト (続き)

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 クラスタで NNMi 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 クラスタの NNMi 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 8 に示した NNMi 付属のスクリプトは、226 ページの表 7 に示したスクリプトで使用します。表 8 に示したスクリプトは直接実行しないでください。

表 8 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。
nnmhamsocs.vbs	MSFC または MSCS の HA クラスタで、NNMi プロセスを起動 / 停止 / 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、%NnmDataDir%\%hacluster%\<resource_group%\hamsocs.vbs に格納され、MSFC または MSCS で使われます。

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
- **Serviceguard** 用の **Linux** 実行時：
 - /usr/local/cmcluster/conf/<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/log/cmcluster
これは、クラスタの問題点に関するログ ファイルです。
 - /var/log/messages*
これらは、リソースの問題点 (ディスクと IP アドレス) に関するログ ファイルです。
 - \$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
<code><resource_group>-app</code>	<ul style="list-style-type: none"> • /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*
<code><resource_group>-dg</code> <code><resource_group>-volume</code> <code><resource_group>-mount</code>	<ul style="list-style-type: none"> • /var/VRTSvcs/log/DiskGroup_A.log • /var/VRTSvcs/log/Volume_A.log • /var/VRTSvcs/log/Mount_A.log • /var/adm/messages*
<code><resource_group>-ip</code>	<ul style="list-style-type: none"> • /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。

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 アドレスの検出とモニタリングが可能になります。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 デバイスに対する IPv4、IPv6 通信 (管理アドレス) の自動選択
 - nms-jboss.properties ファイル内での設定可能な項目の検出
- IPv6 アドレス フォルト モニタリング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
 - モニタリングの設定
 - 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 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 スイープの使用
- 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 導入リファレンス』、『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 システムである必要があります。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、管理する必要がある 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 で検出とモニタリングを行うデバイスと 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、*NNMi インストールガイド*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 9 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
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 をサポートしている 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。詳細については、235 ページの「**NNMi のインストール**」を参照してください。

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 ステータスのモニタリングなど、**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、*NNMi インストール ガイド* 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 オプションで、デュアルスタック管理ノードに対して **SNMP** 管理アドレス設定を指定できます。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。これを行うには、`nms-jboss.properties` ファイルにある以下の行をコメント解除します。

```
com.hp.nnm.snmp.ipVersionPreference=IPv4
```

次に、プロパティ値を、IPv4、IPv6 または None (推奨できません) に設定します。この領域で**設定**の変更を行わない場合、**SNMP** 管理アドレス設定は、デフォルトで IPv4 となります。

- d nms-jboss.properties ファイルを保存して閉じます。
- 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。
- 5 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

6 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。nmmnoderediscover.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、nmmnoderediscover.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モニタリングを開始します。

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。

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 モニタリング

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 アドレスのモニタリングをすぐに停止します。NNMi はこうしたアドレスの IP アドレスの状態を、[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 [モニタの設定] ルールで [IP アドレス障害のポーリング] が有効になっている場合でも、NNMi は「障害 ICMP ポーリングが有効になっています: 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 **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、**SNMP IPv6** ノードを削除します。ライセンス 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「非管理対象」とマークされているノードの管理モードを変更します。nmmmanagementmode.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、nmmmanagementmode.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。nmmnoderediscover.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、nmmnoderediscover.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「非管理対象」とマークされているノードの管理モードを変更します。nmmmanagementmode.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、nmmmanagementmode.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「非管理対象」から「管理対象」に変更したノードを検出できるようにします。nmmnoderediscover.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、nmmnoderediscover.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。

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 で使用する Telnet および SSH プロトコルを設定する
- NNMi 管理サーバーの変更

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 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。
- `nnmbakupembdb.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` — `nnmbakupembdb.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。

- `nmresetembdb.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。

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、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、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 10 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 10 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 10 のリストに示すファイル システム内の NNMi 設定情報と、表 11 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。



現在、カスタム ポーラー データベース テーブルは、完全バックアップにのみ含まれています。

表 10 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/nnm	その他の設定情報
\$NnmInstallDir/misc/nms/lic	その他のライセンス情報
\$NnmInstallDir/newconfig	インストール設定ステージング領域
\$NnmInstallDir/nonOV/jboss/nms/server/nms/conf	jboss の設定
\$NnmInstallDir/nonOV/jboss/nms/server/nms/deploy	jboss 配備ディレクトリ
\$NnmInstallDir/snmp_mibs (Windows のみ)	SNMP MIB の情報

表 10 設定領域ファイルとディレクトリ (続き)

ディレクトリまたはファイル名	説明
\$NnmDataDir/conf	他の HP 製品が共有する設定
\$NnmDataDir/HPOvLIC/LicFile.txt	ライセンス情報
\$NnmDataDir/NNMVersionInfo	NNMi バージョン情報ファイル
\$NnmDataDir/share/snmp_mibs (UNIX のみ)	SNMP MIB の情報
\$NnmDataDir/shared/nnm/certificates	共有 NNMi SSL 証明書
\$NnmDataDir/shared/nnm/conf	共有 NNMi 設定情報
\$NnmDataDir/shared/nnm/conf/licensing	共有 NNMi ライセンス設定情報
\$NnmDataDir/shared/nnm/lrf	共有 NNMi コンポーネント登録ファイル

表 11 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。

バックアップ データを、ある NNMi 管理サーバーから 2 番目の NNMi 管理サーバーに配置することは、どちらのサーバーのデータベース UUID も同じであることを意味します。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、nmrestore.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)
- **OS** のタイプとバージョン
- 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。以下の項目が両方のシステムで同じである必要があります。

- **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、nmrestore.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、ライセンスのマニュアル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行う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。例：

```
nmbackup.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 [247](#) 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。

```
nmrestore.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、[247](#) 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。

```
nmrestore.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 ([244](#) 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。例：

```
nmbackup.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。

```
nmrestore.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くするため、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。例：

```
nmmbackup.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、247 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。

```
nmrestore.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。

```
nmrestore.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、nmbackupembdb.ovpl コマンドと nmrestoreembdb.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。nmbackupembdb.ovpl コマンドと nmrestoreembdb.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

nmresetembdb.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、*nmresetembdb.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。

- 251 ページの「カスタム ポーラー収集のエクスポートの管理」
- 253 ページの「インシデント アクションの管理」
- 255 ページの「NNMi 正規化プロパティの変更」
- 257 ページの「NNMi コンソールとの HTTPS のみ通信を設定する」

カスタム ポーラー収集の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/nm/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\%nmaction.properties
 - **UNIX:** \$NNM_PROPS/shared/nmaction.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/nmaction.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¥nmmaction.properties
 - \$NNM_PROPS/shared/nmmaction.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せて調整します。
- 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。

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** クイック スタート設定ウィザードを実行する前、または **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推奨します。

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 **nnmnodediscover.ovpl -all** スクリプトを実行できます。詳細については、**nnmnodediscover.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%\nnm-topology.properties
 - **UNIX:** \$NNM_PROPS/nnm-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.HOSTNAME_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、**nnmnode rediscover.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。

NNMi コンソールとの HTTPS のみ通信を設定する

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ア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 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、[ヘルプ] > [システム情報] をクリックしてから、[ヘルス] 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。
- **nmmhealth.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`**

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)。デフォルトでは、Microsoft Internet Explorer も Mozilla Firefox のどちらでも telnet コマンドは定義されないため、[Telnet]メニュー項目を使用すると、エラーメッセージが生成されます。telnet、セキュア シェル (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。


- 259 ページの「Telnet メニュー項目の無効化」
- 260 ページの「ssh プロトコルを使用する新規メニュー項目の設定」
- 260 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」
- 267 ページの「Linux で Telnet または SSH を使用する Firefox の設定」
- 268 ページの「Windows レジストリを変更するファイル例」

Telnet メニュー項目の無効化

導入環境で NNMi ユーザーが NNMi コンソールからの telnet 接続を必要としない場合は、[Telnet]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。

管理対象デバイスに対する SSH 接続の新規メニュー項目の作成の詳細については、260 ページの「ssh プロトコルを使用する新規メニュー項目の設定」を参照してください。

NNMi コンソールの [Telnet]メニュー項目の無効化は、NNMi 管理サーバー上で NNMi コンソールにサインインするすべてのユーザーに適用されます。[Telnet]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 インタフェース設定]をクリックします。
- 2 [メニュー項目]タブで、[Telnet... (クライアントから)]行を選択してから、[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。

ssh プロトコルを使用する新規メニュー項目の設定

NNMi コンソールのセキュア シェル アクセスの新規メニュー項目の設定は、この NNMi 管理サーバー上で NNMi コンソールにサインインするすべてのユーザーに適用されます。

以下のメニュー項目コンテキストを含む**[アクション]**メニュー上に新規メニュー項目を作成します。

- ノードオブジェクト タイプの場合は、フル URL を **ssh://\${hostname}** に設定します。
- IP アドレスオブジェクト タイプの場合は、フル URL を **ssh://\${value}** に設定します。

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。

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]>[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-bit Edition]** 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。

タスク 12 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 12 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	<ul style="list-style-type: none"> 262 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」 263 ページの「サードパーティ Telnet クライアント (標準 Windows)」 265 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	<ul style="list-style-type: none"> 263 ページの「サードパーティ Telnet クライアント (標準 Windows)」 265 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	<ul style="list-style-type: none"> 264 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)」 265 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)」
Internet Explorer 64 ビット	64 ビット	<ul style="list-style-type: none"> 262 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」 263 ページの「サードパーティ Telnet クライアント (標準 Windows)」 265 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	<ul style="list-style-type: none"> 262 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」 263 ページの「サードパーティ Telnet クライアント (標準 Windows)」 265 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	<ul style="list-style-type: none"> 263 ページの「サードパーティ Telnet クライアント (標準 Windows)」 265 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	<ul style="list-style-type: none"> 264 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)」 265 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、268 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。例：

```
"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、[今後 telnet リンクは同様に処理する] 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 <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¥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、[今後 telnet リンクは同様に処理する] 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、[今後 telnet リンクは同様に処理する] 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://」を記述するスクリプトが含まれます。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。

- 6 260 ページの「ssh プロトコルを使用する新規メニュー項目の設定」で説明した ssh プロトコルを呼び出す新規 NNMi コンソール メニュー項目を作成します。

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/nmtelnet 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/nmtelnet
```

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、**[新規作成]** をクリックしてから、**[真偽値]** 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/nmtelnet を選択します。
- c **[今後 telnet リンクは同様に処理する]** 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/nmssh` 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/nmssh
```
- 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、**[新規作成]** をクリックしてから、**[真偽値]** 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/nmssh` 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、262 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 %1"
```

nnmputtytelnet.reg の例

このレジストリの内容例は、263 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" %1"
```

nnmtelnet32on64.reg の例

このレジストリの内容例は、264 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" %1"
```

nnmssh.reg の例

このレジストリの内容例は、265 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" %1"
```


NNMi 管理サーバーの変更

他のシステムで HP Network Node Manager i Software 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できますし、NNMi 管理サーバーのハードウェアを変更できます。

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
- 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くするため、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。例：

```
nmmbackup.ovpl -type offline -scope all ¥  
-target nmi_backups¥offline
```

247 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。

```
nmrestore.ovpl -source nmi_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、272 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

`nmconfigexport.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、`nmconfigimport.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。



`nmconfigimport.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、`nmconfigexport.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。



`nmconfigexport.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、`nmconfigexport.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 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) クラスター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

次に、以下のタスク グループのいずれかを実行します。

- 有効な **nnm.keystore** ファイルをリストアする
- 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。

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にて、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にて、以下のコマンドを入力します。

```
nnmlicense.ovpl NNM -f license.txt
```


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關与、または高可用性 (HA) クラスターのメンバーの場合は、サポート担当者にお問い合わせください。

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の変更
- タスク 4: 新規証明書による HTTPS 設定の更新
- 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、276 ページの「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。

- 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の変更

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。例:

```
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: 新規証明書による HTTPS 設定の更新

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。

例:

```
<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。

例:

- 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。

NNMi 9.00 へのアップグレード

表 13 に示した情報に従って、NNMi をアップグレードできます。表 13 の情報は、NNMi 管理サーバー上の NNMi バージョン 8.10 以降の使用を想定して記載されています。

表 13 サポート対象の NNMi アップグレード

NNMi バージョン	NNMi 9.0x へのアップグレード
8.10	対応
8.10 パッチ 1	対応
8.1x パッチ 2 (NNMi 8.11)	対応
8.1x パッチ 3	対応
8.1x パッチ 4 (NNMi 8.12)	対応
8.1x パッチ 5 (NNMi 8.13)	対応
8.1x パッチ 6	対応
8.1x パッチ 7	対応

サポート対象の NNMi 8.10 へのアップグレードパスを表示するには、表 14 を参照してください。NNMi 8.10 より古いバージョンの NNM がインストールされている場合、NNMi 9.00 に直接アップグレードします。

表 14 サポート対象の NNMi アップグレード (NNMi 8.10 へ)

現在のバージョン	NNMi 8.02 へのアップグレード	NNMi 8.03 以降へのアップグレード*	NNMi 8.10 へのアップグレード
NNMi 8.01	対応	対応	NNMi バージョン 8.10 をインストールします。
NNMi 8.02	該当なし	対応	NNMi バージョン 8.10 をインストールします。
NNMi 8.03 以上 *	該当なし	該当なし	NNMi バージョン 8.10 をインストールします。

* NNMi 8.1x を除く NNMi パッチをインストールするには、パッチ インストールの指示を参照してください。

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、オペレーティングシステムの NNMi 8.0x または 8.1x から NNMi 9.0 へアップグレードする。
- 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の NNMi 8.0x または 8.1x から NNMi 9.0 にアップグレードする。

- **Red Hat Linux 4.6 から 5.2 または 5.3 への NNMi の移行。** NNMi 9.00 は、Red Hat Linux 4.6 をサポートしていません。NNMi 9.00 にマイグレーションする前に、オペレーティング システムを Red Hat Linux 5.2 または 5.3 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 9.00 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 9.00 にアップグレードするプロセスを説明します。

この章には、以下のトピックがあります。

- NNMi 8.0x からの起動
- 既存の NNMi 管理サーバー を NNMi 9.00 にアップグレード

NNMi 8.0x からの起動

NNMi 管理サーバーをバージョン 8.10 以降へアップグレードします。既存の NNMi 管理サーバー を NNMi 9.00 にアップグレード の指示に従って続行します。

既存の NNMi 管理サーバー を NNMi 9.00 にアップグレード

*NNMi インストール ガイド*と 295 ページの「追加アップグレード情報」の NNMi 9.00 「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。

以下の手順では、NNMi 管理サーバーから NNMi 9.00 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 管理サーバーで実行する NNMi 8.10 以降を想定しています。

- 1 nnnbackup.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、*nnnbackup.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、万が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 9.00** 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 バージョン 9.00 にアップグレードするプロセスを説明します。

この章には、以下のトピックがあります。

- NNMi 8.0x からの起動
- 別の NNMi 管理サーバーへのアップグレード

NNMi 8.0x からの起動

NNMi 管理サーバーをバージョン 8.10 以降へアップグレードします。別の NNMi 管理サーバーへのアップグレードの指示に従って続行します。

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 295 ページの「追加アップグレード情報」の NNMi 9.00 「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、既存の NNMi 管理サーバーで NNMi 8.10 以降を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 9.00 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、293 ページの「NNMi Oracle データの移行」を参照してください。

- 1 万に備えて、既存 (ソース) の **NNMi 8.1x** 管理サーバーを `nmbbackup.ovpl` スクリプトを使用してバックアップします。この **8.1x** のバックアップにラベルを付けます。詳細については、**NNMi 8.1x** の `nmbbackup.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する場合は、**Oracle** データベース管理者に **NNMi 8.1x** 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 9.00** と最新の統合パッチ (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 9.00** 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 `nmbbackup.ovpl` スクリプトを使用して、**NNMi 9.00** 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 9.00** 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 9.00** の `nmbbackup.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、**NNMi 9.00** および最新の統合パッチ (ある場合) をターゲットの **NNMi** 管理サーバー上に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 `nmmrestore.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、`nmmrestore.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。
- 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。

Red Hat Linux 4.6 から 5.2 または 5.3 への NNMi の 移行

NNMi 9.00 は、Red Hat Linux 4.6 をサポートしていません。NNMi 9.00 にマイグレーションする前に、オペレーティングシステムを Red Hat Linux 5.2 または 5.3 に変更する必要があります。

Red Hat Linux 4.6 サーバーで NNMi 8.1x パッチ 6 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 Red Hat Linux 5.2 または 5.3 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。

Red Hat Linux 4.6 から Red Hat Linux 5.2 または 5.3 への NNMi の変更

Red Hat Linux 4.6 から Red Hat Linux 5.2 または 5.3 への NNMi の変更

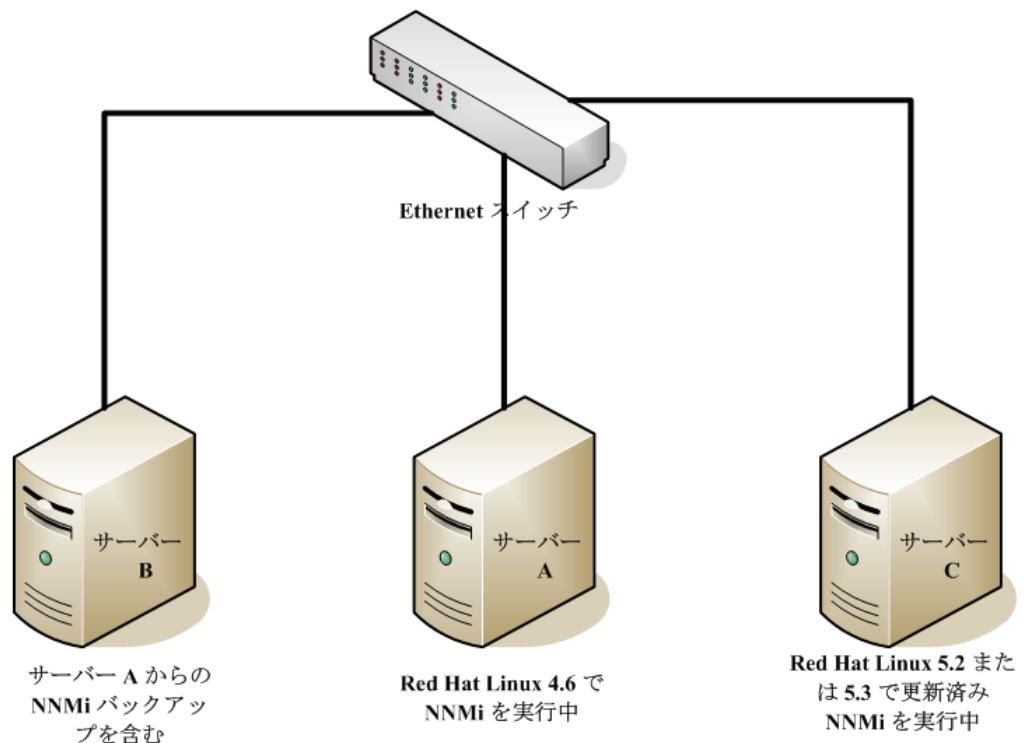
以下の手順を実行するには、Linux Red Hat 4.6 サーバーで NNMi 8.1x パッチ 6 以降が実行されている必要があります。NNMi のバージョン番号を調べるには、**[Network Node Manager i-series について]** ウィンドウで現在のパッチ レベルを書き留めます。バージョンが 8.13.006 以降であることを確認します。それ以前のバージョンの場合は、次に進まないでください。次に進む前に、NNMi 8.1x パッチ 6 以降をインストールする必要があります。

NNMi 8.1x パッチ 6 以降が実行されている NNMi 管理サーバーを、Red Hat Linux 4.6 から Red Hat Linux 5.2 または 5.3 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、Linux Red Hat 4.6 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、Linux Red Hat 5.2 または 5.3 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 /etc/hosts ファイルに、以下のエントリがあることを確認してください。

```
127.0.0.1 localhost
```



- 2 Server A で、`nnmbackup.ovpl -type online -scope all -target /tmp/bak/all` 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、243 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、Red Hat Linux 5.2 または 5.3 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 Red Hat Linux 5.2 または 5.3 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 8.10 をインストールします。
この手順の実行方法については、『*NNMi 8.1x Patch 4 Installation Guide for Linux*』の『*Installing NNMi 8.10 on Red Hat 5.2*』を参照してください。
- 6 Server C で、8.1x パッチ 6 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。
- 7 Server B で、NNMi のバックアップを Server C にコピーします。
- 8 Server C で、`nnmrestore.ovpl -force -source /tmp/bak/all` 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、243 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。

- 9 **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。276 ページの「**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。

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必要があるとします。たとえば、NNMi データを Oracle 10g データベースから Oracle 11g データベースに移行する場合などです。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。

- Oracle 10g データベースに接続された、最新のパッチが適用済みの NNMi 8.1x を NNMi 9.00 にアップグレードする必要がある
- Oracle 10G または Oracle 11G データベースに接続された NNMi 9.00

実施する必要がある 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。

- 既存の Oracle インスタンスが Oracle 10G または 11G を実行している。
- 新しい Oracle インスタンスが Oracle 10G または 11G を実行している。既存の Oracle 11G インスタンスは、Oracle 10G には戻せません。
- 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 8.1x は Oracle 11G サーバーに接続できません。

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、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 8.1x から NNMi 9.0 にアップグレードする場合は、『HP Network Node Manager i Software 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 9.00 を使用している場合は、これらの手順に従って、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 9.00 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
- 機能面の相違点

設定面の相違点

アップグレードすると、以前のバージョンの NNMi の設定ファイルの多くが、新しい保存場所にあることがわかります。

- アップグレード後、NNMi 9.00 の動作に影響するほとんどのプロパティ ファイルは、以下の場所にあります。
 - *Windows:* %NNM_DATA%\shared\%nnm%\conf\%props
 - *Windows:* %NNM_DATA%\%conf%\%nnm%\props\
 - *UNIX:* \$NNM_DATA/shared/nnm/conf/props
 - *UNIX:* \$NNM_DATA/conf/nnm/props/
- ヒープ サイズなど、ovjboss プロセスの起動 JVM オプションを変更するには、以下のファイルを編集します。
 - *Windows:* %NNM_DATA%\shared\%nnm%\conf\%props%\ovjboss.jvmargs
 - *UNIX:* \$NNM_DATA%/shared/nnm/conf/props/ovjboss.jvmargs
- トラップ サーバー プロパティを変更するには、以下のファイルを編集します。
 - *Windows:*
%NNM_DATA%\shared\%nnm%\conf\%props%\nnmtrapserver.propertiesWindows
 - *UNIX:* \$NNM_DATA/shared/nnm/conf/props/nnmtrapserver.properties

- **NNMi 9.00** へアップグレード中、**NNMi** では `nms-jboss.properties` ファイルの内容が保持されます。`ovjboss.jvm.properties` ファイルの保存場所が以下のように変わりました。
 - **Windows:** `%NNM_DATA%\shared\nnm\conf\props\nms-jboss.properties`
 - **UNIX:** `$NNM_DATA/shared/nnm/conf/props/nms-jboss.properties`
- アプリケーション フェイルオーバー プロパティを変更するには、以下のファイルを編集します。
 - **Windows:** `%NNM_DATA%\shared\nnm\conf\props\nms-jboss.properties`
 - **UNIX:** `$NNM_DATA/shared/nnm/conf/props/nms-jboss.properties`
- **port.properties** ファイルにあったポート プロパティを変更するには、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`
- Node Group 設定フォームのチェックボックスを使用して、ノードグループのステータスを選択できるようになりました。**NNMi** 管理サーバー をアップグレード後は、**NNMi** ではアップグレード前の既存のノードグループが保持されます。

機能面の相違点

- コマンドとスクリプトの多くは、実行するためにユーザー名とパスワードが必要になりました。詳細については、実行するコマンドまたはスクリプトのリファレンス ページ、または **UNIX** のマンページを参照してください。
- **Oracle** データベースを使用中の場合、**NNMi** は `nmsdbmgr` プロセスを起動しません。
- ダンプニング設定は、規定では無効化されていません。
 - ダンプニング設定はほとんどの管理イベントに対して有効化されています。
- **nmsetdampeninterval** スクリプトを使用してダンプニング周期を調整することができます。このスクリプトですべてのインシデント設定のダンプニング周期が設定されます。詳細については、`nmsetdampenedinterval.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。
 - アップグレード後は、以下のような **NNMi Northbound** インタフェースを使用するすべての統合で、**nmsetdampeninterval** スクリプトは非常に役に立ちます。
 - **NNMi Northbound** インタフェース
 - **Netcool** ソフトウェア用 **NNMi** 統合モジュール
 - **HP NNMi-HPOM** 統合の **HPOM** エージェント実装
 - **NNMi 9.00** にアップグレードして異なるダンプニング期間 (6 分以外) を設定すると、**nmsetdampeninterval** スクリプトを使用して有効化 **OOB** であるすべてのダンプニング周期を別の値にグローバルにリセットできます。
 - これは手動手順で、アップグレード中は自動で行われません。
- ダンプニングするには、**NNMi 9.00** をインストールする前に、統合設定の **Holding Period** パラメータの値を書き留めます。アップグレード後、**nmsetdampeninterval** スクリプトを実行してこの値を **NNMi** に適用します。

- **NNMi 9.00** はアップグレード中、Network Infrastructure Devices ノードグループとその他のノードグループの Calculate Status 設定を無効化します。
 - ノードグループごとに、簡単に有効化することができます。
 - 大規模な環境の場合、リソースの点で大きなコストがかかる可能性があるため、各ノードグループの **[ステータスの計算]** 設定を十分に検討します。
 - ノードグループのステータスチェックの詳細については、NNMi ヘルプの「ノードグループのステータス詳細をチェック」を参照してください。
- **NNMi 9.00** へアップグレード後は、NNMi では管理アドレスの **ICMP (ping)** が使用されます。
- **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。
- デバイス プロファイル設定を **NNMi 8.x** からアップグレードすると、設定の一部が変更される場合があります。アップグレード中にこれらの値が変更されないようにするには、Author フィールドを HP Network Node Manager 以外の値に変更します。
- **URL** アクション設定を **NNMi 8.x** からアップグレードすると、設定の一部が変更される場合があります。アップグレード中にこれらの値が変更されないようにするには、Author フィールドを HP Network Node Manager 以外の値に変更します。

NNM 6.x/7.x からのアップグレード

この項では以下の章について説明します。

- 製品の比較
- NNM 6.x/7.x からのアップグレード
- NNM 6.x または NNM 7.x と NNMi との統合

製品の比較

この章では、HP Network Node Manager (NNM) 6.x/7.x と HP Network Node Manager i Software の間の重要な違いについて説明します。NNM の前バージョンを使用していた方は、この章を参照しながら NNMi の計画を立てたり設定してください。NNMi を初めてお使いになる方は、この章を読む必要はありません。

この章には、以下のトピックがあります。

- ネットワーク検出
- ステータス モニタリング
- イベント モニタリングのカスタマイズ

ネットワーク検出

検出は、データベースに追加されているネットワークの要素 (デバイス、ノード、およびこれらのコンポーネント) に対して行われます。NNMi では、「インベントリ検出」とは新規ノードを検索することであり、「レイヤ 2 検出」とは以前は **Extended Topology** 検出によって実行されていた接続性モデリングを指します。

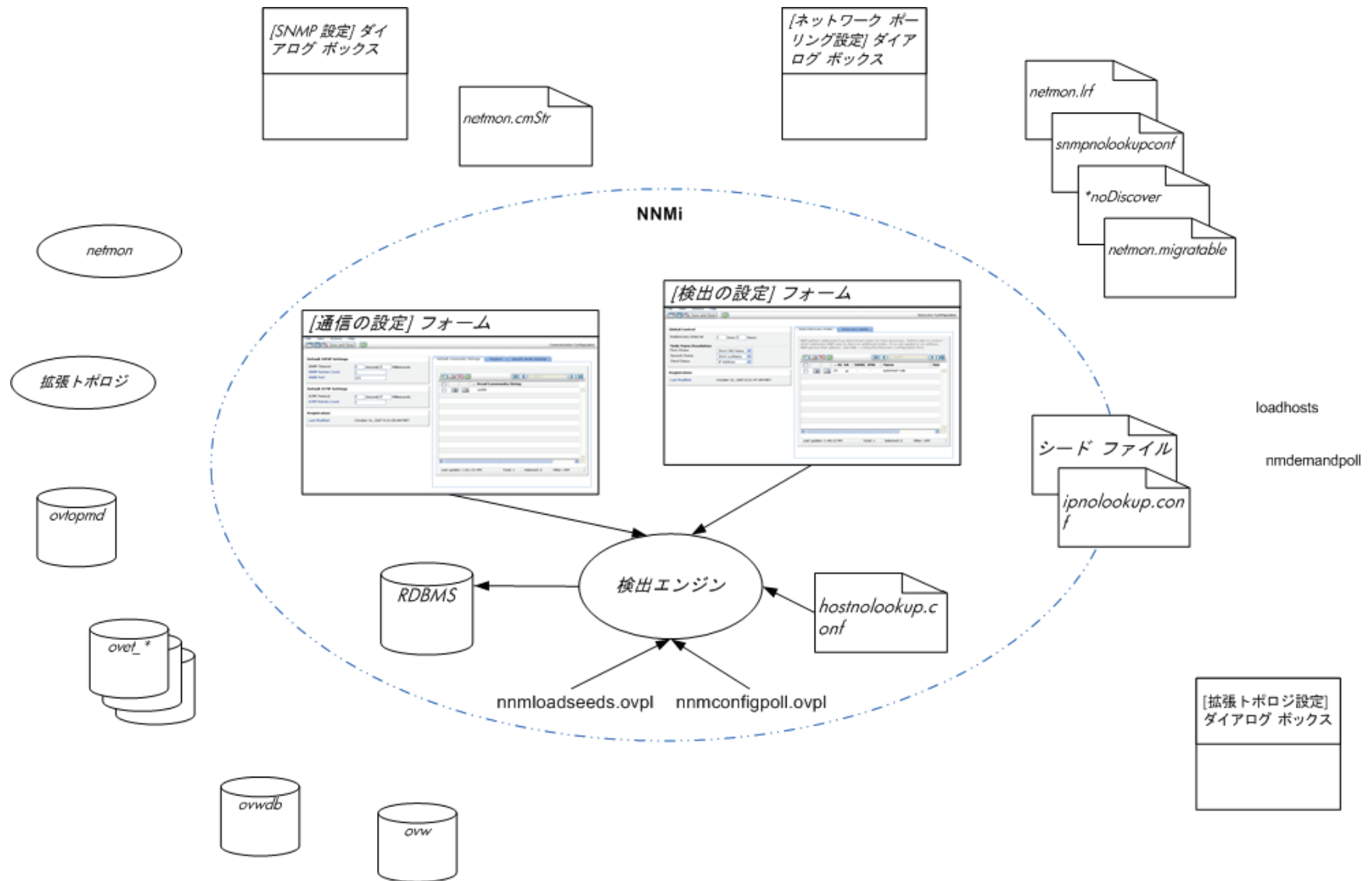
NNM 6.x/7.x のデフォルトでは、NNM は起動すると、自身のループバック アドレスをシードとして使用し、直接接続しているネットワークの自動検出を (自身の IP アドレスおよびサブネット マスクに基づいて) 開始していました。NNMi では、最初から管理者制御が可能です。NNMi 自動検出では、検出を行う前に、検出領域を IP アドレス範囲に基づいて定義し、少なくとも 1 つのシードデバイス (通常はルーター) を指定します。

図 17 の中央に、NNMi での検出を設定するために使用するツール、ファイルおよびコマンドを示しています。周囲には、NNM 6.x/7.x の類似品目を示しています。



Extended Topology 情報は、Extended Topology アドオンを備えた NNM 6.x または NNM 7.x Advanced Edition のみに適用されます。

図 17 検出の設定要素



検出の重要概念

ここでは、NNM 6.x/7.x から NNMi への変更の主な領域を簡単に説明します。NNMi 検出の詳細については、NNMi ヘルプの「ネットワークの検出」を参照してください。

- NNMi は、すべての情報を 1 つのリレーショナル データベース内に保管します。
 - NNMi は、設定が容易な 1 つの統合検出エンジンを使用します。
 - NNMi のスパイラル検出プロセスにより、ネットワークに変化が生じた際のトポロジ情報の継続的な更新が可能になります。トポロジの変化(インベントリとレイヤ 2 の両方)を、定期的な再検出間隔より頻繁に検出できます。
 - NNMi では、すべての検出対象ノードは、管理モード(管理対象、管理除外、またはサービス停止)にかかわらず、ライセンス限度に対してカウントされます。ライセンス限度を超えるノードは検出できません。
 - 自動検出は、NNMi と NNM 6.x/7.x では同じ意味を持っていますが、設定アプローチは異なります。
 - NNMi では、自動検出境界を定義し、少なくとも 1 つの IP アドレス シードを指定してから、検出を実行させます。
 - NNMi 自動検出では、管理が容易な拡大式モデルを使用します。NNMi 自動検出では、指定された境界内のすべてのルーター、スイッチおよびサブネットを見つけ出して管理します。NNMi で検出して管理する追加デバイス タイプを指定します。
- ▶ デフォルトでは、SNMP 以外のノードは NNMi で検出されません。
- シード検出は、NNMi と NNM 6.x/7.x では同じ意味を持っていますが、設定アプローチは異なります。
 - NNMi では、検出シードをユーザー インタフェースで指定します。
 - NNM 6.x/7.x シード ファイルを NNMi で、変更することなく使用できます。
 - NNMi `nmloadseeds.ovpl` コマンドは、NNM 6.x/7.x `loadhosts` コマンドに代わるコマンドです。
 - NNMi 設定ポーリング(`nmconfigpoll.ovpl`)は、デバイス設定情報を決定するための NNM 6.x/7.x 需要ポーリング(`nmdemandpoll`)に代わるものです。

ステータス モニタリング

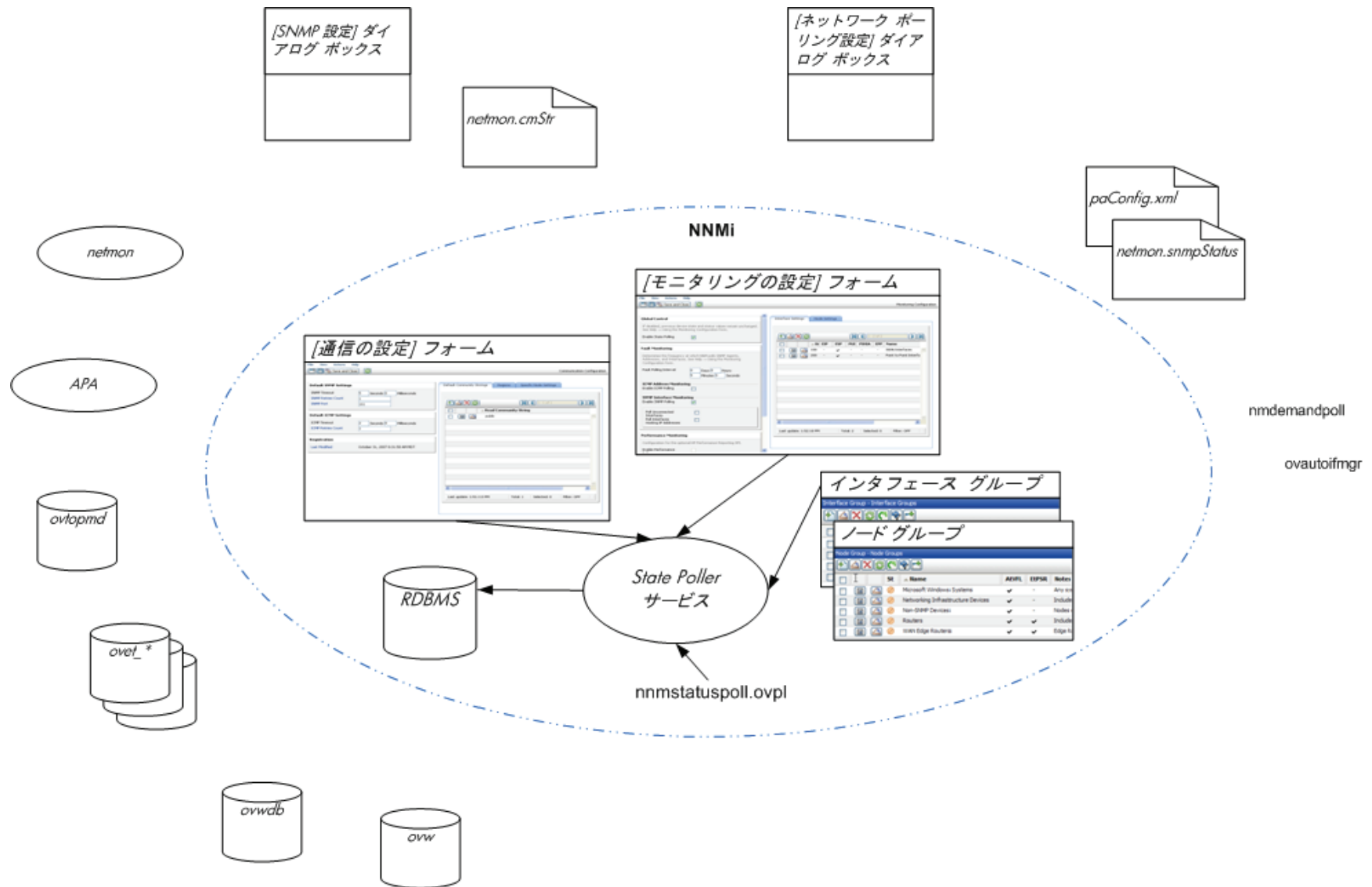
ステータス モニタリングを行うことにより、故障が起こり得るデバイスやコンポーネントの点から見て最新のネットワーク可視化が実現します。ある部品がポーリングに失敗すると、**NNMi** は原因を調査して、根本原因アラームをインシデント ブラウザに送出します。

図 18 の中央に、**NNMi** でのステータス モニタリングを設定するために使用するツール、ファイルおよびコマンドを示しています。周囲には、**NNM 6.x/7.x** の類似品目を示しています。



APA 情報は、**NNM 7.x Advanced Edition** のみに適用されます。

図 18 モニタリングの設定要素



ステータス モニタリングの重要概念

ここでは、NNM 6.x/7.x から NNMi への変更の主な領域を簡単に説明します。NNMi ステータス 監視の詳細については、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。

- 設定は、これでユーザー インタフェースを通じて完了しています。
- NNMi ノード グループおよびインタフェース グループは、トポロジ フィルタに代わるものです。
 - グループは、定義済みの属性のセットでのみフィルタリングできます。
 - グループをブール演算子と連結できません。
 - ノード グループは、sysObjectId ワイルドカードを使用する代わりにデバイス フィルタを使用します。
 - インタフェース グループを、収容側ノードおよびインタフェース タイプのグループに基づいて制限できます。
- ICMP ポーリングは、デフォルトでは無効です。
- 広範な制御機能により、不要なインタフェースの除外が容易です。
- モニタリング設定は、(1) インタフェース設定、(2) ノードの設定、(3) デフォルトのように、固有性の高いものから一般性の高いものへの方向に適合しています。
- モニタリングの動作をシステム全体で変更するには、すべての設定をすべてのレベルで変更します。
- NNMi のステータス ポーリング ([アクション]>[ステータス ポーリング]または nnmstatuspoll.ovpl) は、デバイスのステータスを判定するための NNM 6.x/7.x の需要ポーリング (nmdemandpoll) に代わるものです。
- デフォルトでは、NNMi がポーリングするインタフェースは、レイヤ 2 接続を通じて別の既知のインタフェースに接続しているインタフェースのみです。接続していないインタフェースのポーリングと IP アドレスをホストしているインタフェースのポーリングを有効にできます。

イベント モニタリングのカスタマイズ

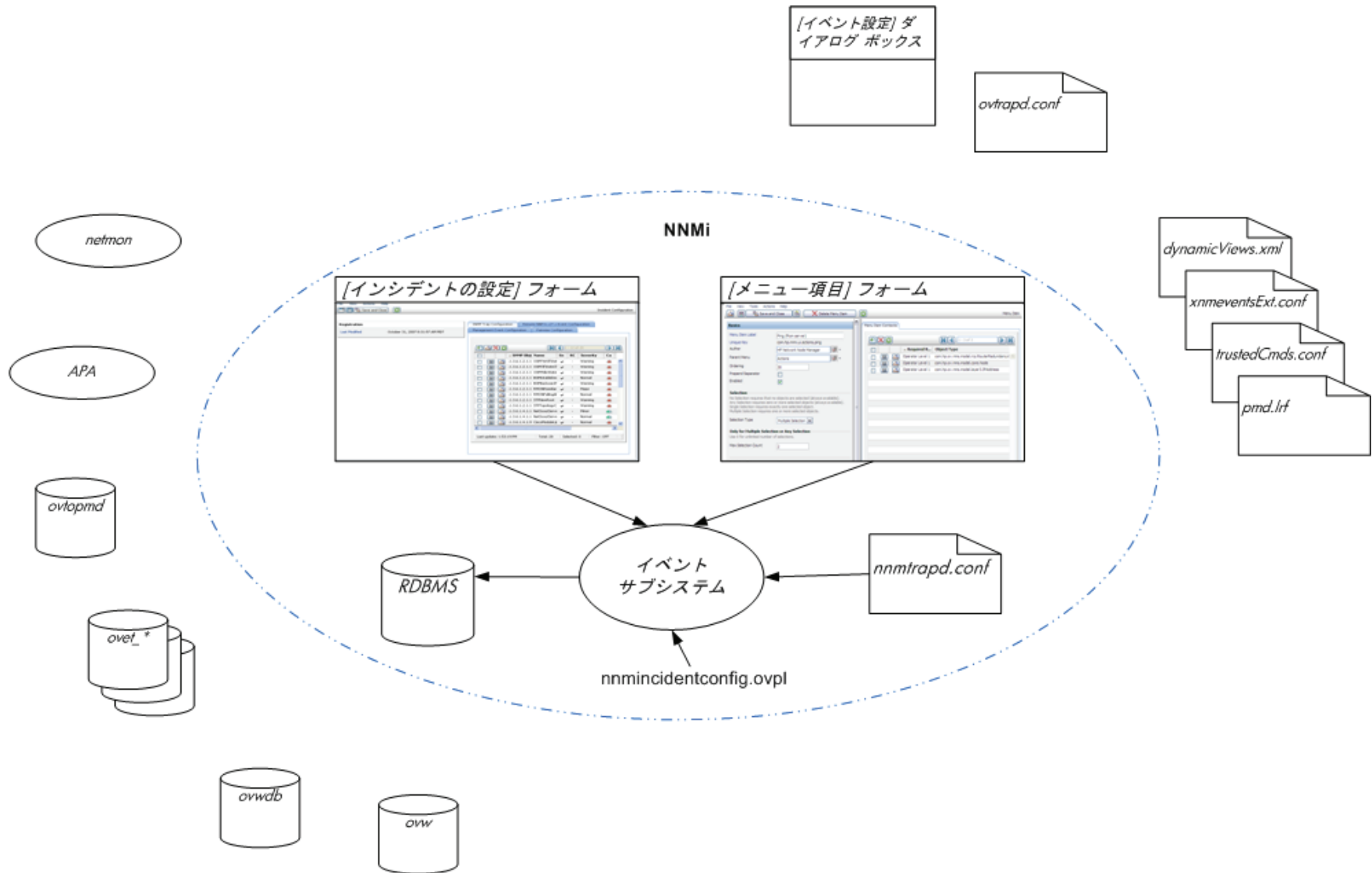
NNMi にはインシデント ビューという 1 つの中心となる場所があり、そこで管理イベント、SNMP トラップ、および NNM 6.x/7.x 転送 イベントをチームが見ることができます。どの SNMP トラップや NNM 6.x/7.x イベントがインシデントとして表示するほど重要であると見なすかをコントロールしてください。

図 19 の中央に、NNMi でのイベント モニタリングを設定するために使用するツール、ファイルおよびコマンドを示しています。周囲には、NNM 6.x/7.x の類似品目を示しています。



APA 情報は、NNMi 7.x Advanced Edition のみに適用されます。

図 19 イベント モニタリングの設定要素



イベント モニタリングの重要概念

ここでは、NNM 6.x/7.x から NNMi への変更の主な領域を簡単に説明します。NNMi インシデントの詳細については、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。

- NNMi では、イベント サブシステムがプロセス間通信で使用されておらず、イベントのボリュームが大きく削減されています。管理者は、各々の IPC メッセージを表示するかログするかを設定する必要がなくなりました。
- NNMi は、受信するよう設定したトラップのみを受信します。設定されていないトラップは、フィルタリングされてイベント パイプラインから除かれます。
- NNMi は、受信するすべてのトラップを表示します。
- NNMi イベント サブシステム プロセスのトラップ フィルタは、[インシデントの設定] フォームでの選択内容に基づいて、明示的に設定されます。
- NNMi nmmincidentconfig.ovpl コマンドは、指定された MIB ファイルのトラップ定義のみをロードします。
- NNMi は、イベント パイプラインで生じるペアワイズ、レート、および重複排除の相関を提供します。(NNMi には、イベント関連システム (ECS) は含まれません。)
- NNMi では、インシデントのライフサイクルの任意の時点で生じるアクションを設定できます。あらゆるスクリプト、実行ファイル、または Jython アクションをアクションとすることができます。
- NNMi URL アクション設定は、イベントの結果として行われるアクションを定義するための dynamicViews.xml および xnmeventsExt.conf 設定ファイルに代わるものです。

NNM 6.x/7.x からのアップグレード



この章では、HP Network Node Manager 6.x または 7.x から、最新バージョンの HP Network Node Manager i Software へのアップグレードの基本的な手順について説明します。バージョンは、このドキュメントのフッタに示されています。この基本的な手順は、ほとんどのユーザーのニーズに応えるものです。この章では、高度なアップグレードのトピックやカスタマイズについては扱いません。これらについては、お客様のニーズを満たすコンサルティング サービスをご利用いただけます。

この章では、次の製品命名規約を使用します。

- **NNM** は、HP Network Node Manager の旧バージョンです (NNM の 6.x と 7.x の全リリースを含みます)。
- **NNMi** は HP Network Node Manager i Software です (NNMi と NNMi Advanced の 8.x の全リリースを含みます)。

この章では、以下のことを想定しています。

- 『NNMi インストール ガイド』の「」の指示に従って NNMi をインストールしてあります。
- NNMi 機能の全般的な理解については、NNMi ヘルプとこのガイドの導入情報で説明されている概念を確認済みです。
- NNMi コンソールの使用法を理解しています。

アップグレード処理の助けとなるツールのリリースや、NNMi の進化に伴って、この章の情報はしばしば更新されます。

NNM および NNMi の最新ドキュメントは、以下のサイトからダウンロードできます。

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

この章には、以下のトピックがあります。

- アップグレード オプション
- フェーズ 1: NNM 管理ステーションからのデータ収集
- フェーズ 2: SNMP 情報のアップグレード
- フェーズ 3: 検出のアップグレード
- フェーズ 4: ステータス モニタリングのアップグレード
- フェーズ 5: イベント設定とイベント削減のアップグレード
- フェーズ 6: グラフィカルな視覚化のアップグレード (OVW)
- フェーズ 6: グラフィカルな視覚化のアップグレード (ホーム ベース)

- フェーズ 7: カスタム スクリプトのアップグレード
- アップグレード ツール リファレンス

アップグレード オプション

新たな始まり

数世代のソフトウェア環境、さまざまなネットワーク環境が備わっている NNM システムは多数あります。経路が決まっている世界で NNM 4.x または 5.x から開始したユーザーは、現在のネットワーク構造には実際には適合しない不必要なお荷物を進展させていることがあります。NNM システムが 2 年以上前のものである場合は、この機会を利用して新しいシステムを開始することを本気で考えてください。現在のネットワークの管理法をすみずみまで再評価すると、使用中の NNM と比較して、オーバーヘッドが大幅に減少し、操作が簡単になる可能性があります。

NNMi の新規にインストールから始める場合は、『NNMi インストール ガイド』の指示に従って NNMi をインストールしてください。次に、この『NNMi 導入リファレンス』の他の章に示したやや複雑な導入作業について検討してください。この章を読む必要はありません。

フェーズ別アップグレード

組織によっては、新規にインストールするよりも、アップグレードをフェーズに分けて行う方法が、スムーズに機能します。このような組織では、新しい NNMi システムで、既存の NNM システムを完全に再生し、置き換える必要があります。この目的に進む道は多数ありますが、HP は次のフェーズをお勧めします。

- **フェーズ 1: NNM 管理ステーションからのデータ収集**
NNMi が提供するツールを使用して、NNM 管理ステーションからのアップグレードに必要な情報を収集します。
- **フェーズ 2: SNMP 情報のアップグレード**
使用中の環境の SNMP アクセス情報で NNMi を設定します。
- **フェーズ 3: 検出のアップグレード**
NNM がオブジェクトを (自動) 検出したのと類似した方法で、NNM が検出したオブジェクトを NNMi が検出するように設定します。
- **フェーズ 4: ステータス モニタリングのアップグレード**
使用中の環境に最も適切なステータス ポーリング間隔とプロトコルを設定します。
- **フェーズ 5: イベント設定とイベント削減のアップグレード**
イベントの重要度、カテゴリ、メッセージを表示し、NNM で設定した自動処理を実行するように NNMi を設定します。重複解除、レート計算、ペアワイズのキャンセル、しきい値監視を設定する必要があることもあります。

- フェーズ 6: グラフィカルな視覚化のアップグレード

以下の方法のいずれか 1 つを選択してください。

- フェーズ 6: グラフィカルな視覚化のアップグレード (OVW)

NNMi に、NNM OVW ロケーション サブマップに似たノード グループ マップを設定します。

- フェーズ 6: グラフィカルな視覚化のアップグレード (ホーム ベース)

NNMi に、NNM 7.x Advanced Edition ホーム ベース コンテナ ビューに似たノード グループ マップを設定します。

- フェーズ 7: カスタム スクリプトのアップグレード

NNM コマンドライン ツールを使用するスクリプトを更新して、NNMi コマンドライン ツールを呼び出します。



NNMi は、既存 NNM システムの管理者のマネージャとして機能できます。イベントを NNMi に転送するように NNM を設定できます。次に、統合ユーザー インタフェース、インシデント所有権、ライフサイクル状態がある NNMi コンソールを使用して、おなじみの NNM ツールに移動できます。NNM を NNMi に統合する場合の指示は、353 ページの「[NNM 6.x または NNM 7.x と NNMi との統合](#)」を参照してください。

表 15 に最も簡単なアップグレードと最も複雑なアップグレードのプロセスの概要を示します。

- 最も簡単な方法としては、NNM から環境に特有の情報をインポートし、改良したデフォルトの NNMi 設定値を NNM から受け入れます。
- 最も詳細で綿密な方法としては、NNM 設定を詳しく調べ、この設定を NNMi で複製します。

この章の残りの部分では、NNM 設定を NNMi に複製するプロセスをたどって行きます。左端のテキストは、特定の手順がアップグレードプロセスにどのように当てはまるかを示しています。

- **NNM から収集**したものは、NNM 管理ステーションで行う作業を示します。
- **NNMi への複製**は、NNMi 管理サーバーで行う作業を示します。
- **NNMi での強化**は、NNMi 管理サーバーで行うオプションの作業を示します。強化は、アップグレードプロセスの間に行うか、その後の任意のタイミングで実行できます。

適切な時点で、指定の作業完了の複雑さの範囲に応じて 1 つまたは複数のオプションが与えられます。

表 15 アップグレードの範囲

フェーズ	最も簡単な方法	最も詳細で綿密な方法
NNM からのデータ収集	<ol style="list-style-type: none"> 1 NNMi が提供するツールを NNM 管理サーバーで使用します。 2 収集したデータを NNMi 管理サーバーにコピーします。 	<ol style="list-style-type: none"> 1 各アップグレード フェーズで、該当する NNM 設定データを手作業で収集します。 2 収集したデータを NNMi 管理サーバーにコピーします。
SNMP 情報	<p>収集したコミュニティ文字列を NNMi にインポートし、どのコミュニティ文字列がどのノードにあてはまるか NNMi が選別するようにします。</p>	<ol style="list-style-type: none"> 1 現在使用中のコミュニティ文字列をすべてエクスポートします。 2 データ ファイルを変更し、内容を特定ノードのコミュニティ文字列として NNMi にインポートします。
検出	<p>検出したノードリストを収集して変更し、ファイルの内容を自動検出ルールのないシードとして NNMi にインポートします。</p>	<ol style="list-style-type: none"> 1 NNM と netmon がノードを検出する方法を決定します (シード、ロードホスト、フィルタ、その他のツール)。 2 シードおよび自動検出ルールを使用して、可能な限り厳密にこの方法を複製します。
ステータス モニタリング	<p>NNMi デフォルトは、ほとんどのユーザー要件に合うように更新されます。デフォルト値を大幅に変更する必要がない可能性があるため、更新したデフォルト値で操作を開始します。</p>	<ol style="list-style-type: none"> 1 ノードの各グループについて、どのポーリング間隔とポーリング方針を NNM および netmon または APA が使用したか正確に調べます。 2 NNMi ノード グループとインタフェースグループを実装し、ポーリング間隔とポーリング方針を複製します。
イベント設定とイベント削減	<ol style="list-style-type: none"> 1 NNM のデフォルト設定で開始します。 2 管理対象デバイスのカスタム トラップの定義を追加します。 3 必要に応じて、自動処理を追加します。 	<ol style="list-style-type: none"> 1 トラップとイベントの種類ごとに、何の NNM カスタマイズが行われたかを正確に調べます。 2 NNMi システム上で、一致するそれぞれのトラップとイベントの種類をカスタマイズします。
グラフィカルな視覚化	<ol style="list-style-type: none"> 1 NNM ovw コンテナをインポートします。 2 ノード グループをコンテナに割り当てます。 <p>OR</p> <ol style="list-style-type: none"> 1 NNM 7.x Advanced Edition コンテナビューをインポートします。 2 ノード グループをコンテナに割り当てます。 	<ol style="list-style-type: none"> 1 最も包括的な NNM マップで、各サブマップに何があるか判定します。 2 各 NNM サブマップの内容に応じて、ノードグループを作成します。 3 各ノードグループについて、NNMi マップを作成し、背景イメージを追加し、各ノードを配置します。
カスタム スクリプト	<p>nnmtopodump.ovp1 コマンドを使用するように既存のスクリプトを修正します。</p>	<p>新しいスクリプトを作成して、NNMi の新しいツールを組み込みます。</p>

フェーズ 1: NNM 管理ステーションからのデータ収集

NNMi は、NNM 設定を NNMi に複製するために必要な主要なデータを収集する、NNM 管理ステーション上で実行するツールを提供します。このツールは、NNM データベースにある情報からテキスト ファイルを作成し、その他の設定情報をコピーします。また、このツールは NNMi 管理サーバーにコピーするため、既知のディレクトリ構造にデータを集めます。

データ収集ツールと、ツールで収集する情報については、348 ページの「データ収集ツール」を参照してください。

NNM から収集 アップグレード ツールによる方法

- 1 NNM システムの完全なバックアップを実行します。
- 2 データ収集ツールのアーカイブを NNMi 管理サーバーから NNM 管理ステーションにコピーします。ファイルの名前と場所は、各コンピュータのオペレーティング システムによって異なります。
 - NNMi 管理サーバーでは、アーカイブは以下のディレクトリにあります。
 - *Windows*: %NnmInstallDir%\migration¥
 - *UNIX*: \$NnmInstallDir/migration/
 - NNM 管理ステーションで、アーカイブを以下の場所に置きます。
 - *Windows*: migration.zip ファイルを NNM インストール フォルダ (*install_dir*、通常は C:\Program Files\HP OpenView) にコピーします。
 - *UNIX*: migration.tar ファイルを /opt/OV/ ディレクトリにコピーします。
- 3 NNM 管理ステーションのオペレーティング システムに適したツールまたはコマンドを使用して、データ収集ツールのアーカイブを解凍します。
- 4 NNM インストール ディレクトリから、ツールを実行します。
 - a migration ディレクトリに移動します。
 - b 収集するデータに対し、期待されるディレクトリ構造を作成します。

```
createMigrationDirs.ovpl
```
 - c NNM データを収集します。

```
nnmmigration.ovpl
```
 - d OVW マップ ロケーション階層データをアップグレード アーカイブに含める場合は、344 ページの「フェーズ 6: グラフィカルな視覚化のアップグレード (OVW)」で説明したように、マップ データを収集するためにアップグレード ツールによる方法を実行します。



NNM 管理ステーションにホーム ベース コンテナ ビューが設定されている場合、この情報はアップグレード アーカイブに含まれます。ほかに必要な作業は必要ありません。

- e 収集したデータをアーカイブします。

archiveMigration.ovpl

このツールは、NNMi 管理サーバーへの単純なデータ転送を行うため、収集したデータから `<hostname>.tar` ファイルを作成します。ツールの実行中は、大量のメモリを消費します。NNM システムに十分なメモリやディスク容量がなくこのツールが機能しない場合は、自分自身でデータをより小さなサイズでアーカイブしたり、必要に応じて個々のファイルをコピーしたりできます。



Windows オペレーティング システムでは、archiveMigration.ovpl の実行に時間がかかる場合があります。データを NNMi システムに移す準備としてデータのアーカイブを行う場合、他のツールを使用することも検討してください。

手動による方法

アップグレード ツールによる方法がお使いの環境でうまくいかない場合、その時点の NNM データの収集については、各フェーズで挙げたステップに従ってください。

NNMi に複写

データ アーカイブを NNMi 管理サーバーにコピーします。

アップグレード ツールによる方法

archiveMigration.ovpl ツールが正常に完了したら、以下の手順を実行します。

- 1 NNMi 管理サーバーで、以下のディレクトリに移動します。
 - **Windows:** %NnmDataDir%\tmp¥
 - **UNIX:** \$NnmDataDir/tmp/
- 2 tmp ディレクトリに、migration ディレクトリと `<hostname>` ディレクトリを、以下の構成に作成します。
 - **Windows:** %NnmDataDir%\tmp¥migration¥<hostname>¥
 - **UNIX:** \$NnmDataDir/tmp/migration/<hostname>/
- 3 `<hostname>.tar` ファイルを NNM 管理ステーションから NNMi 管理サーバー上の以下の場所にコピーします。
 - **Windows:** %NnmDataDir%\tmp¥migration¥<hostname>¥<hostname>.tar
 - **UNIX:** \$NnmDataDir/tmp/migration/<hostname>/<hostname>.tar
- 4 NNMi 管理サーバーで、手順 2 で作成したディレクトリに移動します。
 - **Windows:** %NnmDataDir%\tmp¥migration¥<hostname>¥
 - **UNIX:** \$NnmDataDir/tmp/migration/<hostname>/
- 5 データ アーカイブを解凍します。
 - **Windows:**

```
%NnmInstallDir%\migration¥bin¥restoreMigration.ovpl ¥  
-source <hostname>.tar
```
 - **UNIX:**

```
$NnmInstallDir/migration/bin/restoreMigration.ovpl ¥  
-source <hostname>.tar
```

手動による方法

archiveMigration.ovpl コマンドが正常に完了しなかった場合、データ ファイルを手動でコピーします。

▶ テキスト ファイルを Windows から UNIX にコピーする過程で、ファイルに ^M 文字が挿入されることがあります。

- この問題を回避するには、FTP を ASCII モードで使用してファイルを転送します。
- テキスト ファイルから ^M 文字を削除するには、UNIX システムで dos2ux (または同様の) コマンドを実行します。

フェーズ 2: SNMP 情報のアップグレード

管理対象デバイスとの接続の確立に NNMi が使用する SNMP コミュニティ文字列情報を設定します。

NNM 設定に、名前解決サービスで調べるべきでない IP アドレスまたはホスト名がある場合は、その情報を NNMi に複製します。

使用中のネットワークのカスタム デバイス用に NNMi デバイス プロファイルをカスタマイズします。

SNMP アクセスの設定

NNMi 検出では、設定や接続性に関する特定の情報を収集するために、管理ノードへの SNMP アクセスが必要です。SNMP は、ノードおよびそれに含まれるオブジェクトの稼働状態にアクセスするために、ステータス モニタリングの間も使用されます。

▶ NNM は、一致する領域にリストされた順序でコミュニティ文字列を順に試し、機能する最初のコミュニティ文字列を使用します。NNMi は、設定されたすべてのコミュニティ文字列を並行して試し、機能する最初のコミュニティ文字列を使用します。役に立つ値が複数ある可能性のある最良のコミュニティ文字列を使います。

NNM から収集 アップグレード ツールによる方法

nnmmigration.ovpl ツールが、NNM 管理ステーションからコミュニティ文字列を収集して、snmpCapture.out ファイルにしてあります。

手動による方法

NNM 管理ステーションには、使用中の環境の機器に SNMP がアクセスするための完全な設定情報があります。

1 NNM SNMP 設定をエクスポートするには、以下の操作の 1 つを実行します。

- ユーザー インタフェースを開き、[オプション] > [SNMP 設定] を選択してから、[エクスポート] をクリックします。ターゲット ファイル snmpout.txt の名前を指定します。
- 次のコマンドを実行します。

```
xnmsnmpconf -export > snmpout.txt
```


出力は次の例のようなものになります。

```
10.2.126.75:public:*:::
mytest57.example.net:public:*:::
127.0.0.1:public:*:::
10.97.233.209:mycommstr:*:::
mpls2950.example.net:mycommstr:*:::
mplsce04.example.net:mycommstr:*:::
*.*.*.*:mycommstr:*:8:2:900:::
```

ターゲット ファイルには、コロンで区切られた以下のフィールドがあります。

```
target:community:proxy(* indicates do not proxy):timeout (tenths
of a second):retries:poll interval (seconds):port:set-community:
```

値の明確な解釈を知るには次のコマンドを使います(ただし、インポートでは使わないでください)。

```
xnmssnmpconf -export -verbose
```

ovsnmp.conf ファイル フォーマットの説明は、NNM 管理ステーションにある *ovsnmp.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。

- 2 次のファイルで、設定された代替りのコミュニティ文字列を確認します。

- **Windows:** %OV_CONF%\netmon.cmstr
- **UNIX:** \$OV_CONF/netmon.cmstr

NNMi に複写

アップグレード ツールによる方法

- 1 ディレクトリを次のように変更します。

- **Windows:** %NnmDataDir%\tmp\migration\<hostname>\SNMP\
- **UNIX:** \$NnmDataDir/tmp/migration/<hostname>/SNMP/

- 2 NNM コミュニティ文字列のテキスト ファイルを作成します。

- **Windows:**

```
%NnmInstallDir%\migration\bin\snmpCapture.ovpl %
snmpCapture.out > snmpout.txt
```
- **UNIX:**

```
$NnmInstallDir/migration/bin/snmpCapture.ovpl %
snmpCapture.out > snmpout.txt
```

- 3 コミュニティ文字列を NNMi にロードするにあたっては、手動での方法のいずれかに従ってください。

- 4 NNMi コンソールで、タイムアウト、再試行、ポートを設定します。

手動による方法

コミュニティ文字列を NNMi に入力する方法を選択します。これらの方法それぞれ、316 ページの **手順 2** (アップグレード ツールによる方法) または 315 ページの **手順 1** (手動による方法) で作成した snmpout.txt ファイルの一意のコミュニティ文字列値のリストを使用して処理を始めます。



設定領域 SNMP proxy system と Set community name は転送できません。

簡単な手動による方法

最も簡単な方法としては、NNM コミュニティ文字列をすべて入力し、各デバイスに使う SNMP コミュニティ文字列を NNMi に分かるようにします。コミュニティ文字列の検出は、デフォルトで有効になっています。この機能を使用すると、アップグレードを迅速に処理できます。

- 1 NOC (ネットワーク運営センター) に、NNMi の最初の検出の間は、認証エラーになることを通知します。NOC 職員は、その間、これらの認証エラーを差しさわりのなく無視できます。
- 2 以下の操作の 1 つを完了してください。

- NNMi で使用するフォーマットと一致するように snmpout.txt ファイルを変更します。次に、NNMi を使ってこれらの値をロードします。
 - snmpout.txt ファイルをサンプルとして使用し、NNMi の入力ファイルを手作業で構築します。次に、NNMi を使ってこれらの値をロードします。
 - 以下の手順で、値を NNMi コンソールに入力します。
- a snmpout.txt ファイルの一意のコミュニティ文字列値のリストを確認します。



アップグレード ツールによる方法を使用して snmpCapture.out ファイルから snmpout.txt ファイルを作成した場合、snmpout.txt ファイル内のコミュニティ文字列は一意です。このステップを実行する必要はありません。

- **Windows:** snmpout.txt ファイルを Microsoft Office Excel で開きます。データ行を選択してから、コラム B でソートします。

この例の場合は、次の 2 つの一意のコミュニティ文字列について考えます。

```
public  
mycommstr
```

- **UNIX:** 以下のコマンドを実行します。

```
cut -f 2 -d ':' < snmpout.txt | sort -u
```

- b NNMi コンソールで、[設定] ワークスペースから [通信の設定] を選択します。[デフォルトのコミュニティ文字列] タブに一意の値を入力します。
- c タイムアウト、再試行、およびポートを設定します。

The screenshot shows the NNMi configuration interface. The left pane displays the 'SNMP のデフォルト設定' (Default SNMP Settings) and 'ICMP のデフォルト設定' (Default ICMP Settings). The right pane shows the 'デフォルトの SNMPv1/v2 コミュニティ文字列' (Default SNMPv1/v2 Community Strings) tab, which contains a table of community strings. The table has columns for '読み取りコミュニティ文字列' (Read Community String) and '書き込みコミュニティ文字列' (Write Community String). The table contains two entries: 'ntcgwzloop' and 'ntcpubli'. The '更新済み' (Last Updated) column shows '10/06/04' and the '合計' (Total) is '2'. The '選択済み' (Selected) column is '0'. The 'フィルター' (Filter) is 'オフ' (Off) and '自動更新' (Auto Update) is 'オフ' (Off).

簡単な手動による方法の変更

コミュニティ文字列が使用された IP 領域ごとのグループ コミュニティ文字列。局地的な値を NNMi コンソールにロードしてから、各デバイスに使用する SNMP コミュニティ文字列を NNMi が決定するようにします。簡単な方法よりも認証の失敗は少なくなります。

- 1 snmpout.txt ファイルで、NNM が使っている IP 領域ごとの一意の値のリストを調べます。
- 2 NNMi コンソールで、[設定] ワークスペースから [通信の設定] を選択します。IP 領域を作成してから、領域ごとにコミュニティ文字列を入力します。
- 3 タイムアウト、再試行、およびポートを設定します。

手動による方法の自動化

snmpout.txt ファイルを nnmcommload.ovpl コマンドに必要なフォーマットに変換してから、各デバイスで使用中の個別のコミュニティ文字列をロードします。

- 1 NNMi ツールで使えるよう snmpout.txt ファイルを適合させるには、以下の方法の 1 つを実行します。

- エディタを使って NNMi に適切なファイルを作成します。結果は次のようなものになります。

```
10.2.126.75,public
mytest57.example.net,public
127.0.0.1,public
10.97.233.209,mycommstr
mpls2950.example.net,mycommstr
mplsce04.example.net,mycommstr
```

- UNIX のみ: 以下のコマンドを実行します。

```
awk 'BEGIN {FS = ":" };{printf"%s,%s\n",$1,$2 }' ¥
<snmpout.txt> mysnmp.txt
```

このコマンドはファイル内の個別のノードについて機能します。範囲またはワイルドカードを手作業でトリムします。

- 2 以下のコマンドを実行します。

```
nnmcommload.ovpl -u username -p password -file mysnmp.txt
```

- 3 NNMi コンソールで、デフォルトのコミュニティ文字列、および IP 範囲用のコミュニティ文字列を設定します。
- 4 NNMi コンソールで、タイムアウト、再試行、ポートを設定します。

NNMi コンソール 方法

NNMi コンソールで、[設定] ワークスペースから [通信の設定] を選択します。snmpout.txt ファイルの設定された値を複製します。

NNMi での強化

次の情報を使って、NNMi の通信アクセス設定を強化します。

- ホスト名ワイルドカード (IP 範囲より環境によく適合する場合)
- グローバル デフォルト、IP 範囲、および特定のノードによる ICMP タイムアウトと再試行
- ネットワークの特定のエリアへの SNMP または ICMP のアクセスを有効化または無効化
- 特定のノードについて優先される管理アドレス



NNM は、管理アドレスを選択するとき、最も小さいループバック アドレスを選択します。NNMi 8.1x でも、最も小さいループバック アドレスを選択します。NNMi 8.0x は最も大きいループバック アドレスを選択します。

名前解決の制限

DNS (または他の名前解決) サービスの制限が分かっている場合は、NNM と NNMi にこれらのデバイスのルックアップを避けるよう指示できます。この作業がシステムに該当しない場合は、320 ページの「デバイス プロファイルのカスタマイズ」に進んでください。



ファイル名での大文字小文字の使用は、NNM と NNMi とでは異なります。NNM では、ファイル名に ipNoLookup.conf を使用しますが、NNMi では、ファイル名に ipnolookup.conf を使用します。NNMi では、このファイル名については、すべて小文字のもの以外は正しく解釈できません。

NNM から収集

アップグレード ツールによる方法

nnmmigration.ovpl ツールが、DNS 参照を行わずに使用する IP アドレスとホスト名に関する情報を NNM 管理ステーションから収集し、NNMi の設定用に、ipnolookup.conf ファイルと hostnolookup.conf ファイルのどちらかまたは両方を作成しています。

手動による方法

- 1 次のファイルを確認し、NNM がアドレスからのホスト名解決を除外するアドレスを調べます。
 - **Windows:** %OV_CONF%\ipNoLookup.conf
 - **UNIX:** \$OV_CONF/ipNoLookup.conf



ipNoLookup.conf ファイルが NNM 管理ステーションにない場合、複製する設定はありません。

- 2 次のコマンドを確認し、NNM が名前からのアドレス解決を除外するホスト名を調べます。

```
snmpnolookupconf -dumpCache > snmpnolookup.out
```



snmpnolookup.out ファイルが空の場合、複製する設定はありません。

NNMi に複写 アップグレード ツールによる方法

- 1 可能であれば、nmmigration.ovpl ツールが作成したファイル ipnolookup.conf と hostnolookup.conf を編集して、NNMi 管理サーバーへの参照を削除します。
 - **Windows:**
 - %NnmDataDir%\%tmp%\migration\<hostname%\CONFIG\ipnolookup.conf
 - %NnmDataDir%\%tmp%\migration\<hostname%\DNS\hostnolookup.conf
 - **UNIX:**
 - \$NnmDataDir/tmp/migration/<hostname>/CONFIG/ipnolookup.conf
 - \$NnmDataDir/tmp/migration/<hostname>/DNS/hostnolookup.conf
- 2 編集した設定ファイルを、以下のディレクトリに置きます。
 - **Windows:** %NnmDataDir%\%conf%
 - **UNIX:** \$NnmDataDir/shared/nnm/conf/

手動による方法

- 1 NNM ipNoLookup.conf から得たアドレスを以下のファイルに追加します。
 - **Windows:** %NnmDataDir%\%conf%\ipnolookup.conf
 - **UNIX:** \$NnmDataDir/shared/nnm/conf/ipnolookup.conf



NNMi 管理サーバーの IP アドレスは追加しないでください。

- 2 NNM が (318 ページ の手順 2 で作成した snmpnolookup.out ファイルから) 除外したホスト名を以下のファイルに追加します。
 - **Windows:** %NnmDataDir%\%conf%\hostnolookup.conf
 - **UNIX:** \$NnmDataDir/shared/nnm/conf/hostnolookup.conf



NNMi 管理サーバーのホスト名は追加しないでください。

これらの設定ファイルのフォーマットの詳細については、*ipnolookup.conf* および *hostnolookup.conf* 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 での強化

NNMi は検出の間のみルックアップを実行します。NNM 非ルックアップ設定を NNMi に複製すると、スパイラル検出操作が自動的に強化されます。

NNMi では、表示された名前ラベルとして、DNS ホスト名、IP アドレス、または MIB II sysName の使用を選択できます。これを行うには、以下の手順に従います。

- 1 NNMi コンソールで、[設定] ワークスペースから [検出の設定] を選択します。
- 2 [ノード名解決] エリアでノード名優先を設定します。

デバイス プロファイルのカスタマイズ

NNM が SNMP クエリーからデバイスに直接に収集する設定情報もあります。デバイスのシステム オブジェクト ID (sysObjectID) から導出される情報もあります。NNMi は、sysObjectID に基づくその デバイス プロファイルに従って属性をデバイスにマッピングします。デバイス プロファイルは、監視、ビューのフィルタリング、検出メンテナンス用ノードの分類用にノードをグループ化します。

以下の設定エリアは転送できません。

- カスタム記号
- カスタム データベース フィールドとデフォルト値

NNM から収集

1 NNM のお使いのバージョン用に **OID** ファイルのカスタマイズを決定します。

- **NNM 6.4** 以前は、ファイル `oid_to_sym`、`oid_to_type`、および `HPoid2type` を使用して、システムの `sysObjectID` をデータベース属性にマップし、シンボルを表示していました。
- **NNM 7.x** では、`oid_to_sym` ファイルを `oid_to_sym_reg` ディレクトリ構造に置き換えます。



`nnmmigration.ovpl` ツールは、これらのファイルを `migration` ファイル構造内の `CONFIG` フォルダにコピーします。

NNMi に複写

NNMi には既知のシステム オブジェクト ID について事前設定された多数のデバイス プロファイルが梱包されているので、必要なデバイス プロファイルをすぐに利用できる可能性があります。最も簡単な方法では、検出プロセスを開始し、結果を確認し、必要な場合のみ変更を行います。

ベストプラクティス

HP では、作成または変更する各デバイス プロファイルで作成者を一意に指定し、後で識別できるようにしておくことをお勧めします。

2 NNMi コンソールで、**[設定]** ワークスペースから **[デバイスのプロファイル]** を選択します。カスタマイズした値ごとに `sysObjectID` でエントリを見つけます。

3 必要に応じてデバイス プロファイル設定を更新します。

- NNMi で利用できるエントリについては、設定された値が NNM 属性と一致することを確認します。
- NNMi 内のエントリについては、`sysObjectID` 用に新しいデバイス プロファイルを作成します。将来のリリース用に ID を追加するよう HP に通知する拡張リクエストを送信します。

ベストプラクティス

4 最初の検出の後、プロファイルごとにノード インベントリをソートして、**[No Device Profile]** ノードを見つけます。

[No Device Profile] プロファイル タイプは、`sysObjectID` が以前 NNMi に設定されていなかったことを示します。NNMi は、**[No Device Profile]** のノードにはデフォルト監視設定を使用します。これらのノードのフィルタリングはより困難です。

新しいデバイス プロファイルを構築すると、NNMi データベース内のすべての `sysObjectID` に対して設定済みのデバイス プロファイルが存在するようになります。

フェーズ 3: 検出のアップグレード

検出スケジュールと設定を指定します。NNMi スパイラル検出は、1 つ以上の検出シードを保存するとすぐに始まります。



ネットワーク環境向けの適切なコミュニティ文字列を使用するよう NNMi を設定してから検出を開始します。

最初の検出の後、NNM で手動で設定したデバイス間の接続を複製します。

検出のスケジュール

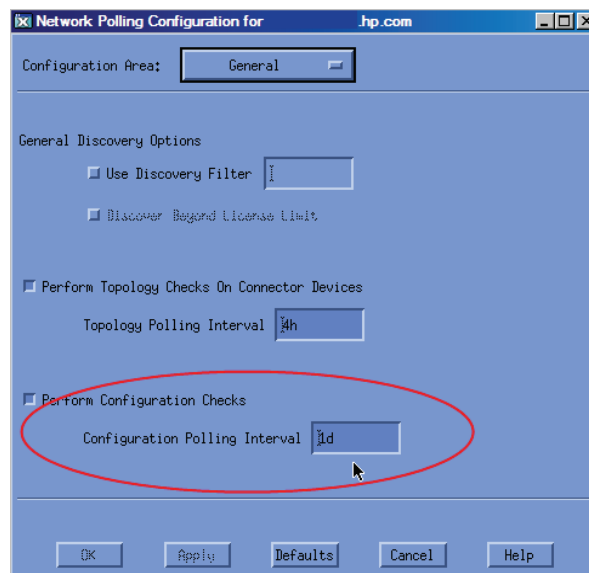
NNM 検出プロセスは独立に実行できます。検出を NNMi にアップグレードするには、NNM がノードを検出する間隔を転送するだけで十分です。

以下のスケジュール設定エリアは NNMi では使用されなくなっており、転送できません。

- トポロジはコネクタ デバイスをチェックします。NNMi が変更の可能性を示すトリガーを見つけるたびにトポロジチェックが自動的に行われるようになりました。
- 設定チェック。設定チェックは、スケジュールされた検出の時点、または NNMi でのトリガーの時点で行われるようになりました。
- レイヤ 2 (拡張トポロジ) 検出動作。NNMi は、デバイスが見つかるそれぞれについてレイヤ 2 検出を実行するため、この動作を別途スケジュールする必要はありません。
- 検出ポーリング間隔の自動調整。

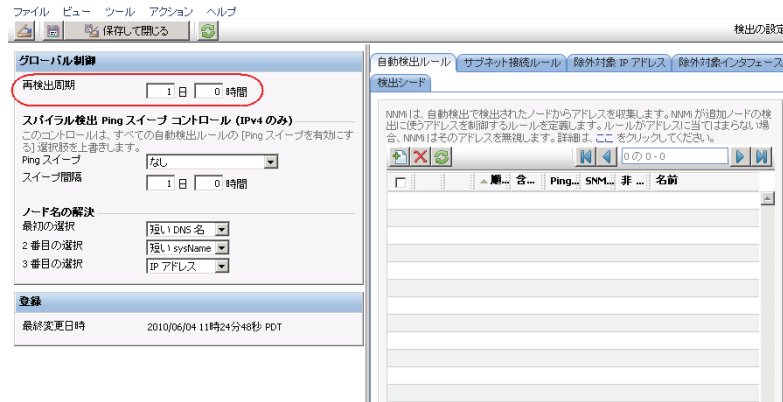
NNM から収集

- 1 NNM が再検出をいつ行うか決めます。
 - a ユーザー インタフェースで、[オプション]>[ネットワーク ポーリング設定] を選択します。
 - b [IP ポーリング] ページで、[検出ポーリング間隔] ボックスを確認します。
 - NNM が固定間隔を使う場合は、NNMi への転送の値に注意してください。
 - NNM が自動調整間隔を使う場合、NNM は最大 24 時間待機します。待機時間は 24 時間のままにしておくこともできますし、新しい値を選択することもできます。
 - 自動検出が有効になっていない場合は、[全般] ページの [設定チェックを実行] の間隔を調べ、NNMi への転送の値に注意してください。



NNMi に複写

- 2 NNMi コンソールで、[設定] ワークスペースから [検出の設定] を選択し、次に [再検出周期] を手順 1 で判定した値に設定します。



NNMi での強化

他の設定更新はすべて自動的に追加されていくので、NNM よりも設定が簡単で、検出が効率的です。

自分の検出方法の選択

NNMi 検出に、次のどのモデルを使うか決定します。

- シードされた検出、自動検出ルールなし。この種類の検出は管理者によって制約されます。管理者は、必要に応じてシードを追加し、検出されるものを制御します。次の操作のみを完了します。
 - 329 ページの「シード検出のためにシードを NNMi に追加します。」
- シードと自動検出ルールに基づいた自動検出。次の両方の操作を完了してください。
 - 324 ページの「自動検出ルールの設定」
 - 329 ページの「シード検出のためにシードを NNMi に追加します。」

NNMi での検出方法との違いの詳細については、NNMi ヘルプの「検出方法の決定」を参照してください。



NNM ライセンスは、管理下にあるノード数に基づいています (ステータス監視)。NNMi ライセンスは、検出されてトポロジに配置されたノード数に基づいています (監視対象および監視対象外ノード)。

この違いがあるので、検出ノード数を少なくしようとする人もいるでしょうが、モニタリングされないノードをデータベースに入れると利点もあります。例：

- サービス プロバイダのアクセス ルーターとそのルーターへの接続は、自分がデバイスの管理を担当していない場合でも、表示できます。
- ステータス モニタリング アルゴリズムはデータベースに表示される接続に基づいています。データベースでリンクの他端にデバイスがないインターフェースは、デフォルトでモニタリングされません。ステータス モニタリング設定でデフォルトを上書きすることもできますし、デバイス検出を選択することもできます。どれを選択するかは、各自の環境についてどこに関心を置くかのバランスで決まります。詳細については、70 ページの「モニタリングされないノードへのインターフェース」を参照してください。

自動検出ルールの設定

NNMi 検出設定は、NNMi の管理対象について考える優れた機会と言えます。NNM 検出設定とフィルタの変換を行う前に、現在のネットワーク環境を考察し、NNMi トポロジに組み込むものの記述について考えてください。

直接変換を行わない場合、NNMi 検出ルールには NNM の次の 2 つのタスク セットが含まれています。つまり、検出のスキープの拡大、およびスキープで検出されるオブジェクトの制限です。



NNMi 設定の場合、検出を拡大または制限する全ルールを定義してから、検出プロセスを開始するシードを入力することが重要です。

以下のスケジュール設定エリアは NNMi では使用されなくなっており、転送できません。

- Windows から IPX 検出
- ライセンスの制限を越える検出
- レイヤー 2 オブジェクトの検出を無効化 (NNMi については常に有効です)
- `netmon.interfaceNoDiscover`
- IP アドレスと `sysObjectID` (およびその派生物) 以外の属性のフィルタによる検出の除外
- `bridge.noDiscover` によるレイヤー 2 検出の制限
- CDP プロトコル エリア (統合ポート、vlan など) に基づいたレイヤー 2 検出の制限
- Extended Topology ゾーンの設定。NNMi のスパイラル検出には該当しなくなっています。

スパイラル検出の設定

NNMi には、NNMi でスパイラル検出を設定する次の 2 つの方法があります。つまり、ノードの手動でのロード (たとえば、ホスト ファイルから)、および自動検出ルールの使用。

ノードの手動でのロード

NNM から収集

- 1 NNM で、`loadhosts` コマンドの出力のあるファイルを見つけます。このファイルには、各ノードの IP アドレスとホスト名、さらに指定されている場合はサブネット マスクがリストされています。

NNM loadhosts の例

`loadhosts` コマンドのファイルの例は次のとおりです。

```
10.2.32.201 lnt04.example.net # comment
10.2.32.202 lnt07.example.net # comment
10.2.32.203 lnt03.example.net # comment
10.2.32.204 lnt02.example.net
10.2.32.205 lnt05.example.net
```

NNMi に複写

- 2 NNMi では、NNM `loadhosts` コマンドと同じ方法で検出シードを使用できます。これを行うには、`-f` オプションを指定して `nnmloadseeds.ovpl` コマンドを使用し、シード ファイルを指定します。

ベストプラクティス



シードを NNMi に設定する前に、すべてのコミュニティ文字列の設定を完了してください。

検出の出力を NNM loadhosts と同じにする場合は、NNMi で設定されている自動検出ルールを無効にします。自動検出ルールを無効にするには、以下の 1 つを実行します。

- **[検出の設定]** フォームからルールを削除します。
- **[自動検出ルール]** フォームで、**[含まれているノードの検出]** チェック ボックスをオフにします。

NNMi のシード ファイルのフォーマットでは、行ごとに IP アドレスまたはノード名 (オプションでコメント付き) があります。詳細については、*nnmloadseeds.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 シード ファイルの例

次の例に、NNM loadhosts コマンドおよびホストファイルと同じ機能の NNMi シード ファイルを示します。

```
10.2.32.201 # comment
10.2.32.202 # comment
lnt03.example.net # comment
lnt02.example.net
10.2.32.205
```

ベストプラクティス

次のファイルには、拡張トポロジのデバイス リストがあります。

- **Windows:** %OV_DB%\nnmet\hosts.nnm
- **UNIX:** \$OV_DB/nnmet/hosts.nnm

最初のフィールド (IP アドレス) または 2 番目のフィールド (ノード名) をコピーして NNMi のシードファイルを作成できます。

UNIX では、次のコマンドを実行してノード名のファイルを作成できます。

```
cut -f 2 hosts.nnm
```

ベストプラクティス

NNMi では、管理アドレスとしてループバック アドレスが必ず優先されます。ループバック アドレスを使わない場合、NNMi では、管理アドレスとしてシードアドレスがおそらく使われます (必ずではありません)。したがって、優先される IP アドレスのあるホストファイルをコピーするのが良いやり方です。ホスト名を使う場合は、DNS が解決されて優先される管理アドレスになることを確認します。しかし、NNMi が管理アドレスとしてこのアドレスを使うことが保証されるわけではありません。管理アドレス選択の詳細については、NNMi ヘルプの「**検出ノード名の選択**」を参照してください。

自動検出ルールの使用

NNM から収集

- 1 NNM に検出フィルタが使われたかどうかを調べます。NNM では、1 つの検出フィルタが検出の範囲全体に適用されます。
 - a NNM ユーザー インタフェースを開きます。
 - b **[オプション]** > **[ネットワーク ポーリング設定]** を選択します。
 - c **[全般]** ページで **[フィルタ使用]** チェック ボックスを確認し、オンの場合は使用中の検出ファイルに注意してください。フィルタを使用しない場合は、329 ページの「シード検出のためにシードを NNMi に追加します。」から続行します。
 - d 次のファイル内で検出フィルタを見つけます。
 - **Windows:** %OV_CONF%\C\filters
 - **UNIX:** \$OV_CONF/C/filters

- e 検出フィルタのロジックを慎重に確認します。

NNMi では、IP アドレスの範囲とシステム オブジェクト ID の範囲をフィルタでできます。変換できるオブジェクトもあります。たとえば、ホスト名ワイルドカードから IP 範囲への変換、またはベンダー名からシステム オブジェクト ID 範囲への変換です。

NNM 検出フィルタの例

次の例に、NNM フィルタを示します。たとえば、ルーター、ブリッジ、Nokia_Firewalls、NetBotz、NetsNSegs です。NetBotz ファイアウォールと Nokia ファイアウォールは sysObjectID で定義されます。

```
Nokia_Firewalls "Nokia Firewalls"
{ ( isNode && ( "SNMP sysObjectID" ~ .1.3.6.1.4.1.94.1.21.2.1.1 ) )
  ||
  ( isNode && ( "SNMP sysObjectID" ~ .1.3.6.1.4.1.94.1.21.2.1.9 ) )
  ||
  ( isNode && ( "SNMP sysObjectID" ~ .1.3.6.1.4.1.94.1.21.2.1.10 ) )
  ||
  ( isNode && ( "SNMP sysObjectID" ~ .1.3.6.1.4.1.94.1.21.2.1.11 ) )
  ||
  ( isNode && ( "SNMP sysObjectID" ~ .1.3.6.1.4.1.94.1.21.2.1.12 ) )
  ||
  ( isNode && ( "SNMP sysObjectID" ~ .1.3.6.1.4.1.94.1.21.2.1.138 ) )
}
```

```
NetBotz "NetBotz"
{ isNode && ( "SNMP sysObjectID" ~ .1.3.6.1.4.1.5528.* ) }
```

```
My_NetInfrastructure "My Network Infrastructure"
{ Routers || Bridges || Nokia_Firewalls || NetBotz || NetsNSegs }
```

NNMi で複写

- 2 NNMi コンソールに検出フィルタを入力します。

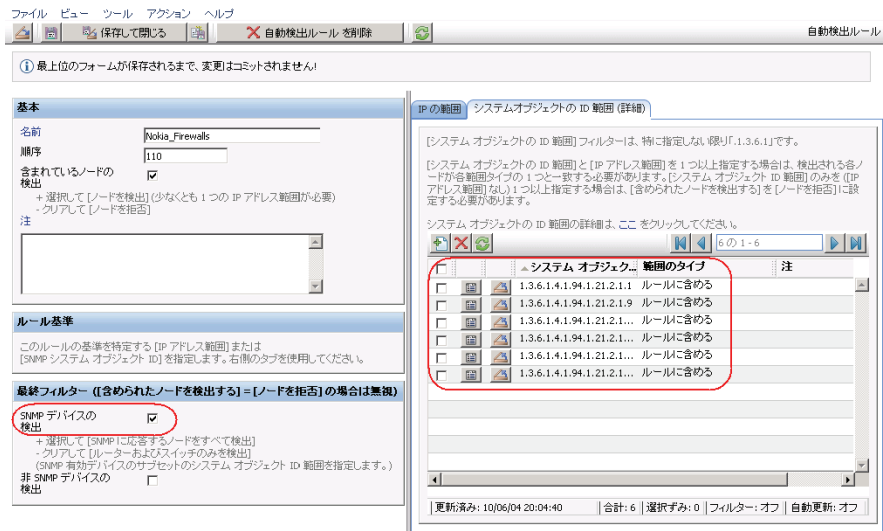
NNMi 検出フィルタエントリの例

たとえば、326 ページの「NNM 検出フィルタの例」に示す NNM フィルタを NNMi に転送するには、自動検出ルールを 3 つ (Nokia ファイアウォールに 1 つ、NetBotz デバイスに 1 つ、ルーターとスイッチに 1 つ) 定義します (NNM 7.x のブリッジと同じ)。NNMi では、NetsNSegs は不要です。この例の場合、検出されるネットワークの範囲は 10.*.* と仮定します。

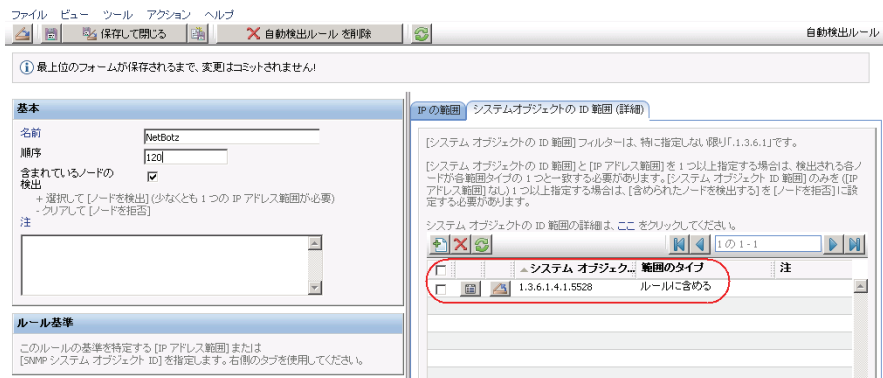
- a Nokia ファイアウォールの場合、ルール名 (Nokia_Firewalls) を入力してから、ネットワーク IP 範囲 10.*.* を入力します。

The screenshot shows the NNMi configuration interface. The 'Basic' tab is selected, and the 'Name' field is set to 'Nokia_Firewalls'. The 'Order' field is set to '110'. The 'Node selection' section is expanded, showing a list of nodes. The 'IP Range' tab is also visible, showing the IP range '10.*.*' and the rule type 'Rule to include'.

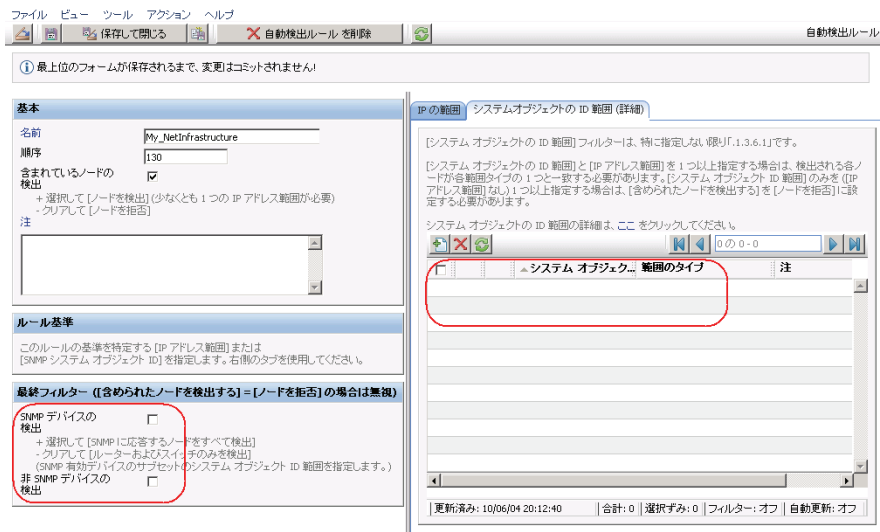
- b 各 sysObjectID を入力し (先頭のピリオドは入力しません)、次に **[SNMP デバイスの検出]** チェック ボックスをオンにします。(デフォルトでは、NNMi はスイッチとルーターのみを検出します。これらのデバイスはスイッチまたはルーターとマークされていないこともあるので、sysObjectIDs を指定するときに **[SNMP デバイスの検出]** チェック ボックスをオンにします)。



- c NetBotz ルールを入力します。このルールは NNMi で .1.3.6.1.4.1.5528.* のようにワイルドカードを 1 つ使用します。NNMi では、アスタリスク (*) を使用する必要はありません。



- d 最後のルールはスイッチとルーター用です。NNMi はデフォルトでこれらのデバイスを検出するため、システム オブジェクト ID は指定しないでください。IP アドレス範囲のみを指定してください。



検出からのアドレスの除外

検出しない IP アドレスを指定できます。[除外対象 IP アドレス] フィルタに、SNMPv1/SNMPv2c エージェントや SNMPv3 エンジンに関連付けられたアドレス (管理アドレス) は指定しないでください。



netmon.noDiscover ファイルが NNM 管理ステーションにない場合、複製する設定はありません。NNMi コンソールの方法に従って、NNMi で検出しない IP アドレスを指定します。

NNM から収集

アップグレード ツールによる方法

nnmmigration.ovpl ツールによって、NNM 管理ステーションから netmon.noDiscover ファイルを収集してあります。

手動による方法

以下のファイルを確認して、NNM が検出から除外する IP アドレスを判定します。

- **Windows:** %OV_CONF%\netmon.noDiscover
- **UNIX:** \$OV_CONF/netmon.noDiscover

NNMi に複写

アップグレード ツールによる方法

1 ディレクトリを次のように変更します。

- **Windows:** %NnmDataDir%\tmp\migration\<hostname>\CONFIG\conf¥
- **UNIX:** \$NnmDataDir/tmp/migration/<hostname>/CONFIG/conf

- 2 netmon.noDiscover ファイルにある IP アドレスを NNMi データベースにインポートします。

- *Windows:*

```
%NnmInstallDir%\bin\nnmdiscocfg.ovpl -excludeIpAdrrs ¥  
-f netmon.noDiscover
```

- *UNIX:*

```
$(NnmInstallDir)/bin/nnmdiscocfg.ovpl -excludeIpAdrrs ¥  
-f netmon.noDiscover
```

NNMi コンソール 方法

NNMi コンソールで、[設定] ワークスペースから [検出の設定] を選択します。[除外対象 IP アドレス] タブで、netmon.noDiscover ファイルから得た IP アドレスを入力します。

シード検出のためにシードを NNMi に追加します。

NNM から収集

アップグレード ツールによる方法

nnmmigration.ovpl ツールが、NNM 管理ステーションから NNM データベース内のデバイス リストを収集し、topology.out ファイルにしました。

手動による方法

次のコマンドを実行して、NNM データベース内のデバイスの正確なリストを調べます。

```
ovtopodump > topology.out
```

NNMi で複写

- 1 NNM から topology.out (エクスポート) ファイルを探します。

- アップグレード ツールによる方法では、このファイルは以下の場所にあります。

- *Windows:*

```
%NnmDataDir%\tmp¥migration¥<hostname>¥TOPO¥topology.out
```

- *UNIX:*

```
$(NnmDataDir)/tmp/migration/<hostname>/TOPO/topology.out
```

- 手動による方法では、このファイルはローカル ディレクトリにあります。

- 2 NNMi にインポートするには、NNM の topology.out ファイルをコピーして編集するか、エントリをファイルに入力し直します。新しいファイルでは、行ごとに 1 つの明確な IP アドレスまたはホスト名が記載されているはずですが、NNMi がサブネットを自動的に判断するため、サブネット プレフィックスを指定する必要はありません。

NNMi シード ファイルの例

```
10.2.32.201 # comment  
10.2.32.202 # comment  
lnt03.example.net # comment  
lnt02.example.net  
10.2.32.205
```



この代わりに、NNMi コンソール を使ってノードのこのリストを追加することもできます。

- 3 以下のコマンドを実行します。

```
nnmloadseeds.ovpl -f newSeedfile
```

詳細については、*nnmloadseeds.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 は、これらのシードに関連付けられたデバイスの検出を直ちに開始し、既存のデバイス プロファイル (およびステータス監視用のノード グループなどのノード グループ) を実装します。NNMi スパイラル検出は進行中です。検出ステータスの判定方法については、『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。

接続のカスタマイズ

デバイス情報が制限される特定の状況では、NNM の **Extended Topology** はネットワーク内のすべての接続を正確に検出およびモデル化しない可能性があります。その結果、接続が存在することが分かっているところに接続が表示されなかったり、接続が存在しないことが分かっているところに接続が示される可能性があります。この状況を是正するためには、正しい接続を手動で作成します。NNMi の接続設定を複製することもできます。

NNM から収集

- 1 次のファイルを確認して、NNM に接続が手動で設定されたかどうか調べます。

- **Windows:** %OV_CONF%\nnmet\connectionEdits
- **UNIX:** \$OV_CONF/nnmet/connectionEdits

これらのファイルの使用法については、『*Using Extended Topology*』マニュアルまたはホワイトペーパーのディレクトリを参照してください。

NNM の接続の例

次の例に、NNM 7.x で 2 つの接続を作成する方法を示します。1 つの接続は ifAlias を基礎にしており、もう 1 つの接続は ifIndex (ボードとともに) を基礎にしています。

```
N1.example.net[ifAlias:MyAlias],N2.example.net[ifAlias:MyOtherAlias]  
Y1.example.net[ 0 [ 999 ]],Y2.example.net[ 0 [ 2 ]]
```

NNMi に複写

- 2 nnmconnect.ovpl ツールを使って、NNMi で接続を編集します。ファイルフォーマットは NNM で使われているものとはまったく異なります。
 - a 接続テンプレートを生成するには、次のコマンドを実行します。

```
nnmconnect.ovpl -t addconn
```

詳細については、*nnmconnect.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。

- b テンプレート ファイル (addconn.xml) を編集して接続を変更または追加します。新しいファイルの構文については、ファイル内のドキュメントを参照してください。

NNMi の接続の例

以下の例では、330 ページの「NNM の接続の例」と同等の NNMi の例を示します。

```
<connectionedits>  
  <connection>  
    <operation>add</operation>  
    <node>N1.example.net</node>  
    <interface>MyAlias</interface>  
    <node>N2.example.net</node>  
    <interface>MyOtherAlias</interface>  
  </connection>
```

```

<connection>
  <operation>add</operation>
  <node>Y1.example.net</node>
  <interface>999</interface>
  <node>Y2.example.net</node>
  <interface>2</interface>
</connection>
</connectionedits>

```

- c 新しい接続情報をデータベースにロードするには、次のコマンドを実行します。
nnmconnedit.ovpl -f addconn.xml
- d NNMi コンソールで、[インベントリ] ワークスペースから [レイヤー 2 の接続] を選択し、結果を確認します。

フェーズ 4: ステータス モニタリングのアップグレード

NNM 6.x では、netmon プロセスがステータス モニタリングを実行します。NNM 7.x では、netmon プロセスまたは APA がステータス モニタリングを実行します。

- netmon プロセスは、インタフェースを含むノードのようなデバイスをモデル化し、おもにモード レベルでポーリング パラメータを適用します。
- APA は、アドレス、インタフェース、集合インタフェース、ボード、およびノードをモデル化します。APA はこれらのどのレベルでもポーリング パラメータを適用できます。

NNMi では、ノード、インタフェース、またはアドレスのレベルでポーリング パラメータを適用できます。

以下の機能動作は、NNMi では使用されなくなっており、転送不能です。

- DHCP ノードの特殊な処理
- ポーリングに応答しないノードの自動削除
- ボードと集合インタフェースは、現在は NNMi でモデル化されておらず、ステータス モニタリングを備えられません。

ポーリング間隔の設定

NNM から収集 NNM netmon ポーリング プロセス

netmon プロセスが NNM 一般ポーラーである場合は、NNM ユーザー インタフェースからポーリング間隔を取得します。

NNM APA ポーリング プロセス

NNM paConfig.xml の例

APA が NNM 一般ポーラーである場合は、paConfig.xml ファイルを見つけ、現在のポーリング間隔を知ります。例：

```

<classSpecification>
  <filterName>isRouter</filterName>
  <parameterList>
    <parameter>
      <name>interval</name>
      <title>Interval to Poll Device</title>
      <description>

```



```

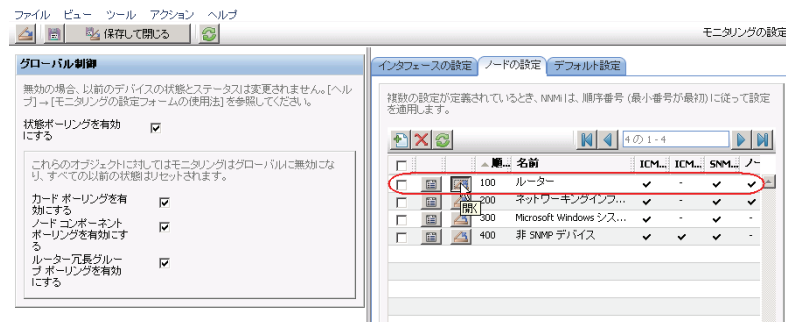
        デバイスがポーリングされる間隔
        in seconds.
    </description>
    <varValue>
        <varType>Integer</varType>
        <value>300</value>
    </varValue>
</parameter>
. . .
</parameterList>
</classSpecification>

```

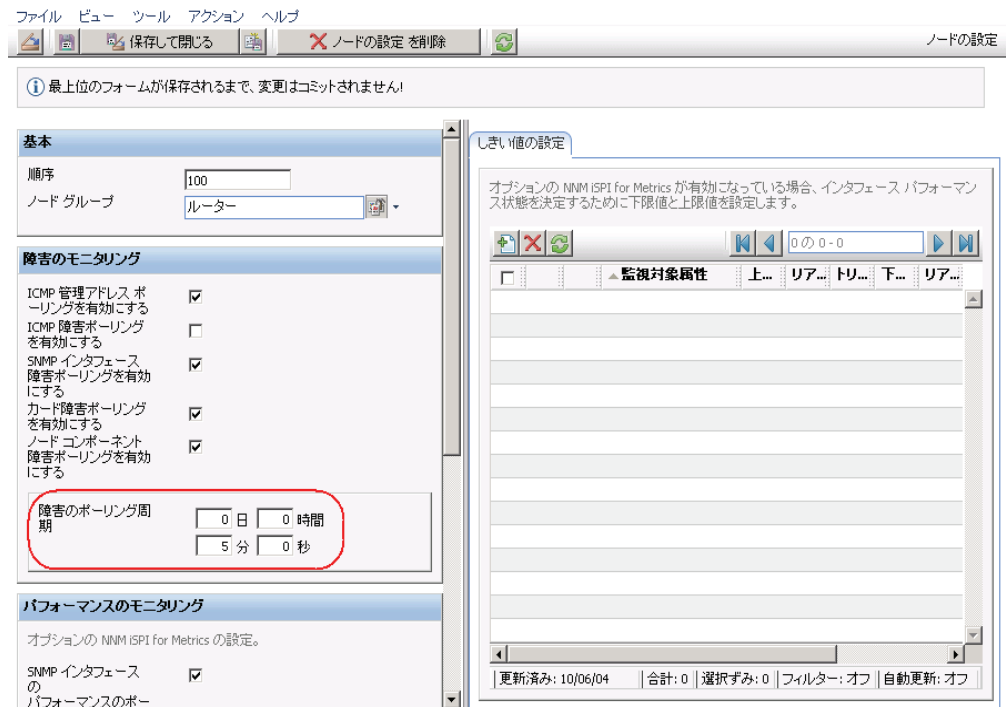
NNMi に複写 NNMi ポーリング プロセス

NNMi ステータス モニタリング設定はノードのグループまたはインタフェースのグループ (またはその両方) に基づいています。

- 1 NNMi コンソールで、**[設定]** ワークスペースから **[モニタリングの設定]** を選択します。
- 2 **[ノードの設定]** タブで、ノードグループを開きます。



- 3 グループの **[障害のポーリング周期]** を設定します。



ポーリング プロトコルの選択

NNM から収集 NNM netmon ポーリング プロセス

デフォルトでは、netmon プロセスは ICMP を使用して各アドレスをポーリングします (インタフェースに相当)。NNM は、一部のデバイスに対しては、netmon プロセスが ICMP ではなく SNMP を使用するように設定できます (両方を使用することはありません)。ICMP を使っているエリアがあるかどうか調べるには、次のファイルを確認します。

- **Windows:** %OV_CONF%\netmon.snmpStatus
- **UNIX:** \$OV_CONF/netmon.snmpStatus

NNM APA ポーリング プロセス

APA はポーリング用に SNMP と ICMP の組み合わせを使用します。APA では、フィルタごとにグループにまとめられたノードまたはインタフェースにポーリング方針が適用されます。フィルタは TopoFilters.xml ファイルで定義します。ポーリング方針は paConfig.xml ファイルで定義します。

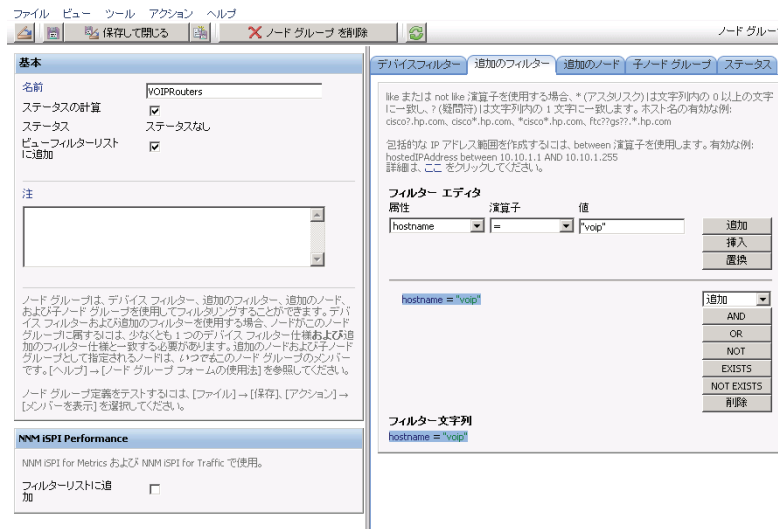
NNMi で複写 NNMi ポーリング プロセス

NNMi では、ノードとインタフェースの集合はノード グループとインタフェース グループとして定義します。ポーリング方針は [モニタリングの設定] フォームでノード グループとインタフェース グループに適用されます。

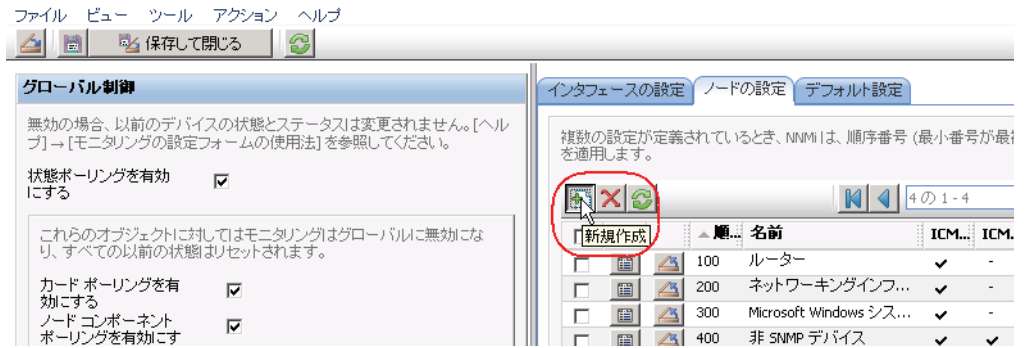
NNMi ポーリング設定の例

たとえば、(SNMP と ping を使って) VOIP ルーターの集合にポーリングを設定するには、以下の手順に従います。

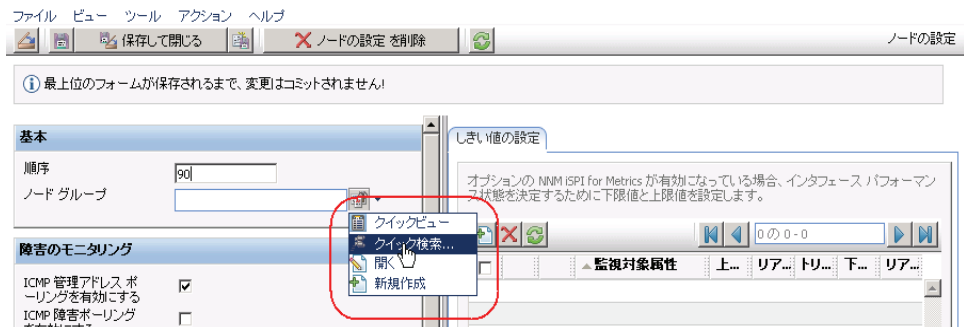
- 1 [ノードグループ] フォームを使って、VOIP ルーターを識別するノードグループを作成します。このフォームを保存し、閉じます。



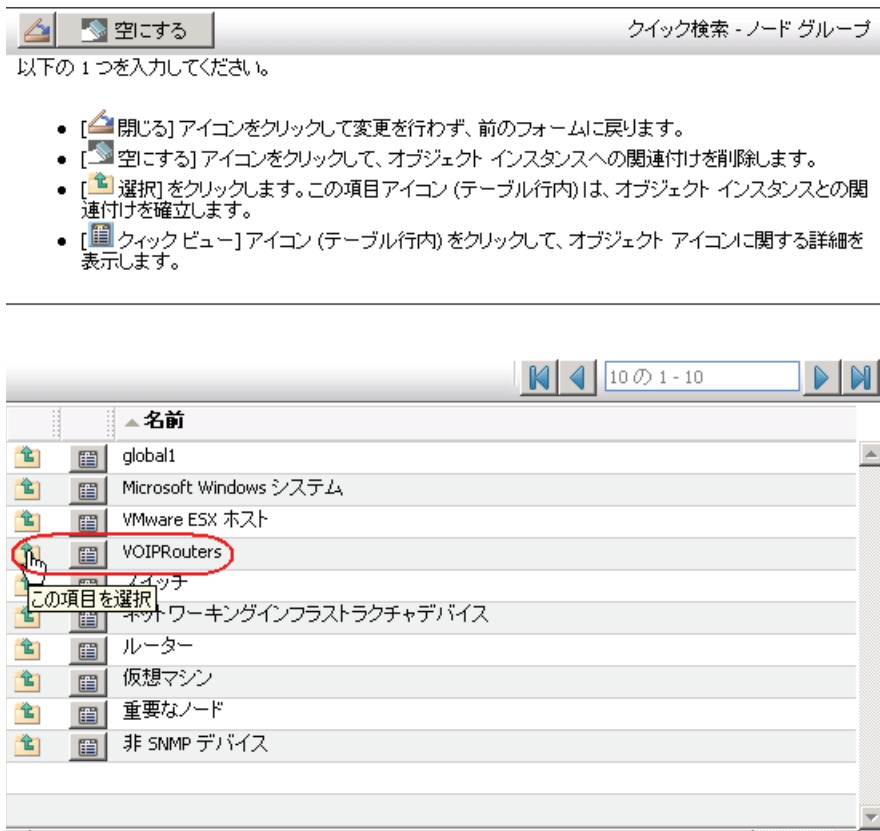
- 2 **[モニタリングの設定]** フォルダで、次のように、新しいノードの設定を追加します。



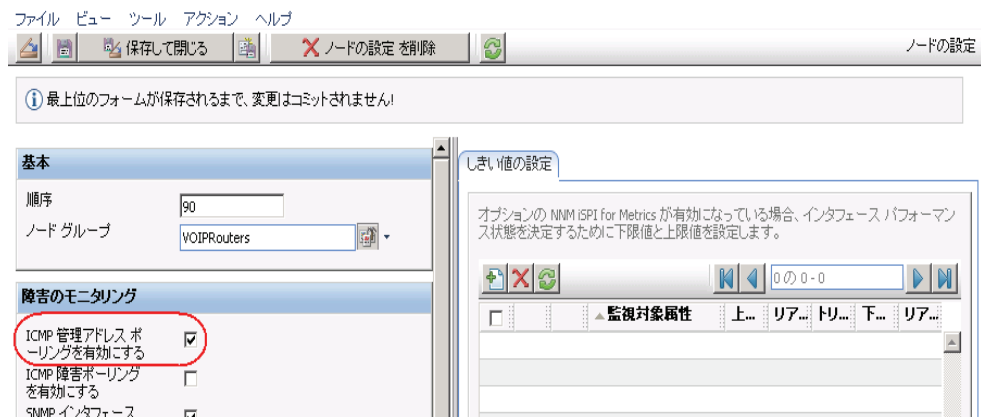
- 3 順序付けの値を指定してから、次のように、**[ノードグループ]** フィールドの高速検索を選択します。



- 4 以下に示すように、**VOIPRouters** ノードグループを選択します。



- 5 以下示すように、[ICMP 管理アドレス ポーリングを有効にする] チェックボックスがオンになっていることを確認します。フォームを保存し、閉じます。



危険域にあるノードの設定

デフォルトで、NNMi には重要ノード用のノードグループがあります。このノードグループは、NNM の危険域にあるノードリストと同じ方法で機能します。

重要ノードが故障または到達不可能な場合、NNMi は、ノードステータスが危険域であると表示し、NodeDown インシデントを生成します。

NNM から収集

NNM netmon ポーリング プロセス

NNM がステータス モニタリングに netmon を使っている場合、NNM は危険域にあるノード用に設定されません。NNMi に新しい危険域にあるノードの設定を作成できます。

NNM APA ポーリング プロセス

次のファイルを確認し、APA についてどのノードが危険域にあると指定されたか調べます。

- **Windows:** %OV_CONF%\nnmet\topology\filter\CriticalNodes.xml
- **UNIX:** \$OV_CONF/nnmet/topology/filter/CriticalNodes.xml

CriticalNodes.xml ファイルは、以下の例に似ています。

NNM CriticalNodes.xml の例

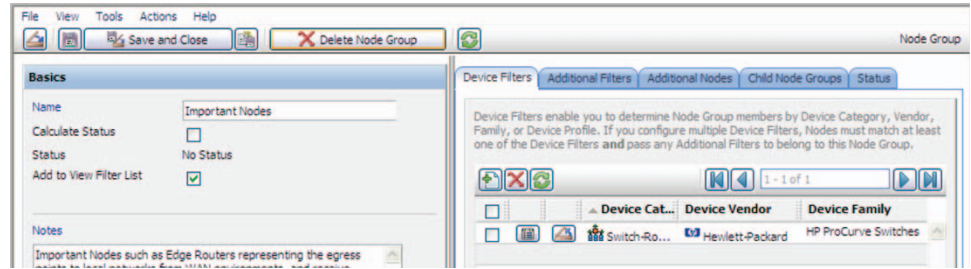
```
<HostIDs xmlns="http://www.hp.com/openview/NetworkTopology/
TopologyFilter" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xsi:schemaLocation="http://www.hp.com/openview/
NetworkTopology/TopologyFilter HostIDFile.xsd">
  <DNSName>router1.example.net</DNSName>
  <DNSName>router7.example.net</DNSName>
  <DNSName>MPLSRtr*.example.net</DNSName>
</HostIDs>
```

NNMi に複写

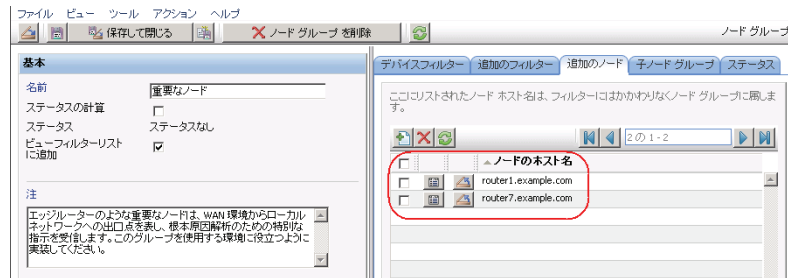
NNMi ポーリング プロセス

- 1 NNMi コンソールで、[設定] ワークスペースから [ノードグループ] を選択します。
- 2 [重要ノード] グループを開きます。
- 3 次のように、ホスト名ワイルドカード、デバイス フィルタ、または特定のノードごとに、重要ノードをグループに追加します。

- a デバイス フィルタを追加します。



- b 特定のノードを追加します。フォームを保存し、閉じます。

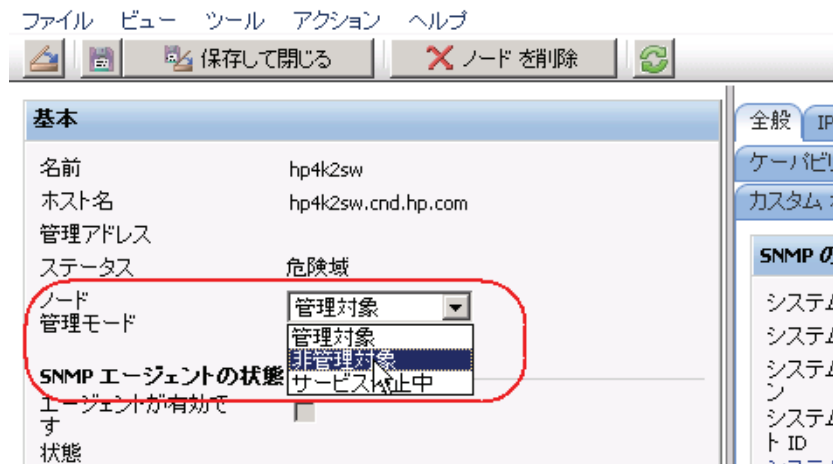


ステータス ポーリングからオブジェクトを除外します。

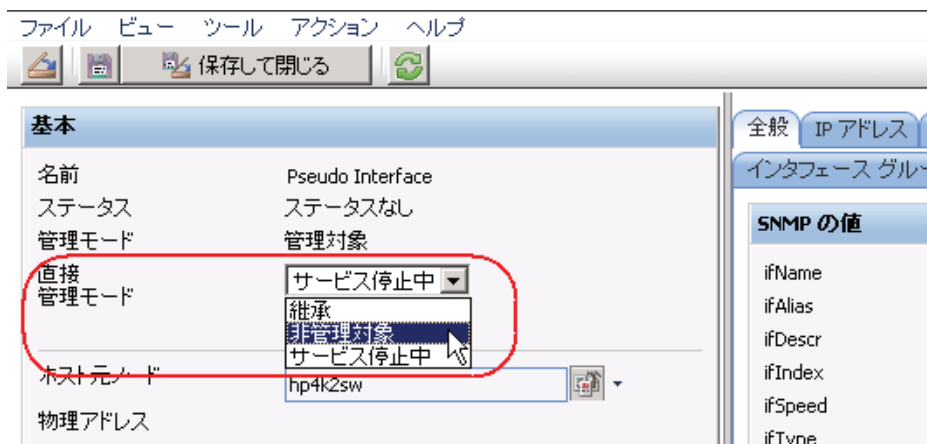
NNM では、ノードまたはインタフェースがモニタリングされるのを停止する (UNMANAGED 「非管理対象」状態に設定する) ほとんどのアクティビティは NNM ユーザー インタフェースによって手動で完了されます。

NNMi はオブジェクトの管理除外プロセスを簡単にします。新しい製品のデフォルトを、手動で実行していたものと一致させることはできます (たとえば、アップリンクのポーリングのみ)。しかし、ノードグループとインタフェースグループを使って設定を管理すれば、設定の自動更新が簡単になります。

ノードまたはインタフェースを **Not Managed (管理対象外)** とマークする必要がある場合もあります。以下に示すように、[ノード] フォームでは個々のノードの管理モードを設定できます。



以下に示すように、[インタフェース] フォームでは個々のインタフェースの管理モードを設定できます。



フェーズ 5: イベント設定とイベント削減のアップグレード

NNM は、拡張 **SNMPv2** フォーマットを使用して、受信イベント (管理対象デバイスからのトラップ、内部プロセス通信、転送されたイベント) の全ソースを分析します。イベントごとに、1つのイベント オブジェクト識別子、1つの名前、および設定パラメータがあります。

NNMi はイベントのさまざまなソースを異なるように処理します。デバイスからのトラップと NNM 管理ステーションから転送されたイベントのフォーマットは **SNMPv2c** です。NNMi 内部で作成されたインシデントには名前だけがあります。イベント オブジェクト識別子はありません。さらに、NNMi 内部プロセス通信では新規 (トラップ以外) メカニズムを使用して、全体的なパフォーマンスが大幅に改善されています。NNMi には、認識されないイベントに対する `no format in trapd.conf` メッセージはありません。認識されないメッセージは破棄されるようになりました。NNM 管理ステーションから NNMi 管理サーバーにイベントを転送する場合は、NNMi 側に転送されるすべてのイベントのインシデント定義があるようにします。

構成要素関連処理の種類 (**suppress** (抑制)、**enhance** (拡張)、**transient** (過渡)、**multisource** (複数ソース)) は、NNMi では使用されなくなっており、転送できません。

デバイスからのトラップの表示

NNM 環境に類似した方法で、デバイスからのトラップを表示するよう NNMi を設定できます。

NNMi には、NNM に同梱されている一般的な **SNMP** トラップおよびベンダー トラップの多くのデフォルト設定があります。これらトラップのカスタマイズによって、NNMi を更新できます。

メッセージと自動アクションに使用できる変数のリストについては、NNMi ヘルプの「インシデント用アクションの設定」と「インシデント アクション設定用の有効なパラメータ」を参照してください。

NNM から収集 アップグレード ツールによる方法

`nnmmigration.ovpl` ツールによって `trapd.conf` ファイルと NNM にロードされている MIB を収集してあります。

手動による方法

NNM 設定にカスタマイズされたトラップがあるかどうか調べます。カテゴリ、重要度、表示メッセージ、または自動処理について行われたカスタマイズに注意してください。

NNMi に複写

アップグレード ツールによる方法

- 1 ディレクトリを次のように変更します。
 - **Windows:** %NnmDataDir%\tmp\migration\<hostname>\CONFIG\conf\
 - **UNIX:** \$NnmDataDir/tmp/migration/<hostname>/CONFIG/conf/
- 2 NNM MIB を NNMi にロードします。

- **Windows:**
%NnmInstallDir%\migration\bin\%nnmmibmigration.ovpl %
-ファイル snmpmib -u <user> -p <password>
- **UNIX:**
\$NnmInstallDir\migration\bin\%nnmmibmigration.ovpl %
-ファイル snmpmib -u <user> -p <password>



このステップでは、MIB エントリの TRAP-TYPE と NOTIFICATION-TYPE のみロードします。NNMi ではその他の MIB 変数は使用されません。

- 3 NNMi に含まれない NNM イベント定義をロードします。
 - **Windows:**
%NnmInstallDir%\migration\bin\%nnmtrapdload.ovpl %
-loadTrapd <lang>\trapd.conf -authorLabel NNM_migration %
-authorKey com.domain.nnmUpgrade -u <user> -p <password>
 - **UNIX:**
\$NnmInstallDir/migration/bin/%nnmtrapdload.ovpl %
-loadTrapd <lang>/trapd.conf -authorLabel NNM_migration %
-authorKey com.domain.nnmUpgrade -u <user> -p <password>

ベストプラクティス

このオペレーションの作成者を一意に指定し、これらのイベント定義を後で識別できるようにしておくことをお勧めします。

手動による方法

- 1 ベンダー MIB ファイルを NNMi 管理サーバーにダウンロードします。
- 2 MIB ごとに次のコマンドを実行します。

```
nnmincidentcfg.ovpl -loadTraps mibFile
```

 - ある MIB に別の MIB ファイルへの依存関係がある場合は、次のコマンドを使用して依存関係を事前にロードします。

```
nnmincidentcfg.ovpl -loadMib mibFile
```

この代わりに、nnmloadmib.ovpl コマンドを使用してから、loadTraps オプションを指定して nnmincidentcfg.ovpl を再実行することもできます。
 - どの MIBs がすでにロードされているか知るには、次のコマンドを使用します。

```
nnmloadmib.ovpl -list
```

詳細については、*nnmincidentcfg.ovpl* と *nnmloadmib.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。



以下のステップでは、TRAP-TYPE と NOTIFICATION-TYPE の MIB エントリのみをロードします。NNMi ではその他の MIB 変数は使用されません。

NNMi での強化

- 3 NNMi コンソールで、[設定] ワークスペースから [インシデントの設定] フォームを選択します。[SNMP トラップ] タブには、受信した SNMP トラップに設定したインシデントが表示されます。
- 4 トラップ インシデントが NNM のインシデントと一致するようにカスタマイズします。トラップ設定フォームで、必要に応じてカテゴリを作成できます。
- 5 (オプション) デフォルト設定 [重大度]、[カテゴリ]、および [メッセージの形式] に加えて、デフォルトの [ファミリー] を設定します。
- 6 (オプション)。トラップが [根本原因インシデント] ビューに表示されるように、トラップを根本原因として分類します。

NNMi で生成された管理イベント表示のカスタマイズ

NNMi では、イベント設定は簡単になっています。NNMi Causal Engine は NNM よりも簡潔な根本原因を生成します。

NNMi で生成されたインシデントを変更し、NNM アラームと類似した外見にします。たとえば、NNMi NodeDown インシデント メッセージを NNM NodeDown アラーム メッセージに類似するようカスタマイズできます。

NNM から収集

NNMi に複写

- 1 NNM で、イベント設定のカスタマイズを決定します。
- 2 NNMi コンソールで、[設定] ワークスペースから [インシデントの設定] フォームを選択します。次に、[管理イベント] タブを選択します。
- 3 イベント番号ではなく名前で、新しいインシデント設定を見つけます。
- 4 オプション。イベント表示を NNM のイベント表示と一致するようカスタマイズするには、トラップ設定フォームでカテゴリを作成します。
- 5 デフォルトの設定 [重大度]、[カテゴリ]、および [メッセージの形式] 設定に加えて、デフォルトの [ファミリー] を設定できます。

トラップのブロック / 無視 / 無効化

NNM にはさまざまなレベルのイベント処理が備わっています。

- トラップが ovtrapd に入ってくる時にトラップをブロック
- IGNORE というラベルのトラップまたはイベントは、処理はするが、保存または表示はしない
- LOGONLY というラベルの (相関) イベントを保存および処理するが、表示はしない
- イベントをカテゴリに保存、処理、表示する
- 設定なしに到着するトラップは、No format in trapd.conf for... (trapd.conf でフォーマットなし) として Alarm Browser に表示され、データベースに保存されます。

NNMi にはもっと簡単な方法があります。disabled(無効) イベントまたはトラップは保存、処理、または表示されません。enabled(有効) イベントまたはトラップは完全に保存、処理、表示されます。NNMi に設定がないイベントはブロックされます。

NNM から収集

アップグレード ツールによる方法

nnmmigration.ovpl ツールによって ovtrapd.conf ファイルを収集してあります。



ovtrapd.conf ファイルは、NNM 7.51 以上で使用可能です。アップグレード ツールによる方法では、トラップ定義を考慮しません。NNM トラップ用に手動で LOGONLY 設定を取り込むことができます。

手動による方法

- 1 トラップを無視するカスタマイズまたはトラップを LOGONLY に設定するカスタマイズを決定します。
- 2 NNM がトラップ フィルタ メカニズム (ovtrapd.conf、NNM 7.51 では新規) を使用するかどうか調べます。

NNMi に複写

アップグレード ツールによる方法

- 1 ディレクトリを次のように変更します。
 - **Windows:** %NnmDataDir%\tmp\migration\<hostname>\CONFIG\conf\
 - **UNIX:** \$NnmDataDir/tmp/migration/<hostname>/CONFIG/conf/
- 2 コメント化されていない行を、NNM ovtrapd.conf ファイルから nnmtrapd.conf ファイルにコピーします。
 - **Windows:**
%NnmInstallDir%\migration\bin\%nnmtrapdMerge.ovpl %
ovtrapd.conf
 - **UNIX:**
\$NnmInstallDir/migration/bin/nnmtrapdMerge.ovpl %
ovtrapd.conf

手動による方法

- 1 NNMi コンソールで、[設定] ワークスペースから [インシデントの設定] フォームを選択します。受信や表示を行わないイベントを見つけ、これらイベントの [使用可能] チェック ボックスをオフにします。
- 2 特定の IP アドレスからトラップをブロックするには、以下のファイルを編集し、NNM からのトラップ フィルタリング情報を使用して NNMi をアップデートします。
 - **Windows:** %NnmDataDir%\shared\%nnm\conf\%nnmtrapd.conf
 - **UNIX:** \$NnmDataDir/shared/nnm/conf/nnmtrapd.conf
- 3 nnmtrapconfig.ovpl コマンドを使用してトラップ ブロッキングを有効にし、トラップ ブロッキングのレートとしきい値を設定します。

このコマンドの使用法については、*nnmtrapconfig.ovpl* リファレンス ページ、または UNIX マニュアルを参照してください。

ライフサイクル移行アクションの設定

NNM から収集

NNMi に複写

- 1 NNM 用に設定された自動処理を決定します。
- 2 NNM 管理ステーションの処理スクリプトを NNMi 管理サーバーにコピーします。この場合、ファイルの位置は重要ではありません。
- 3 NNMi コンソールで、[設定] ワークスペースから [インシデントの設定] フォームを選択します。

- 4 自動アクションを持つ NNM イベントそれぞれに対応する、そのアクションを持つ NNMi インシデントを設定します ([アクション] タブで)。

NNM の動作と一致させるために、[ライフサイクル状態] を [登録済み] に設定します。

NNMi での強化

- 5 次の NNMi 設定テクニックに注意してください。
 - イベント到着時に発生する複数の自動処理を設定できます。
 - 他のライフサイクル状態ごとに、1 つまたは複数の追加処理を設定できます (ライフサイクル状態は、In Progress (進行中)、Completed (完了済み)、Closed (閉じている))。
 - NNM より多くのインシデント属性をコマンドに渡せます。
 - NNMi がコマンドを実行する前に、別の設定ファイルにコマンドを登録する必要はないので、手順は簡単になっています。

追加 (手動) 処理の設定

NNM には、Alarms Browser のメニューから利用できるオペレータの操作または追加の操作が用意されています。NNMi コンソールメニューから利用できる URL 操作で NNM 処理をシミュレートすることもできます。

NNM から収集

NNMi に複写

- 1 NNM にカスタムなオペレータ アクションがないか判定します。
- 2 これらのカスタム アクションについて、URL として利用できるように転送する方法を決定します。
- 3 NNMi コンソールで、[設定] ワークスペースから [ユーザー インタフェースの設定] を選択します。
- 4 [メニュー項目] タブで、[新規作成] をクリックします。
- 5 [メニュー項目] フォームで、[メニュー項目ラベル]、[一意のキー]、[順序]、および [選択タイプ] を入力します。
- 6 [メニュー項目コンテキスト] タブで、[新規作成] をクリックします。
- 7 [メニュー項目コンテキスト] フォームで、[メニュー項目アクション] に対し [新規起動アクション] を選択します。
- 8 [起動アクション] フォームに、アクションの [名前] と [フル URL] を入力します。
- 9 [保存して閉じる] をクリックして NNMi コンソールに戻ります。

イベント相関処理：イベントの繰り返し

NNM では、イベントを複製するときに、最初のイベントまたは最後のイベントのどちらかを親として使用します。

NNMi は、相関特性が [重複解除ストリーム相関処理] の親を新規作成します。この親インシデントは、[全インシデント] インシデント ビューに表示されます。元のイベントは、設定されたインシデント ビューに表示されます。

NNM から収集

- 1 RepeatedEvents 相関処理が NNM に使われるかどうか調べます。
- 2 Repeated 相互関係が NNM に使われるかどうか調べます。
- 3 複製が使われているかどうか調べます (dedup.conf ファイル)。

NNMi に複写

- 4 NNMi コンソールで、[設定] ワークスペースから [インシデントの設定] フォームを選択します。
- 5 重複を削除するインシデント タイプを開きます。
- 6 [重複削除] タブで、以下の手順を実行します。
 - a [有効にする] を選択してモニタリングを有効にします。
 - b カウント ウィンドウを設定します。
 - c 時刻ウィンドウを設定します ([時間]、[分]、および [秒] の各フィールド)。
 - d 新しい親イベントとして、[DuplicateCorrelation] を選択します ([関連処理インシデントの設定])。
 - e [比較の条件] を定義します。

詳細については、NNMi ヘルプの「SNMP トラップインシデントの重複削除の設定」を参照してください。

イベント関連処理：レート計算

NNM では、イベントを複製するときに、最初のイベントまたは最後のイベントのどちらかを親として使用します。

NNMi は、関連特性が [レート ストリーム関連処理] の親を新規作成します。この親インシデントは、[全インシデント] インシデント ビューに表示されます。元のイベントは、設定されたインシデント ビューに表示されます。NNMi では、NNM の継続時間ウィンドウと同じレート動作が保持されています。

NNM から収集

NNMi に複写

- 1 レート関連処理が NNM に使われるかどうか調べます。
- 2 NNMi コンソールで、[設定] ワークスペースから [インシデントの設定] フォームを選択します。
- 3 [管理イベント] タブを選択します。
- 4 カウントするインシデント タイプを開きます。

- 5 **[レート]** タブで、以下の手順を実行します。
 - a **[有効にする]** を選択してモニタリングを有効にします。
 - b カウント ウィンドウを設定します。
 - c 時刻ウィンドウを設定します (**[時間]**、**[分]**、および**[秒]** の各フィールド)。
 - d 新しい親イベントとして **[RateCorrelation]** を選択します (**[相関処理インシデントの設定]**)。
 - e **[比較の条件]** を定義します。

詳細については、NNMi ヘルプの「管理イベント インシデントのレートの設定(時間およびカウント)」を参照してください。

イベント相関処理 : Pairwise のキャンセル

NNMi では、キャンセルは特定の時刻ウィンドウに制限されません。

NNM から収集

- 1 NNM で、PairWise のレート相関処理が使われるかどうか調べます。

- 2 NNM で、過渡的レート相関処理が使われるかどうか調べます。

NNMi に複写

- 3 NNMi コンソールで、**[設定]** ワークスペースから **[インシデントの設定]** フォームを選択します。

- 4 **[Pairwise の設定]** タブで、既存のペアを選択するか、**[新規作成]** をクリックします。

- 5 ペアにされたイベント識別子および一致基準を設定します。

詳細については、NNMi ヘルプの「**[Pairwise の設定]** フォーム」を参照してください。

イベント相関処理 : スケジュールされたメンテナンス

NNMi では、使用不能ノードのモニタリングを抑制できます。これを行うには、サービス外モードを使います。NNM とは異なり、サービス外メンテナンスを前もってスケジュールすることはできません。手動でオブジェクトを管理対象モードに戻す必要があります。



サービス外モードのデバイスが送信した SNMP トラップは NNMi 内で抑制されます。

組織がスケジュールされたメンテナンス相関処理を使っている場合は、一緒にオフラインになったシステムのリストを使用できます。

NNM から収集

- 1 ScheduledMaintenance 相関処理が NNM に使われるかどうか調べます。

NNMi に複写

- 2 NNMi コンソールで、**[設定]** ワークスペースから **[ノード グループ]** を選択します。

- 3 **NNM メンテナンス リスト** 内のノードのセットごとにノード グループを作成します。ノード グループをビューフィルタとして利用できるように設定します。

- 4 メンテナンスのときは、NNMi コンソールで **[インベントリ]** ワークスペースから **[ノード]** を選択します。

- 5 ビューを特定のノード グループにフィルタするには、上端の **[ノードグループフィルタを設定]** セレクタを使用します。

- 6 全ノードを選択してから、**[アクション]**>**[管理モード]**>**[サービス停止中]** を選択します。

- 7 メンテナンスが完了した後、ノードを選択してから、**[アクション]**>**[管理モード]**>**[管理]** を選択します。

フェーズ 6: グラフィカルな視覚化のアップグレード (OVW)

NNM では、OVW マップは複数のサブマップから構成されており、サブマップそれぞれがネットワーク階層における 1 つの場所またはサブネットを示します。NNM 管理者は、複数の OVW マップを定義し、各ユーザーに異なる OVW マップを割り当てることができます。

NNMi では、トポロジ マップは定義されたノード グループに基づいています。トポロジ マップには階層型の関係を持つものもありますが、そのような階層はネットワークのサブネットや場所の制限を受けません。また、全ユーザーが使用可能なトポロジ マップすべてにアクセスできます。

NNMi アップグレード ツールは、1 OVW マップのロケーション サブマップ階層の複製を作り NNMi に置くことができます。マップ構造は、2 つの製品間で大きく異なるので、アップグレード ツールはノード、ネットワーク、またはリーフ ノード要素を NNM から転送しません。

NNM から収集 アップグレード ツールによる方法

- 313 ページの「フェーズ 1: NNM 管理ステーションからのデータ収集」で説明したようにアップグレード ツールが設定されていることを確認します。
- 以下の値になるよう、PERL5LIB 環境変数を設定または作成します。
 - Windows:** `install_dir¥migration¥lib`
 - UNIX:** `/opt/OV/migration/lib`
- NNMi で使用するロケーション階層を最もよく表している NNM マップを特定して開きます。
- 開いたマップで、**[ファイル]>[エクスポート]** をクリックして、以下の名前と場所でマップ データ ファイルを作成します。
 - Windows:** `install_dir¥migration¥ipmap.out`
 - UNIX:** `/opt/OV/migration/ipmap.out`
- ディレクトリを次のように変更します。
 - Windows:** `install_dir¥migration¥`
 - UNIX:** `/opt/OV/migration/`
- マップ データ ファイルを処理します。
 - Windows:**
`install_dir¥migration¥bin¥nnmmapmigration.ovpl ipmap.out`
 - UNIX:**
`/opt/OV/migration/bin/nnmmapmigration.ovpl ipmap.out`このコマンドは、`nnmnodegrouplist.csv` ファイルと `backgrounds.tar` ファイルを作成します。ファイルは以下の場所にあります。
 - Windows:** `install_dir¥migration¥<hostname>¥MAPS¥`
 - UNIX:** `/opt/OV/migration/<hostname>/MAPS`


NNMi で複写 アップグレード ツールによる方法

- まだ行っていない場合は、`nnmnodegrouplist.csv` ファイルと `backgrounds.tar` ファイルを NNM 管理サーバーから以下の場所にコピーします。
 - Windows:** `%NnmDataDir%¥tmp¥migration¥<hostname>¥MAPS¥`
 - UNIX:** `$NnmDataDir/tmp/migration/<hostname>/MAPS/`

- 2 ディレクトリを次のように変更します。
 - **Windows:** %NnmDataDir%\tmp\migration\\MAPS\
 - **UNIX:** \$NnmDataDir/tmp/migration/<hostname>/MAPS/
- 3 NNM ロケーション階層のノード グループ定義を NNMi データベースにインポートします。
 - **Windows:**

```
%NnmInstallDir%\bin\nnmloadnodegroups.ovpl -u <user> %  
-p <password> -r false -f nnmnodegrouplist.csv
```
 - **UNIX:**

```
$NnmInstallDir/bin/nnmloadnodegroups.ovpl -u <user> %  
-p <password> -r false -f nnmnodegrouplist.csv
```
- 4 NNM 背景グラフィクスを NNMi でも使用できるようにします。
 - a NNMi 管理サーバーのオペレーティング システムに合ったツールまたはコマンド (restoreMigration.ovpl など) を使用して backgrounds.tar ファイルを解凍します。
 - b 抽出したファイルを、以下の場所にコピーします。
 - **Windows:** %NnmDataDir%\shared\nnm\www\htdocs\images\
 - **UNIX:** \$NnmDataDir/shared/nnm/www/htdocs/images/

あるいは、FTP を ASCII モードで使用して、個々のイメージファイルを images ディレクトリに転送します。
- 5 NNMi コンソールで、該当する背景グラフィクスをそれぞれのロケーション ノード グループ マップに適用します。
 - a NNMi コンソールで、**[設定]** ワークスペースから **[ノード グループ]** を選択します。
 - b **[注]** ボックスのテキストを確認します。
アップグレード ツールでノード グループを作成した場合、**[注]** フィールドには **OVW** ロケーション シンボルから作成されたことが示されます。OVW サブマップに背景グラフィクスが含まれていた場合、**[注]** にはイメージ名も指定されています。
 - c 複製されたノード グループの **[ノード グループ]** フォームから、**[アクション]> [ノード グループ マップ]** をクリックします。
 - d マップで、**[レイアウトの保存]**  をクリックして、このノード グループ用のノード グループ設定オブジェクトを作成します。
 - e 同じマップで、**[ファイル]> [オープン ノード グループ マップ設定]** をクリックします。

- f **[ノードグループマップの設定]** フォームの **[背景イメージ]** タブで、手順 b で説明したように、このノードグループの **[ノードグループ]** フォームの注のテキストに指定されている背景グラフィック ファイルを指定します。



[ノードグループマップの設定] フォームでは、背景グラフィクス ファイルへのパスは以下のフォーマットです。

```
/nnmbg/images/<optional_directory_structure>/<filename>
```

ファイル システムで、/nnmbg/images/ は以下にマップされます。

— **Windows:** %NnmDataDir%\\$shared¥nnm¥www¥htdocs¥images¥

— **UNIX:** \$NnmDataDir/shared/nnm/www/htdocs/images/

(注のテキストにあるパスが、NNM 管理ステーションに適用されます。)

- 6 **NNMi** コンソールで、ロケーション階層内で最下層レベルのトポロジマップに、1つ以上のノードグループを追加します。

フェーズ 6: グラフィカルな視覚化のアップグレード (ホームベース)

NNM 7.x Advanced Edition では、ホームベースには、ネットワーク トポロジを整理したコンテナ ビューを含めることができます。

NNMi では、トポロジマップは定義されたノードグループに基づいています。トポロジマップには階層型の関係を持つものもありますが、そのような階層はネットワークのサブネットや場所の制限を受けません。また、全ユーザーが使用可能なトポロジマップすべてにアクセスできます。

NNMi アップグレード ツールは、NNMi にホームベース コンテナ ビュー階層を複製できます。マップ構造は、2つの製品間で大きく異なるので、アップグレード ツールはノード、ネットワーク、またはリーフノード要素を NNM から転送しません。

NNM から収集 アップグレード ツールによる方法

nnmmigration.ovpl ツールによって、NNM 管理ステーションからコンテナビューの設定ファイルを収集してあります。

NNMi で複写 アップグレード ツールによる方法

- ディレクトリを次のように変更します。
 - Windows:** %NnmDataDir%\\$tmp¥migration¥<hostname>¥NNMET¥
 - UNIX:** \$NnmDataDir/tmp/migration/<hostname>/NNMET/
- コンテナビューの設定ファイルを解析して、カンマ区切りのノードグループリストを作成します。
 - Windows:**
%NnmInstallDir%\\$migration¥bin¥nnmetmapmigration.ovpl ¥
containers.xml nnmcontainerlist.csv.txt
 - UNIX:**
\$NnmInstallDir/migration/bin/nnmetmapmigration.ovpl ¥
containers.xml nnmcontainerlist.csv

- 3 NNM 7.x Advanced Edition ホーム ベースのコンテナ階層のノード グループ定義を NNMi データベースにインポートします。
 - *Windows:*

```
%NnmInstallDir%\bin\nnmloadnodegroups.ovpl -u <user> %  
-p <password> -r false -f nnmcontainerlist.csv.txt
```
 - *UNIX:*

```
$NnmInstallDir/bin/nnmloadnodegroups.ovpl -u <user> %  
-p <password> -r false -f nnmcontainerlist.csv
```
- 4 NNMi コンソールで、ロケーション階層内で最下層レベルのトポロジ マップに、1つ以上のノード グループを追加します。

フェーズ 7: カスタム スクリプトのアップグレード

NNM には、NNM データベースの内容を読み取るための、コマンド ライン ツールがいくつかあります。これらのツールは、コマンド ラインから使用できます。また、それぞれのネットワーク環境用に作成されたスクリプトに組み込むこともできます。

bin ディレクトリにある `nnmtopodump.ovpl` コマンドは、以前はサポート対象外のツールとして `support` ディレクトリに置かれていたツールの改良版です。更新された `nnmtopodump.ovpl` コマンドでは、NNM `ovtopodump` コマンドと非常によく似たフォーマットのテキスト出力を生成できます。また、カスタム スクリプトの中にある他の NNM コマンドも `nnmtopodump.ovpl` コマンドに置き換えることができます。

NNM から収集

- 1 NNM データベースを読み取るためのカスタム スクリプトを作業ディレクトリにすべてコピーします。

NNMi で複写

- 2 作業ディレクトリを NNMi 管理サーバーにコピーします。
- 3 各スクリプトで、以下のコマンドを呼び出していないか調べます。

- `ovtopodump`
- `ovobjprint`
- `ovet_topodump.ovpl`
- `ovdwquery`

- 4 該当する場合は、この前のステップで挙げたコマンドがある箇所で、`nnmtopodump.ovpl` コマンドを呼び出すようそれぞれのスクリプトを更新します。



`nnmtopodump.ovpl` コマンドは、任意の NNM コマンドを直接置き換えるものではありません。`nnmtopodump.ovpl` からの出力と、期待される出力とを比較し、必要に応じてそれぞれのスクリプトを変更します。

- 5 求める結果を得られるまで、更新したそれぞれのスクリプトをテストしては修正します。

詳細については、`nnmtopodump.ovpl` リファレンス ページ、または UNIX マニュアルを参照してください。

アップグレード ツール リファレンス

このセクションでは、NNMi が提供するツールについて説明します。このツールは、NNM 6.x/7.x 設定の NNMi への複製を支援します。この情報は、このドキュメントのフッターに示された製品、パッチ バージョンの最新情報です。

データ収集ツール

NNM 6.x/7.x 管理ステーションでデータ収集ツールを実行し、NNM 設定情報を 1 か所に集めます。これらのツールを使用する手順は、この章ですでに説明してあります。

NNMi では、データ収集ツールは 2 つのアーカイブ ファイル (Windows オペレーティングシステム用の migration.zip、UNIX オペレーティングシステム用の migration.tar) として同梱されています。NNMi をインストールすると、アーカイブ ファイルは以下の場所にあります。

- **Windows:** %NnmInstallDir%\migration¥
- **UNIX:** \$NnmInstallDir/migration/

データ収集ツールは、NNM 管理ステーションのコマンドという利用上の制限があります。場合によっては、これらのツールを実行しても正常に完了しないことがあります。ラッパー スクリプトが失敗する場合は、ツールを個別に実行できます。ツール単独でも失敗する場合は、ツールの目的を再現して (ここで説明するように) データを自分自身で収集することができます。

表 16 に、データ収集ツール アーカイブ ファイルに含まれているツールをリストします。

表 16 アップグレード データ収集ツール

ツール	説明
createMigrationDirs.ovpl	アップグレード データを保存するためのディレクトリ構造を作成します。データは NNM 管理ステーションから収集されます。詳細については、349 ページの「NNM 設定データ ファイル」を参照してください。
nnmmigration.ovpl	NNM 設定データを収集します。 このツールは、このテーブルで説明している他のツールのほとんどを実行するラッパー スクリプトです。
archiveMigration.ovpl	収集したデータを、NNMi 管理サーバーに転送しやすいよう、1 つの tar アーカイブ ファイル (<hostname>.tar) にまとめます。
captureLocale.ovpl	NNM 管理サーバーの位置を判断し、ローカライズされた設定ファイルの正しいバージョンをツールが収集できるようにします。
hostnolookup.ovpl	snmpnolookupconf -dumpCache を実行して、NNM 検出で無視されるホスト名が入ったテキスト ファイル (DNS ディレクトリの hostnolookup.conf) を作成します。

表 16 アップグレードデータ収集ツール (続き)

ツール	説明
nmmtopodump.ovpl	ovtopodump -lr を実行し、テキスト ファイル (TOPO ディレクトリの ovtopodump.out) にトポロジ データベースのスナップショットを作成します。 このツールは、NNMi 管理サーバーの bin ディレクトリにインストールされている同名のツールとは異なります。
ovmapdump.ovpl	それぞれの OVW マップに対して ovmapdump -l を実行し、テキスト ファイル (MAPS ディレクトリに) にそのマップ データベースのスナップショットを作成します。
ovmibmigration.ovpl	NNM snmpmib ファイルに定義されている MIB がすべて NNM にロードされていることを確認します。
ovwdbDump.ovpl	ovobjprint を実行し、テキスト ファイル (OVWDB ディレクトリの ovobjprint.out) に将来のアップグレード ツールで使用するかもしれないオブジェクト データベースのスナップショットを作成します。
snmpCapture.ovpl	xnmsnmpconf -dumpCache を実行し、テキスト ファイル (SNMP ディレクトリの snmpCapture.out) に SNMP 設定データベースのスナップショットを作成します。 このツールは、表 18 で説明する同名のツールとは異なります。
trapdConfNodes.ovpl	trapd.conf ファイルを解析して、将来のアップグレード ツールで使用する可能性があるノード リスト (EVENTS¥NODES¥*) を作成します。
nnmmmapmigration.ovpl	OVW マップのエクスポート ファイルを解析して、そのマップ (MAPS ディレクトリの nnmnodegroupelist.csv) 内のロケーションのノード グループを特定し、背景イメージ ファイルを収集します。そのイメージ ファイルは、ロケーション サブマップ (MAPS ディレクトリの backgrounds.tar) で使用されます。 このコマンドは、nnmmigration.ovpl ラッパー スクリプトとは別に実行します。

NNM 設定データ ファイル

データ収集ツールは、以下の場所にファイルを保存します。

- *Windows:* install_dir¥migration¥<hostname>¥
- *UNIX:* /opt/OV/migration/<hostname>/

ここで、<hostname> は NNM 管理ステーションのホスト名です。表 17 に、<hostname> ディレクトリの内容をリストします。

表 17 収集された NNM 設定データのファイル構造

ディレクトリ	内容
CONFIG	NNM CONF ディレクトリのコピー
DNS	hostnlookup.conf
EVENTS	NNM 設定内の全 trapd.conf ファイル ノードリスト
MAPS	アプリケーション登録ファイル シンボル登録ファイル 各マップ データベースのフラット ファイル
NNMET	(NNM 7.x Advanced Edition) containers.xml
OVW.MAPS	nnmmapmigration.ovpl ツールからの出力
OVWDB	オブジェクト データベースのフラット ファイル フィールド登録ファイル
SNMP	コミュニティ文字列
TOPO	トポロジデータベースのフラット ファイル
WWW	NNM Web インタフェース ファイル

アップグレード用データ インポート ツール

表 18 は、NNMi で提供される NNM 6.x/7.x データを NNMi データベースにインポートするツールを示したものです。アップグレードプロセスでは、標準の NNMi ツールも使用します。標準ツールについては、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。

表 18 データ インポート ツール

ツール	説明
restoreMigration.ovpl	NNM 6.x/7.x 管理ステーションで archiveMigration.ovpl を実行して作成した NNM 設定アーカイブを解凍します。
nnmetmapmigration.ovpl	NNM 7.x Advanced Edition ホーム ベース コンテナ ビュー定義ファイル (containers.xml) を解析して、NNMi のそのビューにあるロケーションのノード グループを特定します。
nnmmibmigration.ovpl	nnmincidentcfg.ovpl を実行して、NNM snmpmib ファイルにある MIB を NNMi データベースにインポートします。 このツールでは、NNMi にすでにロードされている MIB は再ロードしません。

表 18 データ インポート ツール (続き)

ツール	説明
nnmtrapdload.ovpl	<p>トラップ定義を、NNM trapd.conf ファイルから NNMi データベースにロードします。</p> <p>このツールは、各トラップで最初に見つけた定義のみをロードします。NNMi にすでにロードされているトラップ定義は再ロードしません。</p>
nnmtrapdMerge.ovpl	<p>NNM ovtrapd.conf ファイル内のコメント化されていないコマンドラインをすべて、NNMi nnmtrapd.conf ファイルにマージします。</p>
snmpCapture.ovpl	<p>snmpCapture.out ファイルの内容を STDOUT に出力します。1 行に 1 コミュニティ文字列です。</p> <p>このツールは、表 16 で説明する同名のツールとは異なります。</p>

NNM 6.x または NNM 7.x と NNMi との統合

以下の HP Network Node Manager (NNM) 6.x/7.x の機能を HP Network Node Manager i Software (NNMi) と統合できます。

- NNM 6.x/7.x から NNMi 管理サーバーにイベントを転送して、インシデント ライフサイクルの管理に NNMi インシデント ビューを使用できます。
- いくつかの NNM 6.x/7.x ビューは NNMi 管理サーバーから開くことができます。

この統合は、NNMi へのアップグレードの割合を管理する場合に便利です。

この統合は、多数の NNM 6.x/7.x 管理ステーションを備えた大規模な管理環境にも便利です。ネットワーク全体を通して NNMi の新しい機能を必要としない場合は、NNMi を本来のネットワーク管理ツールとして使用しながら若干の NNM 6.x/7.x 管理ステーションを維持することができます。

この章の内容を使用して、サードパーティの製品を NNMi と統合することもできます。このサードパーティ製品は、SNMP v1、v2c、または v3 トラップを発生させて NNMi 管理サーバーに送信できることが必要です。

この章には、以下のトピックがあります。

- 354 ページの「イベント転送の設定」
- 358 ページの「リモート ビュー起動の設定」
- 361 ページの「統合をテストする」
- 364 ページの「イベント転送のトラブルシューティング」

イベント転送の設定

NNM 6.x/7.x 管理ステーションから NNMi 管理サーバーへのイベント転送を設定するには、以下の手順を順に行います。

- ステップ 1: NNM 6.x/7.x を、NNMi 管理サーバーにイベントを転送するように設定する
- Step 2: (任意) ノードレベルのフィルタリングを使用してイベント数をさらに削減する
- ステップ 3: NNM 6.x/7.x 管理ステーションを NNMi トポロジに追加する
- ステップ 4: (任意) 管理ステーション設定を保存する
- ステップ 5: NNM 6.x/7.x インシデント設定を NNMi コンソールで確認する

ステップ 1: NNM 6.x/7.x を、NNMi 管理サーバーにイベントを転送するように設定する

NNM 6.x/7.x 管理ステーションで、NNMi 管理サーバーに転送したい各々のイベントを設定します。これらのイベントのほとんどは、OpenView Enterprise の下にあります。興味深いイベントとしては、次のようなものがあります。

- OV_Node_Down (OV_Node_Up、Ov_Node_Unknown、その他)
- OV_APA_NODE_DOWN (OV_APA_NODE_Intermittent、その他)
- OV_Station_Critical (OV_Station_Normal、その他)
- OV_Error (OV_Warning、OV_Inform) システムの状態に関する情報
- OV_Message (OV_Popup_Message、その他)

転送が推奨される NNM 6.x/7.x イベントの全一覧については、NNMi コンソールで **[インシデントの設定]** フォームの **[リモート NNM 6.x/7.x イベント]** タブのイベント一覧をご覧ください。

推奨およびサポートされる手順: [イベント設定] ウィンドウを使用する

▶ XServer がない場合は、356 ページの「別の手順: trapd.conf を手順で編集する」を参照してください。

NNM 6.x/7.x イベントを設定して NNMi 管理サーバーに転送するには、以下の手順に従います。

- 1 コマンドプロンプトで、次のように入力します。

```
ovw
```

▶ または、xnmtrap をコマンドラインから実行して、手順 3 から続けます。

- 2 **[オプション]** > **[イベント設定]** をクリックします。
- 3 **[イベント設定]** ウィンドウで、最上部のウィンドウの **Openview** エンタープライズを選択し、一番下のウィンドウでイベント名をダブルクリックします。

▶ イベントを名前ですортするには、**[ビュー]** > **[ソート]** > **[イベント名]** をクリックします。

ベストプラクティス

- 4 NNMi 管理サーバーが転送されたイベントを受信するように指定します。

転送先リスト ファイルを作成してある場合は、このファイルへの完全パスを [転送先] フィールドに入力します。転送先リスト ファイルの書式については、355 ページの「任意：転送先リスト ファイル」を参照してください。

- **Windows:** [イベントの変更] ウィンドウの [転送] タブで、NNMi 管理サーバーのホスト名を [転送先] フィールドに入力します。

[追加] をクリックして、[OK] をクリックします。

- **UNIX:** [イベント設定] ウィンドウの下部の [転送先] フィールドで、NNMi 管理サーバーのホスト名を入力します。

[転送先] フィールドが表示されない場合は、ウィンドウの中央の [イベントの転送] オプションを選択します。

[追加] をクリックして、[OK] をクリックします。

- 5 NNMi 管理サーバーに転送するイベントをすべて設定するまで、手順 3 と手順 4 を繰り返します。

- 6 [ファイル]>[保存] をクリックします。

NNM 6.x/7.x はイベント設定の変更を保存して、新しいイベント設定を自動的に再読み込みします。

任意：転送先リスト ファイル

いくつかのイベントを同じ NNMi 管理サーバーのグループに転送したい場合は、転送先がリストされたファイルを作成します。

転送先リスト ファイルに推奨される場所は、以下のとおりです。

- **Windows:** %OV_CONF%\nnm8EventForwardDestinations.txt
- **UNIX:** \$OV_CONF/nnm8EventForwardDestinations.txt

転送先リスト ファイルは、次の書式を持つテキスト ファイルです。

- 各行は、1 つのノード名かコメント行です。
- コメント行の最初の文字は、# 文字です。

例：

```
# List of destination NNMi Management Servers to receive events.
# This list should be small enough that it does not overwhelm the NNMi operators.
# In general, the events should be node-related, so that Neighbor Views launched remotely
# from the NNMi management server are meaningful.
#
system1.domain.com
system2.comain.com
system3.domain.com
```

詳細については、trapd.conf マンページを参照してください。

転送先リスト ファイルを作成または変更した後で、次のコマンドを実行して再読み込みします。

```
xnmevents -event
```

別の手順 : trapd.conf を手順で編集する

XServer がない場合は、以下のファイルで各イベントの FORWARD フィールドを手動で編集できます。

- **Windows:** %OV_CONF%\%C%\trapd.conf
- **UNIX:** \$OV_CONF/C/trapd.conf

NNMi 管理サーバーを 1 つだけ指定するか、転送先リスト ファイルを指定します。例 :

```
EVENT OV_Message .1.3.6.1.4.1.11.2.17.1.0.58916872 "Application Alert Alarms" Normal
FORMAT $3
FORWARD NNM8Server.domain.com
```

FORWARD フィールドには、リモート マネージャのリストを含めることもできます。例 :

```
FORWARD %REMOTE_MANAGERS_LIST% /etc/opt/OV/share/conf/nnm8EventForwardDestinations.txt
```



trapd.conf ファイルを編集した後で、次のコマンドを実行して NNM にイベント設定を再読み込みさせます。

```
xnmevents -event
```

Step 2: (任意) ノード レベルのフィルタリングを使用してイベント数をさらに削減する

NNM 7.x では、特定のイベントにノード リストを設定できます。ノード リストがあるとき、NNM 7.x 管理ステーションに入ってくるイベントがイベント設定に一致するのは、イベント ソースがノード リスト内にある場合のみです。そのため、イベントが NNMi 管理サーバーに転送されるのは、イベント ソースがノード リスト内にある場合のみになります。ノード リストの典型的な使用事例は、重要ノードから特定のイベントのみを NNMi 管理サーバーへ転送することです。

NNM 7.x でノード リストを作成する場合の詳細は、sources_list マンページで ovtrapd.conf に関する情報を参照してください。

ステップ 3: NNM 6.x/7.x 管理ステーションを NNMi トポロジに追加する

NNM 6.x/7.x 管理ステーションを NNMi トポロジに加えて、NNM 6.x/7.x 管理ステーションが停止したときに NNMi 管理サーバーがインシデントを受信するようにします。

NNM 6.x/7.x 管理ステーションがまだ NNMi 「ノード」インベントリ ビューにない場合、この管理ステーションを検出シードに追加して、検出されるまでお待ちください。

ノードを検出シードに追加する方法については、NNMi ヘルプの「ネットワークの検出」を参照してください。

ステップ 4: (任意) 管理ステーション設定を保存する

新しい設定を保存するには、次のコマンドを実行します。

```
nnmconfigexport.ovpl -u <user> -p <password> -c station ¥  
-f <filename>
```

次のコマンドを実行すると、バックアップを後でインポートできます。

```
nnmconfigimport.ovpl -u <user> -p <password> -f <filename>
```

これらのコマンドについては、それぞれのリファレンス ページ、または UNIX のマンページを参照してください。

ステップ 5: NNM 6.x/7.x インシデント設定を NNMi コンソールで確認する

NNM 6.x/7.x から転送するイベントが (インシデントとして) NNMi で設定されていることを確認します。

NNMi のデフォルト インシデント設定を表示するには、以下の手順を実行します。

- 1 NNMi コンソールで、**[設定]** ワークスペースから **[インシデントの設定]** フォームを選択します。
- 2 **[リモート NNM 6.x/7.x イベント]** タブをクリックします。

このタブには、デフォルトのインシデント設定が表示されます。

このインシデント タイプの **[インシデント]** フォームには、**[NNM 6.x/7.x]** の **[原点]** が表示されます。

NNM 6.x/7.x 管理ステーションから転送するよう設定した 1 つ以上のイベントが **[リモート NNM 6.x/7.x イベント]** タブにリストされていない場合は、リストにないイベントそれぞれについて新しいインシデント設定を追加します。詳細については、NNMi ヘルプの「**インシデントの設定**」を参照してください。



NNM 6.x/7.x のインシデント カテゴリは、NNMi のそれとは異なります。NNM 6.x/7.x アラーム カテゴリと NNMi インシデント カテゴリとの間の関係の詳細は、**カテゴリのマッピング** を参照してください。

カテゴリのマッピング

NNM 6.x/7.x では、設定済みの アラーム カテゴリは以下のとおりです。

- エラー アラーム
- しきい値アラーム
- ステータス アラーム
- 設定アラーム
- アプリケーションアラート アラーム

NNMi では、設定済みのインシデント カテゴリは以下のとおりです。

- アカウンティング
- アプリケーション ステータス
- 設定
- 障害
- パフォーマンス
- セキュリティ
- ステータス

表 19 に、HP が提案する NNM 6.x/7.x アラーム カテゴリから NNMi インシデント カテゴリのマッピングを示します。

表 19 カテゴリ マッピングの提案

NNM 6.x/7.x アラーム カテゴリ	NNMi インシデント カテゴリ
エラー アラーム	アプリケーション ステータス
しきい値アラーム	パフォーマンス
ステータス アラーム	ステータス
設定アラーム	設定
アプリケーションアラートアラーム	アプリケーション ステータス

リモート ビュー起動の設定

NNMi 管理サーバーが NNM 6.x/7.x ビューを NNMi 管理サーバーで表示するように設定するには、以下の手順を順に行います。

- ステップ 1: Java プラグインのインストール
- ステップ 2: NNMi で NNM 6.x/7.x 管理ステーション エンティティを作成する
- ステップ 3: (オプション) その他の NNM 6.x/7.x ビューを設定する

ステップ 1: Java プラグインのインストール

NNMi では Java プラグインは必要ありませんが、NNM 6.x/7.x ビューでは特定バージョンの Java プラグインを使用する必要があります。Java プラグインのバージョンは、NNM のバージョンとオペレーティング システムによって異なります。

お使いの NNM の最新のリリース ノートを参照し、正しいバージョンの Java プラグインをダウンロードして、NNMi コンソール ユーザーが NNM の動的ビューを起動するときを使用するすべての Web ブラウザにインストールしてください。


ステップ 2: NNMi で NNM 6.x/7.x 管理ステーション エンティティを作成する

NNMi 管理サーバーを設定して、NNM 6.x/7.x 管理ステーションから受信したイベントを NNMi のエンティティに関連付けます。この設定により、NNMi 管理サーバーからの NNM 6.x/7.x 動的ビューの起動が可能になります。たとえば、NNMi で表示されている My7xSystem からノード停止を選択して、My7xSystem に戻る URL を起動できます。

▶ 大切なのは、NNM 6.x/7.x 管理ステーションにより送信されたイベントでエンコーディングされているアドレスに一致するプライマリ アドレスを使用することです。このアドレスがよくわからない場合は、カスタム インシデント属性の **RemoteSenderAddress** で NNM 6.x/7.x 管理ステーションから転送されたインシデントについて調べてください。

NNMi で NNM 6.x/7.x 管理ステーションを設定するには、以下の手順を実行します。

1 NNMi コンソールで、**[設定]** ワークスペースから **[管理ステーション (6.x/7.x)]** を選択します。

2  **[新規作成]** をクリックします。


3 **[管理ステーション]** フォームに、以下の情報を入力します。

- **[名前]**— この設定によって表される NNM 6.x/7.x 管理ステーションの識別名。
- **[NNM のバージョン]**— 設定している管理ステーションの NNM バージョン (6.x または 7.x)。
- **[IP アドレス]**— NNM 6.x/7.x 管理ステーションの IP アドレス。この IP アドレスは、NNMi 管理サーバーから到達可能である必要があります。IP アドレスは、以下のどちらかの方法で見つけることができます。
 - ovaddr を NNM 6.x/7.x 管理ステーションのコマンドラインで実行します。
 - NNM 6.x/7.x 管理ステーションから転送されたインシデントのカスタム インシデント属性 (CIA) を判別します。

▶ この方法が有効なのは、354 ページの「イベント転送の設定」で説明した手順をすでに済ませており、設定したイベントが NNM 6.x/7.x 管理ステーションで発生して NNMi 管理サーバーへ転送されている場合のみです。

- **[ovas ポート]**— 設定している NNM 7.x 管理ステーションの OpenView アプリケーションサーバー (ovas) のポート番号。NNM 7.x 管理ステーションでは、このポート番号は通常は 7510 です。

▶ ovas ポートは、Extended Topology アドオンを備えた NNM 6.x にも適用されます。

- **[Web サーバー ポート]**— 設定している NNM 6.x/7.x 管理ステーションの Web サーバーのポート番号。
 - Windows OS の NNM 6.x 管理ステーションでは、このポート番号は通常は 80 です。
 - UNIX OS の NNM 6.x 管理ステーションでは、このポート番号は通常は 3443 です。
 - あらゆる OS での NNM 7.x 管理ステーションでは、このポート番号は通常は 3443 です。
 - **[説明]**— 設定している NNM 6.x/7.x 管理ステーションの説明。
- 4  **[保存して閉じる]** をクリックします。
 - 5 NNMi コンソールからサインアウトします。
次に NNMi コンソールにサインインするときに、**[アクション]** メニューに NNM 6.x/7.x ビューを起動するための新しい項目が表示されます。

ステップ 3: (オプション) その他の NNM 6.x/7.x ビューを設定する

以下の URL は、既定では追加されていません。これらの URL はいずれも NNM 6.x/7.x 配備に追加できます。

選択を必要としない URL

- MIB ブラウザの URL 例:

`http://192.168.1.xxx:3443/OvCgi/OpenView5.exe?Action=Snmp&Host=speed2.cnd.hp.com`

- Report Presenter の URL 例:

`http://192.168.1.xxx:3443/OvCgi/nmRptPresenter.exe`

- Topology Summary の URL 例:

`http://192.168.1.xxx:7510/topology/summary`

- SNMP Data Presenter (MIB フォーム / テーブル contrib. graphs):

`http://192.168.1.xxx:3443/OvCgi/snmpviewer.exe?Context=Performance&sel=10.97.245.242`

- OV Launcher の URL 例:

`http://system.example.com:3443/OvCgi/ovlaunch.exe`

- jovw の URL 例:

(Web ベースの ovw は、ovw セッションを実行中であることが必要です。実行していないと、エラー ダイアログ "Cannot find an ovw on host ..." がセッション ID xxx:x をデフォルト名とするマップとともに表示されます。)

`http://system.example.com:3443/OvCgi/jovw.exe`



この URL は、次のようなオプションでのコンテキスト ノードとマップ名を使用できません。`jovw.exe?mapName=default&ObjectName=10.1.12.33`

- ovalarm の URL 例:

`http://system.example.com:3443/OvCgi/ovalarm.exe`

- トポロジ詳細を要求するフォーム (名前、IP アドレス、物理アドレス UUID、OvwId でノードを入力します):

`http://192.168.1.xxx:7510/topology/topoDetail`

選択を必要とする URL

- `ovwId` を使用しているノード詳細:

`http://192.168.1.xxx:7510/topology/topoDetail?objectType=ovwId&objectValue=3&Show+Details=Show+Details`

- `UUID` を使用しているノード詳細:

`http://192.168.1.xxx:7510/topology/topoDetail?objectType=uuid&objectValue=3dasfasdf&Show+Details=Show+Details`

統合をテストする

NNM 6.x/7.x と NNMi 管理サーバーとの統合を正しく設定したことを確認するには、以下の手順の 1 つ以上を必要に応じて行います。

- テスト 1: イベント転送の確認
- テスト 2: NNMi からの NNM 6.x/7.x 動的ビューの起動

テスト 1: イベント転送の確認

ネットワーク状態が正常な場合、一般に NNM 6.x/7.x がネットワーク イベントを受信します。NNM 6.x/7.x 管理ステーションは設定されたイベントを NNMi に転送し、NNMi ではそれをリモートで生成された 6.x/7.x インシデントとして表示します。テストを迅速に行うために、テスト イベントを生成したり、テスト ネットワークまたはテスト デバイス上に実際のネットワーク エラーを作成することができます。

NNM 6.x/7.x 管理ステーションから NNMi 管理サーバーへのイベント転送を確認するには、以下の手順に従います。

- 1 NNM 6.x/7.x 管理ステーションで、転送されるイベントの 1 つを発生する状況をつくります。

最も簡単な方法は、`sendMsg.ovpl` コマンドを NNM 6.x/7.x 管理ステーションで実行することです。このコマンドの実行方法については、363 ページの「[sendMsg.ovpl](#)」を参照してください。

もう 1 つの方法は、ネットワーク障害を NNM 6.x/7.x システム上で生成またはシミュレートすることです。362 ページの「[テスト用のインタフェース停止、インタフェース開始イベントの生成](#)」を参照してください。

- 2 生成されたイベントを NNMi コンソールで表示するには、[\[インシデントの参照\]](#) ワークスペースで [\[NNM 6.x/7.x イベント\]](#) を選択します。

NNM 6.x/7.x 管理ステーションから発生させたイベントがこのビューで見えるはずです。



また、NNMi 管理サーバーで `nnmdumpevents -t` を実行し、NNMi 管理サーバーが受信したイベントのリストを見ることもできます。

テスト用のインタフェース停止、インタフェース開始イベントの生成



以下のテスト手順では、NNM 6.x/7.x の設定を変更する必要があります。この手順は、本稼働しているネットワーク管理ステーションでは行わないでください。

- 1 NNM 7.x 管理ステーションで、**Extended Topology** が有効であれば、それを無効化します。

```
setupExtTopo.ovpl -disable
```

- 2 NNM 6.x/7.x 管理ステーションの ECS ユーザー インタフェースで、どの相関関係がアクティブかに注意し、すべての相関関係を無効化します。
- 3 ノード上の各 IP インタフェースについて、以下のコマンドを 1 回ずつ実行してインタフェース停止のテスト イベントを生成します。それによってノード停止イベントが発生する場合があります。

```
ovtopofix -S Down <IPADDR>
```

<IPADDR> は、NNM 6.x/7.x 管理ステーション トポロジのインタフェースの 1 つの IP アドレスです。使用する IP アドレスを決定するには、次のコマンドを実行します。

```
ovtopodump > topology.txt
```

topology.txt ファイルから、NODES という語を探し、NNM 6.x/7.x 管理ステーション用のエントリを見つけます。例：

NODES:

1516	IP	mplscexx.xxx.xx.com	Marginal	10.2.120.72
1516/1517	IP	mplscexx.xxx.xx.com	Normal	10.2.120.72
1516/2046	IP	mplscexx.xxx.xx.com	Critical	10.97.255.28
1516/2047	IP	mplscexx.xxx.xx.com	Critical	10.16.160.5
1516/2050	-	mplscexx.xxx.xx.com	Normal	-
1516/2051	-	mplscexx.xxx.xx.com	Normal	-
1516/2052	-	mplscexx.xxx.xx.com	Normal	-
1516/2053	-	mplscexx.xxx.xx.com	Normal	-
1516/5250	IP	mplscexx.xxx.xx.com	Critical	10.40.40.1
1516/5251	IP	mplscexx.xxx.xx.com	Critical	10.40.40.2

すべての IP インタフェースのステータスが Critical (危険域) になると、NNM はノードを停止として表示します。



また、NNM 6.x/7.x 管理ステーションのノード名またはトポロジ ID を ovtopofix コマンドの最後の引数として指定できます。その他のオプションについては、*ovtopofix* マニュアルを参照してください。



テストしているイベント (この場合は OV_IF_Up/OV_IF_Down で、それぞれ .1.3.6.1.4.1.11.2.17.1.0.58916866 と .1.3.6.1.4.1.11.2.17.1.0.58916867) が NNMi 管理サーバーに転送されるよう設定されていることを確認します。

- 4 イベント ブラウザをクリーンアップするため、各 IP インタフェースについて以下のコマンドを 1 回ずつ実行し、インタフェース開始イベントとノード開始イベントを生成します。

```
ovtopofix -S Up <IPADDR>
```

- 5 NNM 6.x/7.x 管理ステーションの ECS ユーザー インタフェースで、手順 2 で無効化した相関関係を再度有効化します。
- 6 手順 1 で Extended Topology を無効化した場合は、NNM 7.x 管理ステーションで再度有効化します。

```
setupExtTopo.ovpl
```

sendMsg.ovpl

sendMsg.ovpl コマンドを実行すると、OV_Message イベントを発生させることができます。例：

- **Windows:**

```
%OV_CONTRIB%\NNM\sendMsg\sendMsg.ovpl "" "Test from %COMPUTERNAME%"
```

- **UNIX:**

```
$OV_CONTRIB/NNM/sendMsg/sendMsg.ovpl "" "Test from `hostname` on `date`"
```

sendMsg.ovpl コマンドを実行するたびに、NNM 6.x/7.x では sendMsg.ovpl コマンドラインで追加したテキストを含む OV_Message イベントが発生します。例：

```
1183160690 6 Fri Jun 29 17:44:50 2007 <none> a Test from speed2 on  
Fri Jun 29 17:44:50 MDT 2007;1 17.1.0.58916872 0
```

このイベントは、NNM 6.x/7.x 管理ステーションの「すべてのアラーム」ブラウザで表示されます。

ベストプラクティス

新しいアラームを見分けやすくするには、sendMsg.ovpl コマンドを実行する前に**[すべてのアラーム]**ブラウザですべてのアラームを削除します。



デフォルトでは、OV_Message インシデントは NNMi では設定されていません。このテストを実行するには、NNM 6.x/7.x の OV_Message イベントを NNMi 管理サーバーに転送するよう設定する必要があり、OV_Message インシデントは、NNMi の**[インシデントの設定]**フォームで設定する必要があります。

NNM 6.x/7.x システムへのトラップをテストする

NNM 6.x/7.x がトラップを転送するよう設定すると、転送されているトラップを受信していることを確認できます。

以下の例のようなコマンドを使用すると、NNM 6.x/7.x 管理ステーションでトラップを手動で生成できます。

```
snmptrap -p 162 hostname "" "" 6 1234 "" .1.3.6.1.3.1.1.5.3 ¥  
octetstring "Test Trap"
```



この例では、SNMP_Link_Down トラップを生成します。転送されるように設定したトラップのイベント オブジェクト識別名を使用してください。

hostname は、NNM 6.x/7.x システムの名前です。詳細については、snmptrap マンページを参照してください。

テスト 2: NNMi からの NNM 6.x/7.x 動的ビューの起動

- 1 NNMi コンソールで、設定した NNM 6.x/7.x 管理ステーションを開きます。

[アクション] メニューに以下のアクションがあります。

- NNM 6.x/7.x ホーム ペース
- NNM 6.x/7.x ovw
- NNM 6.x/7.x MIB ブラウザ
- NNM 6.x/7.x ランチャー
- NNM 6.x/7.x アラーム



これらのアクションを使用できない場合、NNMi コンソールをサインアウトしてから、再度 NNMi コンソールにサインインします。

- 2 それぞれのビューを [アクション] メニューから開きます。

イベント転送のトラブルシューティング

表示されるはずの NNM 6.x/7.x イベントが [NNM 6.x/7.x イベント] インシデント ビューに表示されない場合は、以下の手順に従って問題を解決してください。

- 1 NNM 6.x/7.x 管理ステーションで、次のコマンドを実行します。

```
ovdumpevents -t -l <n>
```

ここで **<n>** は、イベント履歴をさかのぼる分時間を指定します。たとえば、*n* の値が 1 の場合、ovdumpevents コマンドは NNM 6.x/7.x 管理ステーションで最後の *n* 分間に発生したイベントを表示します。

- 2 予想したイベントが ovdumpevents 出力に含まれていない場合、そのイベントは発生しませんでした。この状況のトラブルシューティングについては、NNM 6.x/7.x のドキュメントを参照してください。
- 3 手順 1 を、予想したすべてのイベントが NNM 6.x/7.x 管理ステーションの ovdumpevents 出力に含まれるまで繰り返してください。
- 4 NNMi 管理サーバーで、次のコマンドを実行します。

```
nnmdumpevents -t -l <n>
```

ここで **<n>** は、イベント履歴をさかのぼる分時間を指定します。たとえば、*n* の値が 1 の場合、nnmdumpevents コマンドは NNMi 管理サーバーで最後の *n* 分間に発生したイベントを表示します。

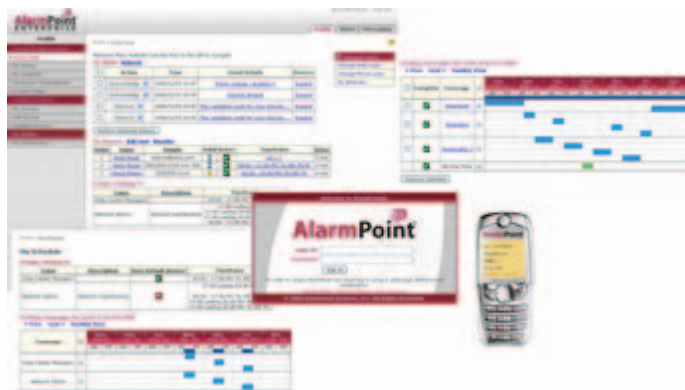
- 5 nnm rumpevents 出力に含まれるはずなのに含まれていない各イベントについて、そのイベントの設定を NNM 6.x/7.x 管理ステーションの **[Event Configurator]** ウィンドウで確認します。
 - **[イベントの転送]** オプションが選択されていることを確認します。
 - NNMi 管理サーバーの名前かまたは IP アドレスを、「**転送されるイベントの転送先**」リストで確認します。詳細については、354 ページの「**ステップ 1: NNM 6.x/7.x を、NNMi 管理サーバーにイベントを転送するように設定する**」を参照してください。
- 6 手順 5 を、予想したすべてのイベントが NNMi 管理サーバーの nnm rumpevents 出力に含まれるまで繰り返してください。
- 7 NNMi コンソールで、**[NNM 6.x/7.x イベント]** インシデント ビューを調べます。結果が予想と異なる場合は、**[インシデントの設定]** フォームの **[リモート NNM 6.x/7.x イベント]** タブでインシデント設定を確認してください。

NNMi との統合

この項では以下の章について説明します。

- AlarmPoint
- CiscoWorks LAN Management Solution
- Clarus Systems ClarusIPC Plus⁺
- HP Asset Manager
- HP Business Availability Center My BSM
- HP Business Service Management トポロジ
- HP Network Automation
- HP ProCurve Manager Plus
- HP Systems Insight Manager
- HP Universal CMDB
- nGenius Performance Manager
- NNMi ノースバウンドインタフェース
- HP Operations Manager
- Netcool ソフトウェア用 HP NNMi 統合モジュール

AlarmPoint



AlarmPoint Systems AlarmPoint 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。

AlarmPoint は、自動化エンジンまたは **HP Network Node Manager i Software** 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なるように、統合できます。NNMi と統合すると、注意が必要なイベントを検出したときに、**AlarmPoint** から、適切な担当者、ベンダー、カスタマに対して、電話をかける、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できるようになります。

また、**AlarmPoint** 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。**AlarmPoint** 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 **AlarmPoint Enterprise** ライセンスに含まれる **AlarmPoint Mobile Gateway** は、**AlarmPoint** 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。**AlarmPoint Mobile Gateway** 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、ダッシュボードをモニタリングし、洗練されたレポートを生成できます。

AlarmPoint Express は、NNMi のバンドル パッケージに含まれています。拡張機能セットおよび **AlarmPoint Mobile Gateway** と一緒に版の異なる **AlarmPoint** ソフトウェアを購入する場合は、詳細については、HP 販売員にお尋ねになるか、sales@alarmpoint.com 宛てにメールでお問い合わせください。

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-AlarmPoint 統合](#)
- [HP NNMi-AlarmPoint Mobile Gateway 統合](#)

HP NNMi-AlarmPoint 統合

HP NNMi-AlarmPoint 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 AlarmPoint 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-AlarmPoint 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 AlarmPoint 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、AlarmPoint 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、AlarmPoint、AlarmPoint Mobile Gateway、または AlarmPoint と AlarmPoint Mobile Gateway の両方と統合できます。

値

HP NNMi-AlarmPoint 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、AlarmPoint 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づき、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。

処理中には、AlarmPoint 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、AlarmPoint 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。

AlarmPoint 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、AlarmPoint 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。



AlarmPoint の機能限定版である AlarmPoint Express は、NNMi の特定バージョンで使用できます。AlarmPoint Express 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。AlarmPoint Express は、AlarmPoint 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。AlarmPoint Express 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。

サポートされるバージョン

このセクションの情報は、以下の製品バージョンに当てはまります。

- AlarmPoint バージョン 4.0 以降
- AlarmPoint Java Client バージョン 4.0 以降
- NNMi バージョン 8.10 以降 (NNMi 統合イネーブルメント ライセンスが付属している場合)



NNMi 統合実施可能ライセンスは、AlarmPoint Express との統合では必要ありません。

ドキュメント

HP NNMi-AlarmPoint 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。

AlarmPoint のドキュメントスイートでは、AlarmPoint 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 AlarmPoint Customer Support サイトからダウンロードできます。

<https://connect.alarmpoint.com>



『AlarmPoint Express for HP NNMi Quick Start Guide』では、AlarmPoint の特徴について概要が説明されています。このガイドでは、HP NNMi-AlarmPoint Express 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ます。

HP NNMi-AlarmPoint 統合の有効化

NNMi との両方の AlarmPoint 統合を実装する場合は、まず HP NNMi-AlarmPoint 統合を有効にし、それから HP NNMi-AlarmPoint Mobile Gateway 統合を有効にすることを推奨します。

AlarmPoint for NNMi 統合のインストール方法と設定方法の手順概要は、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 AlarmPoint Web サーバーと AlarmPoint 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。AlarmPoint Web サーバーに、NNMi 用の AlarmPoint サブスクリプション パネルをインストールします。
- 5 AlarmPoint Developer IDE を使って、NNMi 用の AlarmPoint アクション スクリプトをインストールします。
- 6 AlarmPoint 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 AlarmPoint 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 for NNMi を設定します。

- 9 AlarmPoint スクリプトをトリガーする、NNMi インシデント タイプを設定します。
- 10 統合によって、AlarmPoint 通知に NNMi インシデント パラメータが挿入されることと、AlarmPoint 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-AlarmPoint 統合の使用法

NNMi と AlarmPoint 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 AlarmPoint に送信し、AlarmPoint はその情報を適切な受信者に通知します。
- 4 受信者は、表 20 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 コールを介して受信者による受諾、注釈付加、または優先度変更があると、NNMi が更新されます。

表 20 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、問題が実際に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-AlarmPoint 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。

AlarmPoint 配備の削除に関する詳細については、『AlarmPoint 対応 HP Network Node Manager i-series 統合ガイド』を参照してください。

HP NNMi-AlarmPoint 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-AlarmPoint Mobile Gateway 統合

HP NNMi-AlarmPoint Mobile Gateway 統合について

NNMi 環境に AlarmPoint Mobile Gateway を統合することにより、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、AlarmPoint、AlarmPoint Mobile Gateway、または AlarmPoint と AlarmPoint Mobile Gateway の両方と統合できます。

値

HP NNMi-AlarmPoint Mobile Gateway 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

サポートされるバージョン

このセクションの情報は、以下の製品バージョンに当てはまります。

- AlarmPoint Mobile Gateway バージョン 4.0 以降
- AlarmPoint Integration Agent バージョン 4.0 以降
- NNMi バージョン 8.10 以降 (NNMi 統合イネーブルメント ライセンスが付属している場合)



NNMi 統合実施可能ライセンスは、AlarmPoint Express で実行されている AlarmPoint Mobile Gateway との統合では必要ありません。

ドキュメント

HP NNMi-AlarmPoint Mobile Gateway 統合については、この統合に付属の『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。

AlarmPoint のドキュメント スイートでは、AlarmPoint 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 AlarmPoint Customer Support サイトからダウンロードできます。

<https://connect.alarmpoint.com>

HP NNMi-AlarmPoint Mobile Gateway 統合の有効化

NNMi との両方の AlarmPoint 統合を実装する場合は、まず HP NNMi-AlarmPoint 統合を有効にし、それから HP NNMi-AlarmPoint Mobile Gateway 統合を有効にすることを推奨します。371 ページの「HP NNMi-AlarmPoint 統合の有効化」を参照してください。

NNMi 統合用の AlarmPoint Mobile Gateway をインストールおよび設定する手順の概要を以下に示します。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 をバージョン 8.1x からバージョン 8.13 にアップグレードできます。AlarmPoint 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 AlarmPoint Integration Agent を AlarmPoint サーバーにインストールします。
- 2 Web Service Library を AlarmPoint Integration Agent と Web サーバーにインストールします。
- 3 AlarmPoint Mobile Gateway を AlarmPoint 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 AlarmPoint で、イベント ドメイン (HP NNMi-AlarmPoint 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 AlarmPoint Mobile Gateway と NNMi の間のやり取りを確認します。

HP NNMi-AlarmPoint Mobile Gateway 統合の使用法

HP NNMi-AlarmPoint Mobile Gateway 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 (AlarmPoint Mobile Gateway 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『*AlarmPoint Mobile Gateway Guide*』を参照してください。

HP NNMi–AlarmPoint Mobile Gateway 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。

AlarmPoint Mobile Gateway 配備の削除に関する詳細については、『**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 Mobile Gateway 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。

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、モニタリング、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 の統合
- HP NNMi-CiscoWorks LMS 統合の有効化
- HP NNMi-CiscoWorks LMS 統合の使用法
- HP NNMi-CiscoWorks LMS の統合設定の変更
- 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 の統合

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。

サポートされるバージョン

この章の情報は、以下の製品バージョンに当てはまります。

- CiscoWorks LMS バージョン 3.1 以降
- NNMi バージョン 8.13 以降

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 対応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。

- CiscoWorks LMS バージョン 3.1:
http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_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/ciscoverks_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 ([統合モジュール設定] > [CiscoWorks LMS]) を開きます。
- 2 [統合を有効化] 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、381 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、382 ページの「CiscoWorks LMS サーバー接続」を参照してください。
- 5 フォームの下端の [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。例：

```
nnmloadmib.ovpl -load cpqghost.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 の統合設定の変更

- 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、381 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 フォームの上端の [統合を有効化] 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。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 ([統合モジュール設定] > [CiscoWorks LMS]) を開きます。
- 2 フォームの上端の [統合を有効化] 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。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、379 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、[統合モジュール設定] ワークスペースから利用できます。



[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 21 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 21 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。 <ul style="list-style-type: none">• HTTPS を使用するように NNMi コンソールが設定されている場合は、[NNMi SSL 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 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 <code>nnmofficialfqdn.ovpl -t</code> 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。 <ul style="list-style-type: none">• Windows: %NnmDataDir%\conf\%nm\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 21 NNMi 管理サーバー情報 (続き)

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。

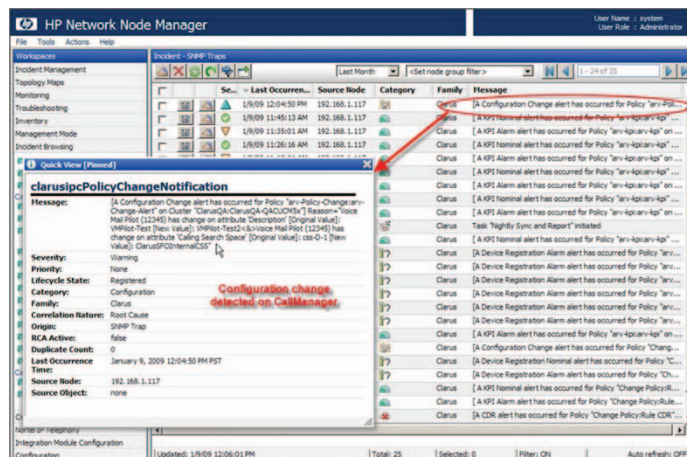
CiscoWorks LMS サーバー接続

表 22 に、CiscoWorks LMS サーバーに接続して V 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 22 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。 <ul style="list-style-type: none"> • HTTPS を使用するように CiscoWorks LMS を設定する場合は、[CiscoWorks LMS SSL 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 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 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

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トイングを行い、IP テレフォニ デバイス管理を一元管理します。

サポートされるバージョン

このセクションの情報は、以下の製品バージョンに当てはまります。

- ClarusIPC Plus⁺ バージョン 2.6.1 以降
- NNMi バージョン 8.10 以降 (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

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、各種ポリシー、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。

サポートされるバージョン

このセクションの情報は、以下の製品バージョンに当てはまります。

- ClarusIPC Plus+ バージョン 2.6.1 以降
- NNMi バージョン 8.11 以降 (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 ライセンスを取得している場合)



NNMi バージョン 8.11 は、NNMi バージョン 8.10 に対するパッチです。

- NNM iSPI for IP Telephony バージョン 8.11 以降 (サポート対象のオペレーティング システム上のもの)



NNM iSPI for IP Telephony バージョン 8.11 は、NNM iSPI for IP Telephony バージョン 8.10 に対するパッチです。

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-suite 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。

サポートされるバージョン

この章の情報は、以下の製品バージョンに当てはまります。

- Asset Manager バージョン 5.2x と HP Connect-It バージョン 4.1x
- NNMi バージョン 9.00 以降

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

FHP 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 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ーフェイスを使用して、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、そのインターフェイスで、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。

サポートされるバージョン

この章の情報は、以下の製品バージョンに当てはまります。

- BAC バージョン 7.54、8.03 または 8.04



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 バージョン 8.11 以降
- オプション。NNM iSPI for Performance バージョン 8.1x

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 23 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。393 ページの表 24 にこのモジュールの説明が記載されています。

表 23 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 24 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 設定] フォームを開きます ([統合モジュール設定] > [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] をクリックします。
 - d [HP NNMi-HP BAC My BSM 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、[次へ] をクリックします。これらのフィールドの詳細は、400 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 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 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 管理者インターフェイスで、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、396 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] > [ドキュメントライブラリ] > 「NNMi Elsewhere と URL の統合」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、空の要素 `<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
<code>nnmi-portlet</code>	NNMi URL を表示する <code>iframe</code> 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。
<code>nnmi-auth</code>	NNM iSPI for Performance へのシングルサインオンを管理する <code>iframe</code> 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。
<code>ispiperf-portlet</code>	NNM iSPI for Performance レポートの URL を表示する <code>iframe</code> 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 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/nm/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 におけるシングルサインオンの設定方法については、109 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](#)」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。
 - 2 398 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。
- 399 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 管理者インターフェイスで、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 管理者インターフェイスで、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 25 は、[HP NNMi—HP BAC My BSM 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 25 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 管理者インターフェイスに表示されます。
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。これは、事前入力済みのフィールドで、現在の NNMi コンソール セッションの NNMi 管理に接続するホスト名とポート番号です。 <ul style="list-style-type: none">• 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。 <ul style="list-style-type: none">• 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 NNMi コンソール セッションで NNM iSPI for Performance サーバーに接続するホスト名とポート番号です。 <ul style="list-style-type: none">• 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 25 モジュールの設定情報 (続き)

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	<p>[iSPI for Performance ポートレットを無効にする] 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。</p> <p>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。</p>

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
- 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
- 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 トポロジ統合は、NNMi トポロジを使用して BSM 運用データベース (ODB) にデータを入力します。BSM は、設定項目 (CI) として 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。

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。

サポートされるバージョン

この章の情報は、以下の製品バージョンに当てはまります。

- BSM バージョン 9.00 以降
- NNMi バージョン 9.00 以降

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

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 NNMi コンソールで、[HP NNMi-HP BSM 統合設定] フォームを開きます ([統合モジュール設定] > [HP BSM])。
- 2 [統合を有効化] 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、407 ページの「NNMi 管理サーバー接続」を参照してください。
- 4 BSM 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、407 ページの「BSM サーバー接続」を参照してください。
- 5 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、408 ページの「BSM トポロジフィルタ」を参照してください。
- 6 フォームの下端の [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

HP NNMi-HP BSM トポロジ統合により、BSM ODB に以下の CI タイプが入力されます。

- インフラストラクチャ エlement > ノード
NNMi トポロジのノード。408 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。
- インフラストラクチャ エlement > ネットワーク エンティティ > 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。
- インフラストラクチャ エlement > ネットワーク エンティティ > IpSubnet
NNMi トポロジのすべてのサブネット。
- インフラストラクチャ エlement > ネットワーク エンティティ > Layer2Connection
統合が ノード CI として BSM に入力する接続エンドを少なくとも 2 つ持つ NNMi Layer 2 接続。

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 ODB 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 統合設定] フォームを開きます ([統合モジュール設定] > [HP BSM])。
- 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、406 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 フォームの上端の [統合を有効化] 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。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 統合設定]** フォームを開きます (**[統合モジュール設定]** > **[HP BSM]**)。
- 2 フォームの上端の **[統合を有効化]** 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。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

ODB 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。

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 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、**[統合モジュール設定]** ワークスペースから利用できます。

▶ **[HP NNMi-HP BSM トポロジ統合設定]** 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。

- 407 ページの「**NNMi 管理サーバー接続**」
- 407 ページの「**BSM サーバー接続**」
- 408 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 26 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 26 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。 <ul style="list-style-type: none">• HTTPS を使用するように NNMi コンソールが設定されている場合は、[NNMi SSL 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 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 <code>nnmofficialfqdn.ovpl -t</code> 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。 <ul style="list-style-type: none">• Windows: %NnmDataDir%\conf\%nm%\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 サーバー接続

表 27 に、BSM ページを開く BSM サーバーへの接続パラメータをリストします。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 27 BSM サーバー情報

BSM 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。 <ul style="list-style-type: none">• BSM が HTTPS を使用するように設定されている場合は、[BSM SSL 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 を使用するように設定されている場合は、[BSM SSL 有効化] チェック ボックスをオフにします。
BSM ホスト	BSM サーバーの完全修飾ドメイン名。

表 27 BSM サーバー情報 (続き)

BSM サーバー パラメータ	説明
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 ユーザー インタフェースに接続するためのユーザー名。このユーザーには管理者権限が与えられている必要があります。
BSM パスワード	指定した BSM ユーザーのパスワード。

BSM トポロジ フィルタ

デフォルトでは、HP NNMi-HP BSM トポロジ統合は、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を BSM で管理します。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 2 つの例は、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 28 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 28 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	<p>BSM に挿入する一連のプライマリ ノードを含む NNMi ノード グループ。統合により、このノード グループのすべてのノードに関する情報が ODB に入力されます。</p> <p>NNMi で [ノード グループ] フォームの [名前] フィールドに記述されているとおりに (引用符または追加文字は含みません) ノード グループの名前を入力します。</p> <p>トポロジ フィルタ 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、NNMi トポロジ内のすべてのノードとインタフェースを ODB に入力します。この場合、統合は、[追加接続ノード グループ] フィールドの値を無視します。</p>
追加接続ノード グループ	<p>BSM 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 ODB に入力されます。</p> <p>NNMi で [ノード グループ] フォームの [名前] フィールドに記述されているとおりに (引用符または追加文字は含みません) ノード グループの名前を入力します。</p> <p>トポロジ フィルタ 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。</p> <p>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。</p> <p>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 統合は、NNMi トポロジ内のすべてのノードとインタフェースを ODB に入力します。この場合、統合は、[追加接続ノード グループ] フィールドの値を無視します。</p>

HP 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。

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
- 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

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。

この統合は、NNMi が管理するデバイスの自動設定や管理対象デバイスへのアクセス情報による NNMi 設定の更新を行います。

既存の NNMi 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
- (NNM iSPI NET) 不整合の速度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。

サポートされるバージョン

この章の情報は、以下の製品バージョンに当てはまります。

- NA バージョン 7.50.02 と NA 7.50.02 サービス パックおよび最新バージョンのコネクタ
- NA バージョン 7.60.01 と NA 7.60.01 サービス パック、ホットフィックス 107743、および最新バージョンのコネクタ
- NNMi バージョン 9.00 以降 (Windows、Linux、または Solaris オペレーティング システムのみ)

以前のバージョンの NNMi での HP NNMi-HP NA 統合の設定については、NA とともに提供されたドキュメントを参照してください。

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、NA と通信するように NNMi を設定する方法と、NNMi コンソールから統合を使用する方法を説明します。

NA 製品メディアに含まれている *HP Network Automation NNM Integration User's Guide (HP Network Automation NNM 統合ユーザー ガイド)* には、NA ユーザー インタフェースから統合を使用する方法が説明されています。

HP NNMi-HP NA 統合の有効化

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。



2009 年 1 月版の NA 7.50 向け *HP Network Automation NNM Integration User's Guide (HP Network Automation NNM 統合ユーザー ガイド)* には、NNMi バージョン 8.10 との統合の設定方法が説明されています。NNMi バージョン 8.11 以降については、*HP Network Automation NNM Integration User's Guide (HP Network Automation NNM 統合ユーザー ガイド)* の指示よりもこの章の指示を優先してください。

- 1 NNMi 管理サーバーで、最新の NA 統合パッチに含まれる NNMi コネクタをインストールします。
 - NNMi 管理サーバーとは異なるコンピュータで NA サーバーを実行している場合は、以下のいずれかのコネクタ インストーラを実行します。NA サーバーのオペレーティング システムに対応するコネクタを選択します。
 - na_nnm_connector_windows.exe
 - na_nnm_connector_solaris.bin
 - na_nnm_connector_linux.bin
 - NA サーバーと NNMi 管理サーバーが同じコンピュータで実行している場合は、以下のいずれかのコネクタ インストーラを実行します。NA サーバーのオペレーティング システムに対応するコネクタを選択します。
 - na_nnm_coresidency_windows.exe
 - na_nnm_coresidency_solaris.bin
 - na_nnm_coresidency_linux.bin

コネクタ インストーラによって **NNMi** 管理サーバーが検出され、**NNMi** 管理サーバーに **NA** と通信するためのコンポーネントがインストールされます。また、**NA** データベースに **NNMi** トポロジもインポートされます。



コネクタ インストーラで **NNMi HTTP** ポートの指定を求められたら、**NNMi** コンソールに接続するポートを入力します。このポートは **NNMi** のインストール中に設定されており、以下のファイルで指定されています。

- **Windows:** %NnmDataDir%\conf\%nm%\props\nms-local.properties
- **UNIX:** \$NnmDataDir/conf/nnm/props/nms-local.properties

以下のようにしてポートの値を調べます。

- **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。

2 **NNMi** 管理サーバーで、**NNMi** と **NA** の接続を設定します。

- NNMi** コンソールで、**[HP NNMi-HP NA 統合設定]** フォームを開きます (**[統合モジュール設定]** > **[HP NA]**)。
- [統合を有効化]** 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。
- 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、423 ページの「**NNMi 管理サーバー接続**」を参照してください。
- 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、424 ページの「**NA サーバー接続**」を参照してください。



統合には、**NA Web** サービスへの **HTTP** 接続が必要であるため、**[HP NA SSL 有効]** チェック ボックスをオフのままにします。

- (**NNM iSPI NET**) **[HP NA 接続チェック間隔]** フィールドに値を入力します。このフィールドの詳細については、424 ページの「**統合動作**」を参照してください。
- フォームの下端の **[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。メッセージに **NA** サーバーへの接続に関する問題が示されている場合は、**[HP NNMi-HP NA 統合設定]** フォームをもう一度開いて (またはメッセージ ウィンドウで **ALT+ 左矢印** を押して)、エラー メッセージのテキストが示すとおり **NA** サーバーへの接続の値を調整します。

3 (**NNM iSPI NET**) 統合が、不整合の速度や全二重設定の接続を検出するようにするには、**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** サーバーで以下の手順を実行します。

- 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。

NNMi コネクタのトポロジ インポート プロセスによって **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、NA インベントリのデバイスと通信するための各パスワードのパスワードルールを作成します。
 - 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。
 - 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**])。
 - 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 トポロジからインポートされた各デバイスに、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。
- 4 オプション。NA サーバーで、NA と NNMi の接続を設定します。
- a NA 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**])。
[**NNM ホスト**]、[**NNM HTTP ポート**]、[**NNM ユーザー名**]、および [**NNM パスワード**] フィールドは、NNMi コネクタのインストール中に提供された情報が事前入力されています。
 - b サービス停止イベントを生成するデバイス タスクを選択して設定および適合チェック障害の応答を選択し、サービス停止の動作を設定します。
詳細については、418 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。
 - c SNMP コミュニティ文字列の伝播の動作を選択します。
詳細については、419 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。
 - d ページの下にある [**保存**] をクリックします。

HP NNMi-HP NA 統合の使用

HP NNMi-HP NA 統合は、NNMi と NA の両方に機能を追加します。

統合が提供する NNMi 機能

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。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。NA ウィンドウを表示するには、NA ユーザーの資格情報を入力する必要があります。

HP NNMi-HP NA 統合を有効にすると、NNMi コンソールに以下のアクションが追加されます。

- [**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、417 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、417 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。
- **(NNM iSPI NET) [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、417 ページの「**不整合な状態のレイヤー 2 接続の特定 (NNM iSPI NET)**」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。その周期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 29 には、変更されたインシデントがリストされています。

表 29 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

表 29 NA Diagnostics で設定された NNMi インシデント (続き)

NNMi インシデント	NA Diagnostic
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 29 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、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、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 (NNM iSPI NET)

NNMi 管理サーバーに NNM iSPI NET ライセンス キーがインストールされており、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 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。



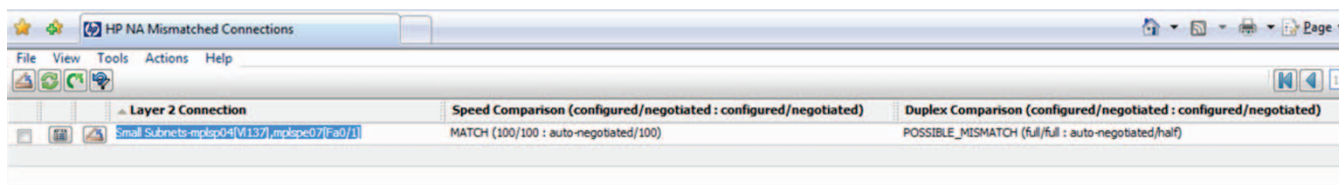
NNMi は、NA インベントリにレイヤー 2 接続を形成するインタフェース用の MAC アドレスが含まれている場合にのみ、不整合分析を実行します。NA インタフェースのレコードに有効な MAC アドレスが含まれていない場合は、NA のトポロジ データ収集診断を実行して、MAC アドレス フィールドを更新します。

[アクション]>[不整合の接続を表示] コマンドは、図 20 に示されるように、速度や全二重の不整合が含まれると NNMi が考えるレイヤー 2 接続のテーブルを表示します。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 NNMi の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、または両方の値が潜在的に競合しており、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ことを示します。

[HP NNMi-HP NA 統合設定] フォームの HP NA 接続チェック周期パラメータは、接続クエリの頻度を指定します。

図 20 不整合接続テーブルの例



Layer 2 Connection	Speed Comparison (configured/negotiated : configured/negotiated)	Duplex Comparison (configured/negotiated : configured/negotiated)
Small_Subnets-mpls04[V137],mplspc07[Fa0/1]	MATCH (100/100 : auto-negotiated/100)	POSSIBLE_MISMATCH (full/full : auto-negotiated/half)

統合により提供される NA 機能

HP NNMi-HP NA 統合によって、以下の機能について、NA から NNMi への通信 (NNMi Web サービスの呼び出しによる) を行えるようになります。

- デバイス設定中のネットワーク管理の無効化
- デバイス コミュニティ文字列の変更の伝播

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。以下のタスクのいずれかまたはすべてを選択できます。

- コマンド スクリプトの実行
- 診断の実行
- デバイス ソフトウェアの更新
- パスワードの配布
- ACL の削除

- Syslog の設定
- デバイスの再起動
- 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



タスクを 1 つも選択しないと、この機能を無効にできます。

デバイス設定が正しく行われなかった場合、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でない場合に、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。

- デバイスにアクセスするために NA が使用する SNMP コミュニティ文字列が変更した場合、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 インベントリに追加された場合、NA は、デバイスの管理に使用するコミュニティ文字列を NNMi に通知します。

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 インベントリへの NNMi 8.10 デバイスのインポート

NA インベントリは、NNMi トポロジが変更しても自動的に更新されません。NNMi トポロジに新しいデバイスを追加した後、それらのデバイスを NA インベントリにインポートします。



定期的にインポート コマンドを実行し、NA インベントリを最新の状態に維持します。

NA インベントリに NNMi デバイス情報をインポートするには、以下の手順を実行します。

- 1 NNMi 管理サーバーで、NA のルート ディレクトリに変更します。デフォルトは以下の場所です。
 - *Windows*: C:\NA
 - *UNIX*: /opt/NA
- 2 以下のコマンドを実行します。
 - *Windows*: nnmimport.bat
 - *UNIX*: nnmimport.sh

HP NNMi-HP NA 統合の変更

- 1 NNMi コンソールで、[HP NNMi-HP NA 統合設定] フォームを開きます ([統合モジュール設定] > [HP NA])。
- 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、423 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。
- 3 フォームの上端の [統合を有効化] 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。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 統合設定] フォームを開きます ([統合モジュール設定] > [HP NA])。
- 2 フォームの上端の [統合を有効化] 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。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

▶ 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、423 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 統合が正しく機能したことがない場合は、以下のファイルが存在するかどうかを確認します。

- **Windows:** C:\NA\annmimport.csv
- **UNIX:** /opt/NA/annmimport.csv

annmimport.csv ファイルが存在しない場合は、413 ページの**手順 1**に記載されているとおりに **NNMi** コネクタをアンインストールし、再インストールを行います。

- 2 **NNMi** コンソールで、**[HP NNMi-HP NA 統合設定]** フォームを開きます (**[統合モジュール設定]** > **[HP NA]**)。

このフォームのフィールドの詳細は、423 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。

- 3 統合のステータスを確認するには、**[HP NNMi-HP NA 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)。

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 4** を継続します。

- 4 **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 NA ユーザー**の資格情報を使用して、**[HP NNMi-HP NA 統合設定]** フォームから **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** 管理者にログイン資格情報を問い合わせてください。

- 5 **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 統合設定]** フォームの値に関係する場合：

- **[HP NA SSL 有効化]** 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、**HP NA ホスト**の値です。
- **<naport>** は、**HP 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 6**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。

- 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 2** 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>/nmm/

以下のように、変数が **[HP NNMi-HP NA 統合設定]** フォームの値に関係する場合：

- **[HP NNMi SSL 有効化]** チェック ボックスがオンの場合、<protocol> は https です。
 - **[HP NNMi SSL 有効化]** チェック ボックスがオフの場合、<protocol> は http です。
 - <NNMiServer> は、**HP NNMi ホスト**の値です。
 - <port> は、**HP 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が、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続けます。

「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 **[HP NNMi ユーザー]** と **[HP NNMi パスワード]** の値を確認します。

- **[HP NNMi-HP NA 統合設定]** フォームにリストされている **[HP NNMi ユーザー]** に管理者ロールがあり、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、**[HP NNMi-HP NA 統合設定]** フォームに対応するパスワードを再入力します。
- **[HP NNMi-HP NA 統合設定]** フォームにリストされている **[HP NNMi ユーザー]** に Web サービス クライアント ロールがある場合は、NNMi 管理者に連絡し、**[HP NNMi ユーザー]** および **[HP 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** で使用して正常に接続できた値で、**[HP NNMi-HP NA 統合設定]** フォームを更新します。

詳細については、423 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 フォームの下端の **[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。

- 10 415 ページの「**HP NNMi-HP NA 統合の使用**」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。

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] フォームには、NNMi と NA 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、[統合モジュール設定] ワークスペースから利用できます。



[HP NNMi-HP NA 統合設定] フォームには、管理者ロールを持つ NNMi ユーザーのみがアクセスできます。

[HP NNMi-HP NA 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。

- 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 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 30 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 30 NNMi 管理サーバー情報

フィールド	説明
HP NNMi SSL 有効化	接続プロトコル指定。 <ul style="list-style-type: none">• NNMi コンソールが HTTPS を使用するよう設定されている場合は、[HP NNMi SSL 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。• NNMi コンソールが HTTP を使用するよう設定されている場合は、[HP NNMi SSL 有効化] チェックボックスをオフにします。
HP 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 <code>nnmofficialfqdn.ovpl -t</code> 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。
HP 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。 <ul style="list-style-type: none">• Windows: %NnmDataDir%\%conf%\nnm\props\nms-local.properties• UNIX: \$NnmDataDir/conf/nnm/props/nms-local.properties SSL 以外の接続では、 <code>jboss.http.port</code> 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、 <code>jboss.https.port</code> の値を使用します。これはデフォルトでは 443 です。

表 30 NNMi 管理サーバー情報 (続き)

フィールド	説明
HP 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。
HP 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 31 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 31 NA サーバー情報

HP NA サーバー パラメータ	説明
HP NA SSL 有効化	NA Web サービスに接続するための接続プロトコルの指定。 統合には、NA Web サービスへの HTTP 接続が必要であるため、[HP NA SSL 有効] チェック ボックスをオフのままにします。
HP 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。
HP 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。 <ul style="list-style-type: none"> 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
HP 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。
HP 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

HP NA 接続チェック周期 パラメータは、417 ページの「不整合な状態のレイヤー 2 接続の特定 (NNM iSPI NET)」に説明されているように、NNMi トポロジ内のすべてのレイヤー 2 接続のインタフェース データを NNMi が確認する周期を指定します。接続チェックのデフォルトの周期は 24 時間です。



接続チェック機能には、NNM iSPI NET ライセンスが必要です。NNMi 管理サーバーに NNM iSPI NET ライセンス キーがインストールされていない場合、[HP NA 接続チェック周期] フィールドは無効になります。

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、およびモニタリング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、モニタリング、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モニタリング機能

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-suite Software を含めることにより、PCM Plus を使用して ProCurve デバイスをモニタリング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。

サポートされるバージョン

この章の情報は、以下の製品バージョンに当てはまります。

- PCM Plus バージョン 3.10 (不具合 53323 のホットフィックスを含む)
- NNMi バージョン 9.00:

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 つのインストールを NNMi バージョン 8.1x または NNM バージョン 7.x と統合することができますが、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。

サポートされるバージョン

この章の情報は、以下の製品バージョンに当てはまります。

- HP RAMS バージョン 9.00 以降
- NNMi バージョン 9.00 以降 (NNMi Advanced ライセンスを取得している場合)

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 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。

サポートされるバージョン

この章の情報は、以下の製品バージョンに当てはまります。

- SIM バージョン 5.30 以降
- NNMi バージョン 8.13 以降

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 対応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 (**[統合モジュール設定]** > **[HP SIM]**)。
- 2 **[統合を有効化]** 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、434 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、434 ページの「SIM サーバー接続」を参照してください。
- 5 フォームの下端の **[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\SystemInsightManager
```
 - *UNIX*:


```
$NNM_SNMP_MIBS/Vendor/Hewlett-Packard/SystemInsightManager
```
- 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。例：


```
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、`SystemInsightManager` 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、433 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 フォームの上端の [統合を有効化] 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。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 ([統合モジュール設定] > [HP SIM])。
- 2 フォームの上端の [統合を有効化] 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。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、431 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、**[統合モジュール設定]** ワークスペースから利用できます。



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 32 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 32 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。 <ul style="list-style-type: none">• HTTPS を使用するように NNMi コンソールが設定されている場合は、[NNMi SSL 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 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 <code>nnmofficialfqdn.ovpl -t</code> 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。 <ul style="list-style-type: none">• <i>Windows:</i> %NnmDataDir%\%conf%\nnm\props\nms-local.properties• <i>UNIX:</i> \$NnmDataDir/conf/nnm/props/nms-local.properties SSL 以外の接続では、 <code>jboss.http.port</code> 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、 <code>jboss.https.port</code> 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 33 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 33 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。 <ul style="list-style-type: none">• SIM が HTTPS を使用するように設定されている場合は、[HP SIM SSL 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 を使用するように設定されている場合は、[HP SIM SSL 有効化] チェック ボックスをオフにします。

表 33 SIM サーバー情報 (続き)

SIM サーバー パラ メータ	説明
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)。

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。

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。

サポートされるバージョン

この章の情報は、以下の製品バージョンに当てはまります。

- UCMDB バージョン 8.03 以降
- NNMi バージョン 9.00 以降

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。

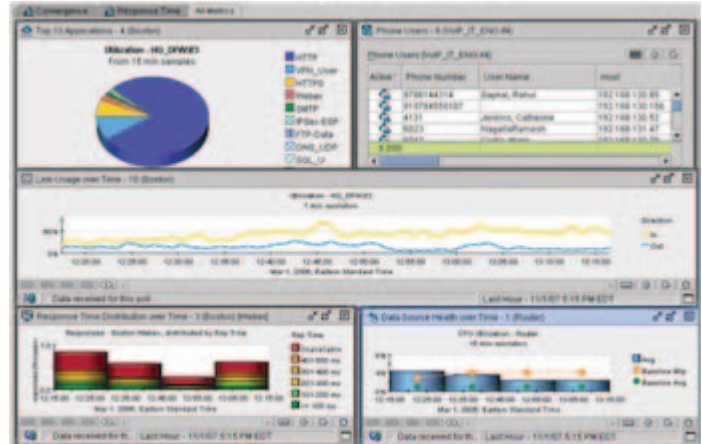
ドキュメント

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『HP Universal CMDB-HP Network Node Manager (NNMi) 統合ガイド』で詳しく説明されています。

HP NNMi-HP UCMDB 統合の使用方法

HP NNMi-HP UCMDB 統合の有効化、使用方法、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 Universal CMDB-HP Network Node Manager (NNMi) 統合ガイド*を参照してください。

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モニタリング
- 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 では、広範囲のネットワーク 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法パターンをモニタリングできます。次に、nGenius Performance Manager は、リアルタイムと履歴のビューおよび以下の情報を示すレポートの集合で結果を表示します。

- 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-suite Software 環境に組み入れると、ネットワーク デバイスのモニタリングと管理のために NNMi を使用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見通しを得られます。

HP NNMi–nGenius Performance Manager 統合では、以下の機能を使用できます。

- nGenius Performance Manager サーバーを受信し、NNMi インシデント ビューでアラームをプローブします。
- 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 ビューの NetScout アイコンで nGenius プローブを表示します。
- NNMi コンソール から nGenius Performance Manager QuickViews を起動します。
- NNMi コンソール から nGenius Performance Manager アプリケーションを起動します。
- NNMi インシデント ビューで利用できる nGenius Performance Manager インシデントについて NNMi レイヤー 2 および レイヤー 3 の近隣接続ビューを起動します。
- NNMi インシデント ビューで利用できる nGenius Performance Manager インシデント用に NNMi パス ビュー マップを起動します。
- nGenius Performance Manager が生成する各アラームについて NNMi にクリア トラップ アラームを転送します。

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。

サポートされるバージョン

この章の情報は、以下の製品バージョンに当てはまります。

- nGenius Performance Manager バージョン 4.6 MR1 (ビルド 654) 以降
- nGenius Performance Manager に同梱された nGenius K2 バージョン
- CDM Agent Firmware バージョン 4.6 MR1 (ビルド 627) 以降
- nGenius InfiniStream アプライアンス バージョン 4.6 MR1 (ビルド 631) 以降
- NNMi バージョン 9.00 以降

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は、同じオペレーティング システムでも、異なるオペレーティング システムでも構いません。

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 v4.3 と HP Network Node Manager i Software の統合 (NetScout パーツ番号 733-0089 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

管理特権またはルート特権を持つユーザーが、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。ユーティリティは、nGenius サーバー用のすべての NNMi 統合関連設定データを 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 v4.3 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 内部で 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 v4.3* 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

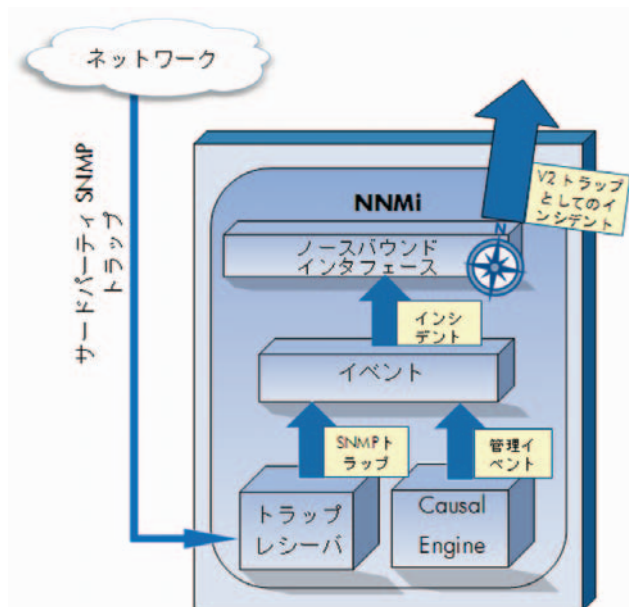
HP NNMi–nGenius Performance Manager 統合の無効化の詳細については、「*nGenius Performance Manager v4.3* と *HP Network Node Manager i Software* の統合」を参照してください。

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



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 Operations Manager (HPOM)。詳細については、459 ページの「HP NNMi-HPOM 統合 (HPOM 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、495 ページの「Netcool ソフトウェア用 HP NNMi 統合モジュール」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 ノースバウンドインタフェースの転送先] 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、インシデント関連処理通知、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 対応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、ノースバウンド アプリケーションの一部。
 - 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 の機能です。
- 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 NNMi Northbound 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 8.1x からアップグレードした NNMi ノースバウンド インタフェース

NNMi 9.00 にアップグレードすると、NNMi Northbound インタフェース設定は **[HP NNMi-Northbound インタフェースの転送先]** フォーム。(このフォームにアクセスするには、**[統合モジュールの設定]** > **[Northbound インタフェース]** をクリックし、転送先を選択してから、**[編集]** をクリックします。) アップグレードした設定が、現在の Northbound アプリケーションに適していることを確認します。



Northbound 転送先で HP Operations Manager (HPOM) エージェントを識別する場合は、以下の推奨事項が適用されます。

長期にわたるメンテナンスを行うため、統合設定を **[HP NNMi-Northbound インタフェースの転送先]** フォームから **[HP NNMi-HPOM エージェント転送先]** フォームに変換することをお勧めします。(このフォームにアクセスするには、**[統合モジュール設定]** > **[HPOM]** をクリックしてから、**[新規作成]** をクリックします。) 設定を変換した後、**[HP NNMi-Northbound インタフェースの転送先]** フォームから送信先を削除します。

表 34 に、NNMi 8.13 から NNMi 9.00 への NNMi Northbound インタフェース設定パラメータのマッピングを示します。これらのフィールドの詳細は、454 ページの「**[NNMi ノースバウンドインタフェースの転送先]** フォームのリファレンス」を参照してください。

表 34 NNMi 8.13 から NNMi 9.00 への NNMi Northbound インタフェース設定パラメータ

NNMi 8.13 Northbound インタフェースパラメータ	NNMi 9.00 Northbound インタフェースパラメータ
NNMi FQDN を使用	選択されていない場合、 [ホスト] フィールドの [ループバックの使用] オプションまたは [その他] オプションにマッピングされます。 選択されている場合、 [ホスト] フィールドの [NNMi FQDN] オプションにマッピングされます。
トラップ先ホスト	[ホスト] フィールドにマッピングされます。
トラップ先ポート	[ポート] フィールドにマッピングされます。
トラップ コミュニティ文字列	[コミュニティ文字列] フィールドにマッピングされます。

表 34 NNMi 8.13 から NNMi 9.00 への NNMi Northbound インタフェース設定パラメータ

NNMi 8.13 Northbound インタフェース パラメータ	NNMi 9.00 Northbound インタフェース パラメータ
保留時間 (分)	直接のマッピング先はありません。インシデント設定フォームの [ダンプニング] タブでインシデント個々の保留時間を定義するか、 <code>nnmsetdampenedinterval.ovpl</code> を使用してすべてのインシデント設定に対して同じ保留時間を設定します。詳細については、 <code>nnmsetdampenendinterval.ovpl</code> 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。
サードパーティ トラップを送信	選択されていない場合、 [管理] インシデントにマッピングされます。 選択されている場合、 [両方] インシデントにマッピングされます。
NNMi で https を使用	[NNMi コンソール アクセス] フィールドにマッピングされます。
ループバックを許可	ホスト名または IP アドレスに非ループバック インタフェースがある場合は、 [ホスト] フィールドの [NNMi FQDN] オプション、または [その他] オプションにマッピングされます。 設定済みホスト名または IP アドレスにループバック専用インタフェースがある場合は、 [ホスト] フィールドの [ループバックの使用] オプションにマッピングされます。
トラップ転送先 IP アドレス	同じです。
アップタイム (秒)	同じです。
最終スweep時間	使用できません。統合の動作に変更はありません。
NNMi URL	同じです。
ダンプニングされたストリームが有効 すべてのストリームが有効	フィールドは使用できません。統合の動作に変更はありません。
なし	その他のフィールドは、456 ページの「 統合コンテンツ 」の説明にあるとおり、NNMi Northbound インタフェースのデフォルトの動作に設定されます。

新規 NNMi Northbound インタフェース設定

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 インタフェースの転送先]** フォーム (**[統合モジュールの設定]** > **[ノースバウンド インタフェース]**) を開き、**[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。)
 - b **[使用可能]** 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、455 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、456 ページの「統合コンテンツ」を参照してください。

- e フォームの下端の [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。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、456 ページの「統合コンテンツ」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。

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。

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。

標準 NNMi 管理イベントの場合、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 の汎用トラップとして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 は各受信 SNMPv1、v2c、および v3 形式のトラップを 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。

転送されるトラップの形式は **SNMPv2c** です。



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。元々のトラップ ソースを判断するには、**IncidentNodeHostname (n+21)** および **IncidentNodeMgmtAddr (n+24) varbind** の値を調べてください。**n** は、**MIB** でトラップに定義されている **varbind** の数を示します。

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、83 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

エンハンスド解決済 みトラップ

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

インシデント関連処理通知

Northbound 転送先にインシデント関連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関連処理されると、NNMi はインシデント関連処理トラップを 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関連変更を複製することができます。

単一関連トラップ

単一関連トラップ オプションの場合、この統合では、以下の関連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関連関係を示します。

- 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)

グループ関連トラップ

グループ関連トラップ オプションの場合、この統合では、以下の関連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 において、親子インシデント関連関係を示します。

- 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 インタフェースの転送先] フォーム ([統合モジュールの設定] > [ノースバウンド]) 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、454 ページの「[NNMi ノースバウンド インタフェースの転送先] 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 [使用可能] 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 インタフェースの転送先]** フォーム (**[統合モジュールの設定]** > **[ノースバウンド]**) 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 **[使用可能]** 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 インタフェースの転送先]** フォーム (**[統合モジュールの設定]** > **[ノースバウンド]**) を開きます。
 - b 転送先を選択し、**[編集]** をクリックします。
 - c **[使用可能]** 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 **[解決済みの根本原因インシデント]** 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 `LifecycleStateChangeEvent` 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。

```
nnmsnmnotify.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、**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 フェー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 フェー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- ノースバウンド インタフェースの転送先] フォームの **[ホスト]** 識別で、**[NNMi FQDN]** または **[ループバックの使用]** 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- ノースバウンド インタフェースの転送先]** 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 ノースバウンド インタフェースの転送先] フォームのリファレンス

HP NNMi-Northbound インタフェースの転送先 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含まれます。このフォームは、**[統合モジュール設定]** ワークスペースから利用できます。(**[HP NNMi- ノースバウンド インタフェースの転送先]** フォームで、**[新規作成]** 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- ノースバウンド インタフェースの転送先]** フォームにアクセスできます。

[HP NNMi- ノースバウンド インタフェースの転送先] フォームには、以下の領域の情報が表示されます。

- 455 ページの「Northbound アプリケーションの接続パラメータ」
- 456 ページの「統合コンテンツ」
- 458 ページの「Northbound 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- ノースバウンド インタフェースの転送先]** 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 35 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 35 Northbound アプリケーションの接続情報

フィールド	説明
ホスト	<p>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。</p> <p>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。</p> <ul style="list-style-type: none">• 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。 <p>注: NNMi 管理サーバーが NNMi アプリケーション フェイルオーバーに参加する場合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、453 ページの「アプリケーション フェイルオーバーと NNMi ノースバウンド インタフェース」を参照してください。</p>
ポート	<p>Northbound アプリケーションが SNMP トラップを受信する UDP ポート。</p> <p>Northbound アプリケーション固有のポート番号を入力します。</p> <p>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。</p>
コミュニティ文字列	<p>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。</p> <p>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。</p> <p>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。</p>

統合コンテンツ

表 36 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 36 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	<p>インシデント転送の指定。</p> <ul style="list-style-type: none"> ● 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。 <p>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、447 ページの「インシデント転送」を参照してください。</p>
ライフサイクル状態の変化	<p>インシデント変更通知の仕様。</p> <ul style="list-style-type: none"> ● 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。 <p>詳細については、448 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。</p>

表 36 NNMi ノースバウンド インタフェースの内容設定情報 (続き)

フィールド	説明
<p>関連処理</p>	<p>インシデント関連処理通知の仕様。</p> <ul style="list-style-type: none"> • なし NNMi は、NNMi 因果関係分析によるインシデント関連処理結果を 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関連関係ごとにトラップを 1 つ送信します。 • グループ NNMi は、親インシデントに相関するすべての子インシデントをリストした関連処理ごとに、トラップを 1 つ送信します。 <p>詳細については、449 ページの「インシデント関連処理通知」を参照してください。</p>
<p>削除</p>	<p>インシデント削除の仕様。</p> <ul style="list-style-type: none"> • 送信しない NNMi は、インシデントが NNMi で削除されても 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。 <p>詳細については、449 ページの「インシデント削除通知」を参照してください。</p>
<p>NNMi コンソール アクセス</p>	<p>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。</p> <p>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。</p> <p>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。</p>

表 36 NNMi ノースバウンド インタフェースの内容設定情報 (続き)

フィールド	説明
Incident Filter(インシデント フィルタ)	<p>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。</p> <p>以下のオプションの 1 つを選択します。</p> <ul style="list-style-type: none"> • なし NNMi はすべてのイベントを 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。 <p>インシデント フィルタを指定します。</p> <ul style="list-style-type: none"> • 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。 <p>詳細については、450 ページの「イベント転送フィルタ」を参照してください。</p>

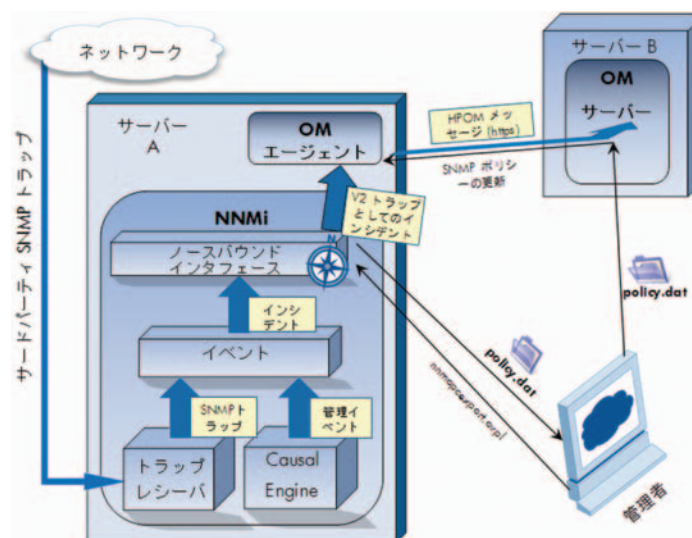
Northbound 転送先のステータス情報

表 37 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 37 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	<p>転送先ホスト名の解決先となる IP アドレス。</p> <p>この値は、このノースバウンド転送先に固有です。</p>
アップタイム (秒)	<p>Northbound コンポーネントが最後に起動されてからの時間 (秒)。NNMi が 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。</p> <p>この値は、NNMi Northbound インタフェースを使用するすべての統合に対して同じです。</p>
NNMi URL	<p>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。</p> <p>この値は、このノースバウンド転送先に固有です。</p>

HP 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 モニタリング、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 (HPOM 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 (HPOM エージェント実装)

HP NNMi-HPOM 統合の HPOM 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 HPOM エージェント実装は、NNMi ノースバウンド インタフェース特有の実装です。これについては、443 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。

HPOM エージェントと HP NNMi-HPOM 統合の 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を転送すると、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、HP NNMi 幽 POM 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。

- 460 ページの「HP NNMi-HPOM 統合について (HPOM エージェント実装)」
- 461 ページの「HP NNMi-HPOM 統合の有効化 (HPOM エージェント実装)」
- 465 ページの「HP NNMi-HPOM 統合の使用法 (HPOM エージェント実装)」

- 466 ページの「[HP NNMi-HPOM 統合設定の変更 \(HPOM エージェント実装\)](#)」
- 467 ページの「[HP NNMi-HPOM 統合の無効化 \(HPOM エージェント実装\)](#)」
- 468 ページの「[HP NNMi-HPOM 統合のトラブルシューティング \(HPOM エージェント実装\)](#)」
- 471 ページの「[\[HP NNMi-HPOM エージェント転送先\] フォーム リファレンス \(HPOM エージェント実装\)](#)」

HP NNMi-HPOM 統合について (HPOM エージェント実装)

HP NNMi-HPOM 統合では、NNMi 管理イベントを SNMPv2c トラップとして NNMi 管理サーバーの HPOM エージェントに転送します。HPOM 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。HPOM 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 HPOM エージェントに転送することもできます。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 HPOM 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 HPOM 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 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。
- 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。

サポートされるバージョン

このセクションの情報は、以下の製品バージョンに当てはまります。

- Windows 用 HPOM バージョン 8.10 以降
- UNIX 用 HPOM バージョン 8.30 以降 (UNIX 用 HPOM バージョン 9.00 以降も含む)
- Linux 用 HPOM バージョン 9.00 以降
- NNMi バージョン 9.00 以降

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、異なっても構いません。

HPOM 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 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、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 (HPOM エージェント実装)

HP NNMi-HPOM 統合の HPOM 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 8.1x からアップグレードされた統合設定

NNMi バージョン 9.00 より前は、HP NNMi-HPOM 統合の HPOM エージェント実装は、[HP NNMi-Northbound インタフェース設定] フォームで有効にしました。NNMi 8.1x 設定の NNMi 9.00 へのマッピングについては、445 ページの「[NNMi 8.1x からアップグレードした NNMi ノーズバウンド インタフェース](#)」を参照してください。

長期にわたるメンテナンスを行うため、統合設定を [HP NNMi-Northbound インタフェースの転送先] フォームから [HP NNMi-HPOM エージェント転送先] フォームに変換することをお勧めします。設定を変換した後、[HP NNMi-Northbound インタフェースの転送先] フォームから送信先を削除します。

新規統合設定

HP NNMi-HPOM 統合を有効化するには、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
```

SNMP トラップ ポリシーには、各管理イベントの SNMPv2c トラップ定義と現在の NNMi 設定の SNMP トラップが含まれます。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。

生成したポリシー ファイルのカスタマイズについては、以下のリファレンスを参照してください。

— *Windows* 用 HPOM: HPOM ヘルプの「ポリシーの開発」

— *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』

- 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 HPOM エージェントをインストールします。

- c 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』
 - *opnode(1M)*、*opcbcdist(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』
 - *opnode(1M)*、*opcbcdist(1M)*、*opcragt(1M)*、*opccfgupl(1M)*、および *opcpolicy(1M)* マンページ

3 NNMi と HPOM 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。

HPOM エージェントは、このポートで、NNMi がここに転送する SNMP トラップを待機します。統合を有効化している間、手順 4 (HPOM 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。

HPOM 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、ほとんどの場合、HPOM エージェントで使用可能です。

- 4 NNMi 管理サーバーで、以下のコマンドを入力して、HPOM エージェントに、NNMi から SNMP トラップを受信するためのカスタム ポートを設定します。
- *Windows* NNMi 管理サーバー：


```
ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> ¥
-set SNMP_SESSION_MODE NNM_LIBS
```
 - *UNIX* NNMi 管理サーバー：


```
ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> ¥
-set SNMP_SESSION_MODE NO_TRAPD
```
- <custom_port>では、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、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 統合選択] フォームを開きます ([統合モジュールの設定] > [HPOM])。
 - b [HPOM エージェント実装] 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 エージェント転送先] フォームで、[使用可能] 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 HPOM 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、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、471 ページの「HPOM 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、472 ページの「統合コンテンツ」を参照してください。
 - f フォームの下端の [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 **HPOM** エージェント実装の場合、**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.name  
nnm.server.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。

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 (HPOM エージェント実装)

HP NNMi-HPOM 統合により、NNMi 管理イベントは HPOM へ一方向に渡されます。HPOM ポリシーにより、HPOM が着信トラップの処理と表示をどう行うかが決まります。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、HPOM 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。)

統合が HPOM に転送するトラップのタイプについては、447 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。

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関連付けるようにポリシーを設定できます。

NNMi が HPOM エージェントに送信する SNMP トラップの内容と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。

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 (HPOM エージェント実装)

新規 NNMi トラップの HPOM ポリシーの更新

統合を設定した後に、新しい SNMP トラップを NNMi に追加した場合、以下の手順を実行します。

- 1 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 新しいポリシーを NNMi 管理対象ノードに配布します。

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 統合選択]** フォームを開きます (**[統合モジュールの設定]** > **[HPOM]**)。
- 2 **[HPOM エージェント実装]** 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、471 ページの「**[HP NNMi-HPOM エージェント転送先]** フォーム リファレンス (**HPOM エージェント実装**)」を参照してください。

- 5 フォームの上端の **[統合を有効化]** 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。

HP NNMi-HPOM 統合の無効化 (HPOM 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。

HPOM 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 統合選択]** フォームを開きます (**[統合モジュールの設定]** > **[HPOM]**)。
- 2 **[HPOM エージェント実装]** 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 フォームの上端の **[統合を有効化]** 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。

または、HPOM ドキュメントの説明に従って、SNMP トラップ ポリシーを無効化または削除します。

HP NNMi-HPOM 統合のトラブルシューティング (HPOM エージェント実装)

HPOM は転送されたインシデントを受信しない



次の手順で、OVBIN 環境変数は HPOM 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、HPOM 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 であってはなりません。また、[HP NNMi-HPOM エージェント転送先] 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 HPOM エージェント設定を評価します。

- HPOM エージェント設定が期待通りの場合、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、464 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 エージェント転送先] フォームの [ポート] フィールドの値と一致しない場合、463 ページの手順 3 から 464 ページの手順 5 までを必要に応じて繰り返します。

3 NNMi 管理サーバーで、HPOM 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`
- **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
```

出力が期待通りの場合、HPOM エージェントを再起動します。

- 4 NNMi 管理サーバーで、HPOM エージェントが期待されている SNMP トラップ ポート上でリッスン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 [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。

出力が期待通りの場合、HPOM エージェントを再起動します。

- 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、[462 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 HPOM 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、[462 ページの \[手順 2\]\(#\)](#) で作成したポリシー ファイルの名前です。

- 7 HPOM 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 HPOM 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 HPOM エージェントのトレースを有効化して、トラップが HPOM エージェントに到着するかどうか判定します。

HPOM 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 が管理イベントを HPOM エージェントに転送していることを確認します。

詳細については、[451 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。

転送されたインシデントの中に HPOM が受信しないものがある

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、HPOM ポリシーによってトラップが抑制されてい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、462 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、HPOM 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、HPOM 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。

HPOM 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 エージェント転送先] フォーム リファレンス (HPOM エージェント実装)

[HP NNMi-HPOM エージェント転送先] 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、[統合モジュール設定] ワークスペースから利用できます。([HP NNMi-HPOM 統合選択] フォームで、[HPOM エージェント実装] 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 エージェント転送先] 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 エージェント転送先] フォームでは、以下の領域の情報を収集します。

- 471 ページの「HPOM エージェント接続」
- 472 ページの「統合コンテンツ」
- 474 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-HPOM エージェント転送先] フォームの値を更新し、[送信] をクリックします。

HPOM エージェント接続

表 38 に、HPOM 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 38 HPOM エージェント接続情報

フィールド	説明
ホスト	<p>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。HPOM 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。</p> <p>この統合では、HPOM エージェント ホストを特定手段として、以下の方法がサポートされています。</p> <ul style="list-style-type: none">• NNMi FQDN NNMi が NNMi 管理サーバー上の HPOM 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。 <p>注: NNMi 管理サーバーが NNMi アプリケーション フェイルオーバーに参加する場合、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は 453 ページの「アプリケーション フェイルオーバーと NNMi ノースバウンド インタフェース」を参照してください。</p>

表 38 HPOM エージェント接続情報 (続き)

フィールド	説明
ポート	<p>HPOM エージェントが SNMP トラップを受信する UDP ポート。</p> <p>HPOM 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、463 ページの手順 3 で定義したポートです。</p> <p>ポートを決定するには、NNMi 管理サーバー上で <code>ovconfget -eaagt</code> コマンドを実行します。トラップ ポートは、SNMP_TRAP_PORT 変数の値です。</p> <p>注: このポート番号は、NNMi コンソールの [通信の設定] フォームの [SNMP ポート] フィールドで設定した、NNMi が SNMP トラップを受信するためのポートと別にする必要があります。</p>
コミュニティ文字列	<p>HPOM 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。</p> <p>HPOM 統合では、デフォルト値 public を使用します。</p>

統合コンテンツ

表 39 に、NNMi が HPOM 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 39 HPOM エージェント統合コンテンツ設定情報

フィールド	説明
インシデント	<p>インシデント転送の指定。</p> <ul style="list-style-type: none"> • 管理 NNMi は、NNMi が生成した管理イベントのみを HOPM 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 HOPM エージェントを転送します。 • 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 HPOM エージェントに転送します。 これがデフォルト設定です。 <p>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、447 ページの「インシデント転送」を参照してください。</p>

表 39 HPOM エージェント統合コンテンツ設定情報 (続き)

フィールド	説明
ライフサイクル状態の変化	<p>インシデント変更通知の仕様。</p> <ul style="list-style-type: none"> ● 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 HPOM 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 HPOM 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 HPOM エージェントに送信します。また、この統合では、ライフサイクル状態が [進行中]、[完了]、または [解決済み] に変化したインシデントごとに、インシデント ライフサイクル状態変化トラップを HPOM エージェントに送信します。 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、448 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。
関連処理	<p>インシデント関連処理通知の仕様。</p> <ul style="list-style-type: none"> ● 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関連処理について、HPOM 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関連関係ごとにトラップを 1 つ送信します。 ● グループ NNMi は、親インシデントに相関するすべての子インシデントをリストした関連処理ごとに、トラップを 1 つ送信します。 詳細については、449 ページの「インシデント関連処理通知」を参照してください。
削除	<p>インシデント削除の仕様。</p> <ul style="list-style-type: none"> ● 送信しない NNMi は、NNMi でインシデントが削除されても、HPOM 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 HPOM エージェントに送信します。 詳細については、449 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	<p>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 HPOM エージェントに送信するトラップには、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。</p>

表 39 HPOM エージェント統合コンテンツ設定情報 (続き)

フィールド	説明
Incident Filter(インシデント フィルタ)	<p>HPOM 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。</p> <p>以下のオプションの 1 つを選択します。</p> <ul style="list-style-type: none"> • なし NNMi はすべてのイベントを HPOM 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。 <p>インシデント フィルタを指定します。</p> <ul style="list-style-type: none"> • 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。 <p>詳細については、450 ページの「イベント転送フィルタ」を参照してください。</p>

転送先ステータス情報

表 40 に、HPOM 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 40 HPOM エージェント統合ステータス情報

フィールド	説明
トラップ転送先 IP アドレス	<p>HPOM エージェント転送先ホスト名で解決する IP アドレス。</p> <p>この値は、この HPOM エージェント転送先に対して一意です。</p>
アップタイム (秒)	<p>Northbound コンポーネントが最後に起動されてからの時間 (秒)。NNMi が HPOM エージェントに送信するトラップには、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)。</p> <p>この値は、NNMi Northbound インタフェースを使用するすべての統合に対して同じです。</p>
NNMi URL	<p>NNMi コンソールに接続するための URL。NNMi が HPOM エージェントに送信するトラップには、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)。</p> <p>この値は、このノースバウンド転送先に固有です。</p>

HP NNMi-HPOM 統合 (Web サービス実装)

HPOM 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。

HPOM エージェントと HP NNMi-HPOM 統合の 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を転送すると、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、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。

- 475 ページの「[HP NNMi-HPOM 統合について \(Web サービス実装\)](#)」
- 477 ページの「[HP NNMi-HPOM 統合の有効化 \(Web サービス実装\)](#)」
- 481 ページの「[HP NNMi-HPOM 統合の使用法 \(Web サービス実装\)](#)」
- 482 ページの「[HP NNMi-HPOM 統合設定の変更 \(Web サービス実装\)](#)」
- 483 ページの「[HP NNMi-HPOM 統合の無効化 \(Web サービス実装\)](#)」
- 483 ページの「[HP NNMi-HPOM 統合のトラブルシューティング \(Web サービス実装\)](#)」
- 488 ページの「[\[HP NNMi-HPOM Web サービス統合設定\] 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 統合は NNMi インシデントを HPOM アクティブ メッセージブラウザに転送します。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。

サポートされるバージョン

このセクションの情報は、以下の製品バージョンに当てはまります。

- Windows 用 HPOM バージョン 8.10 以降
- UNIX 用 HPOM バージョン 8.30 以降 (UNIX 用 HPOM バージョン 9.00 以降も含む)
- Linux 用 HPOM バージョン 9.00 以降
- NNMi バージョン 9.00 以降

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 統合選択] フォームを開きます ([統合モジュールの設定] > [HPOM])。
 - b [Web サービス実装] をクリックします。
 - c [HP NNMi-HPOM Web サービス統合設定] 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 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、488 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、489 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、490 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 **[追加の HPOM サーバー]** リストに表示されます。

- h フォームの下端の **[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 統合選択]** フォームを開きます (**[統合モジュールの設定]** > **[HPOM]**)。
 - b **[Web サービス実装]** をクリックします。
 - c **[HP NNMi-HPOM Web サービス統合設定]** 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 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、488 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、489 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、490 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 [**追加の HPOM サーバー**] リストに表示されます。

h フォームの下端の [**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 フォームの下端の [**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 21 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 21 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

重要度	受信	最後の発生日時	ソースノード	ソースオブ...	カテ...	ファ...	発...	メッセージ
危険域	5	10/06/09 0:43:28	ntc6kgw02	Et1/0				インタフェースで Disc...

図 22 は、Windows 用 HPOM で受信された NNMi インシデントを示します。図 23 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。



479 ページの手順 4 (Windows 用 HPOM) および 480 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 22 Forwarded Incident in HPOM for Windows (Windows 用 HPOM で転送済みのインシデント)

重要度	受信	サービス	ノード	アプリケー...	オブジェ...	テキスト
危険域	2010/06/07 13:20:33	Server	G11NVM113(管...	NNMi	なし	インタフェースで Cisco E...

図 23 Forwarded Incident in HPOM for UNIX (UNIX 用 HPOM で転送済みのインシデント)

Severity	Time Received	Node	Application	Object	Message Text	nnm.source.name
critical	08:56:39 09/2...	ovccrt1...	NNMi	Interface	Cisco Agent Interface Down (linkDown Trap) on interf...	Et1/0

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 統合選択] フォームを開きます ([統合モジュールの設定] > [HPOM])。
- 2 [Web サービス実装] 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、488 ページの「[HP NNMi-HPOM Web サービス統合設定] フォーム リファレンス」を参照してください。
- 4 フォームの上端の [統合を有効化] 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。

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 統合選択]** フォームを開きます (**[統合モジュールの設定]** > **[HPOM]**)。
- 2 **[Web サービス実装]** をクリックします。
- 3 フォームの上端の **[統合を有効化]** 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。

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 統合選択]** フォームを開きます (**[統合モジュールの設定]** > **[HPOM]**)。
- 2 **[Web サービス実装]** 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。

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。482 ページの「[HP NNMi-HPOM 統合設定の変更 \(Web サービス実装\)](#)」に説明してあ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 統合選択]** フォームを開きます (**[統合モジュールの設定]** > **[HPOM]**)。
- 2 **[Web サービス実装]** をクリックします。

このフォームのフィールドの詳細は、488 ページの「[\[HP NNMi-HPOM Web サービス統合設定\] 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。

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。478 ページの**手順 3 (Windows 用の HPOM)** と 480 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>://<NNMIserv>:<port>/nmm/

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。

- <NNMIserv> 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、488 ページの表 41 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が、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 サービス統合設定]** フォームに再入力します。

- **[HP NNMi-HPOM Web サービス統合設定]** 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 サービス統合設定]** フォームを更新します。

詳細については、488 ページの「**[HP NNMi-HPOM Web サービス統合設定]** フォーム リファレンス」を参照してください。
- 8 フォームの下端の **[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に設定する必要があります。478 ページの手順 3 (Windows 用の HPOM) と 480 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。479 ページの手順 4 (Windows 用 HPOM) および 480 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 サービス統合設定] フォーム リファレンス

[HP NNMi-HPOM Web サービス統合設定] 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、[統合モジュール設定] ワークスペースから利用できます。([HP NNMi-HPOM 統合選択] フォームで、[Web サービス実装] をクリックします。)



[HP NNMi-HPOM Web サービス統合設定] 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。

- 488 ページの「NNMi 管理サーバー接続」
- 489 ページの「HPOM Management Server Connection(HPOM 管理サーバー接続)」
- 490 ページの「統合動作」
- 491 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 41 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 41 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 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した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 <code>nnmofficialfqdn.ovpl -t</code> 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。 <ul style="list-style-type: none"> • Windows: %NnmDataDir%\%conf%\nnm\props\%nms-local.properties • UNIX: \$NnmDataDir/conf/nnm/props/nms-local.properties SSL 以外の接続では、 <code>jboss.http.port</code> 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 41 NNMi 管理サーバー接続情報 (続き)

フィールド	説明
NNMi User(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。 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 Integration 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 42 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 42 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。 <ul style="list-style-type: none"> 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、tracert 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。 <ul style="list-style-type: none"> 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 <code>ovtomcatbctl -getconf</code> 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 42 HPOM 管理サーバー接続情報 (続き)

HPOM サーバー パラメータ	説明
HPOM User(HPOM ユーザー)	<p>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。</p> <p><i>Windows</i> のみ : <i>Windows</i> 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。<i>Windows</i> ユーザーを <Windows_domain><username> の形式で指定します。</p> <p>ベスト プラクティス :</p> <ul style="list-style-type: none"> • <i>Windows</i> 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。) • <i>UNIX</i> 用 HPOM または <i>Linux</i> 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 43 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 43 統合動作情報

フィールド	説明
Forward Only(転送のみ)	<p>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。</p> <ul style="list-style-type: none"> • 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))	<p>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。</p> <p>デフォルト値は 5 分です。</p>
Incident Filter(インシデント フィルタ)	<p>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。</p> <p>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。</p> <p>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。</p>

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、492 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 統合選択] フォームを開きます ([統合モジュールの設定] > [HPOM])。
- 2 [Web サービス実装] 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
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。
性質	<ul style="list-style-type: none">• ROOTCAUSE• SECONDARYROOTCAUSE• SYMPTOM• SERVICEIMPACT• STREAMCORRELATION• INFO• なし

属性	使用できる値
原点	<ul style="list-style-type: none"> • MANAGEMENTSOFTWARE • MANUALLYCREATED • SYMPTOM • REMOTELYGENERATED • SNMPTRAP • SYSLOG • OTHER
ファミリー	<ul style="list-style-type: none"> • 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
カテゴリ	<ul style="list-style-type: none"> • 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
重大度	<ul style="list-style-type: none"> • 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 フォームの下端の **[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

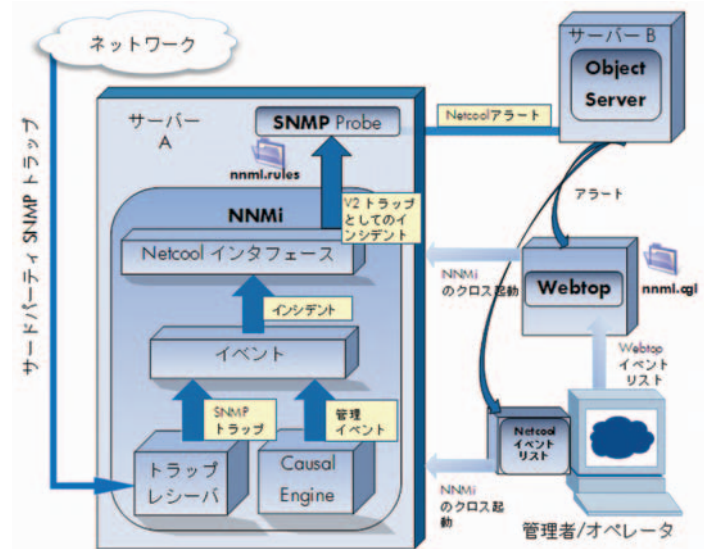
```
severity>=MINOR  
nature=ROOTCAUSE  
nature=SERVICEIMPACT
```

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、**severity(重要度)** が **MINOR** 以上の **NodeDown** インシデントと **severity(重要度)** が **MAJOR** の **InterfaceDown** インシデントを転送するには、フィルタの **severity(重要度)** を **>=MINOR** に設定し、**HPOM** ロジックを使用して不要な **InterfaceDown** メッセージをフィルタで除外します。
- 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。

Netcool ソフトウェア用 HP NNMi 統合モジュール



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。

- Netcool ソフトウェア用 HP NNMi 統合モジュール
- Netcool ソフトウェア用 HP NNMi 統合モジュールの有効化
- Netcool ソフトウェア用 HP NNMi 統合モジュールの使用法
- Netcool ソフトウェア用 HP NNMi 統合モジュールの変更
- Netcool ソフトウェア用 HP NNMi 統合モジュールの無効化
- Netcool ソフトウェア用 HP NNMi 統合モジュール のトラブルシューティング
- Netcool ソフトウェア用 HP NNMi 統合モジュール 転送先フォームのリファレンス

Netcool ソフトウェア用 HP NNMi 統合モジュール

Netcool ソフトウェア用 HP NNMi 統合モジュールは、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 443 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。

サポートされるバージョン

この章の情報は、以下の製品バージョンに当てはまります。

- Netcool/OMNibus バージョン 7.2.1
- Netcool/OMNibus SNMP Probe バージョン 7.2.1



Netcool ソフトウェア用 NNMi 統合モジュールは、リストされたバージョンの Netcool 製品で検証されています。統合はほかのバージョンの Netcool 製品で正しく機能するはずですが、HP は、リストされたバージョンの Netcool 製品のみとの統合の使用をサポートしています。

- NNMi バージョン 9.00 以降 (Netcool ソフトウェア用 NNMi 統合モジュール ライセンスを取得している場合)



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され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。

Netcool ソフトウェア用 HP NNMi 統合モジュールの有効化

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。

NNMi 8.1x からアップグレードした Netcool ソフトウェア用 NNMi 統合モジュール

NNMi 9.00 にアップグレードすると、Netcool ソフトウェア用 NNMi 統合モジュール設定は **[Netcool ソフトウェア用 HP NNMi 統合モジュール転送先]** フォームに移動します。(このフォームにアクセスするには、**[統合モジュールの設定]** > **[Netcool]** をクリックし、**[編集]** をクリックします)。アップグレード設定が正確であることを確認します。

表 44 に、NNMi 8.13 から NNMi 9.00 への Netcool ソフトウェア用 NNMi 統合モジュール設定パラメータのマッピングを示します。

表 44 NNMi 8.13 と NNMi 9.00 の Netcool ソフトウェア用 NNMi 統合モジュール統合設定パラメータ

NNMi 8.13 Netcool ソフトウェア用 NNMi 統合モジュール パラメータ	NNMi 9.00 Netcool ソフトウェア用 NNMi 統合モジュール パラメータ
NNMi FQDN を使用 トラップ先ホスト	[ホスト] フィールドの [NNMi FQDN] オプションにマッピングされます。
トラップ先ポート	[ポート] フィールドにマッピングされます。
トラップ コミュニティ文字列	[コミュニティ文字列] フィールドにマッピングされます。
保留時間 (分)	直接のマッピング先はありません。インシデント設定フォームの [ダンプニング] タブでインシデント個々の保留時間を定義するか、 <code>nnmsetdampenedinterval.ovpl</code> を使用してすべてのインシデント設定に対して同じ保留時間を設定します。詳細については、 <code>nnmsetdampenedinterval.ovpl</code> リファレンス ページ、または UNIX マニュアルを参照してください。
サードパーティ トラップを送信	選択されていない場合、 [管理] インシデントにマッピングされます。 選択されている場合、 [両方] インシデントにマッピングされます。

表 44 NNMi 8.13 と NNMi 9.00 の Netcool ソフトウェア用 NNMi 統合モジュール統合設定パラメータ

NNMi 8.13 Netcool ソフトウェア用 NNMi 統合モジュール パラメータ	NNMi 9.00 Netcool ソフトウェア用 NNMi 統合モジュール パラメータ
NNMi で https を使用	[NNMi コンソール アクセス] フィールドにマッピングされます。
ループバックを許可	選択されていない場合、[ホスト] フィールドの [NNMi FQDN] オプションまたは [その他] オプションにマッピングされます。 選択されている場合、[ホスト] フィールドの [ループバックを使用] オプションにマッピングされます。
トラップ転送先 IP アドレス	同じです。
アップタイム (秒)	同じです。
最終スweep時間	使用できません。統合の動作に変更はありません。
NNMi URL	同じです。
ダンプニングされたストリームが有効 すべてのストリームが有効	フィールドは使用できません。統合の動作に変更はありません。
なし	その他のフィールドは、456 ページの「統合コンテンツ」の説明にあるとおり、Northbound インタフェースのデフォルトの動作に設定されます。

新規 Netcool ソフトウェア用 NNMi 統合モジュール設定

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、[Netcool ソフトウェア用 HP NNMi 統合モジュール設定アクション] フォームを開きます ([統合モジュール設定] > [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。
 - **nnmi_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、**[Netcool ソフトウェア用 HP NNMi 統合モジュール設定アクション]** フォームを開きます (**[統合モジュール設定] > [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。)
 - d **[Netcool ソフトウェア用 HP NNMi 統合モジュール転送先]** フォームで **[有効化]** 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、504 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、505 ページの「**統合コンテンツ**」を参照してください。
 - g フォームの下端の **[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。

Netcool ソフトウェア用 HP NNMi 統合モジュールの使用法

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、447 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、83 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。

497 ページの「[Netcool ソフトウェア用 HP NNMi 統合モジュールの有効化](#)」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。

Netcool ソフトウェア用 HP NNMi 統合モジュールの変更

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、**[Netcool ソフトウェア用 HP NNMi 統合モジュール設定アクション]** フォームを開きます (**[統合モジュール設定]** > **[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、504 ページの「**Netcool ソフトウェア用 HP NNMi 統合モジュール 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 **[有効化]** 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。

Netcool ソフトウェア用 HP NNMi 統合モジュールの無効化

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、**[Netcool ソフトウェア用 HP NNMi 統合モジュール設定アクション]** フォームを開きます (**[統合モジュール設定]** > **[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 **[Netcool ソフトウェア用 HP NNMi 統合モジュール転送先]** フォームで、フォームの上にある **[有効化]** 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。

Netcool ソフトウェア用 HP NNMi 統合モジュール 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、451 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。

Netcool ソフトウェア用 HP NNMi 統合モジュール 転送先 フォームのリファレンス

[Netcool ソフトウェア用 HP NNMi 統合モジュール転送先] 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、[統合モジュール設定] ワークスペースから利用できます ([Netcool ソフトウェア用 HP NNMi 統合モジュール設定アクション] 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 [Netcool ソフトウェア用 HP NNMi 統合モジュール転送先] フォームにアクセスできます。

[Netcool ソフトウェア用 HP NNMi 統合モジュール 転送先] フォームでは、以下の領域の情報を収集します。

- 504 ページの「Netcool/OMNIbus SNMP Probe の接続」
- 505 ページの「統合コンテンツ」
- 508 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、[Netcool ソフトウェア用 HP NNMi 統合モジュール転送先] 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 45 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 45 Netcool/OMNIbus SNMP Probe の接続情報

フィールド	説明
ホスト	<p>NNMi 管理サーバーの完全修飾ドメイン名 (推奨) または IP アドレス。これは、Netcool/OMNIbus SNMP Probe が SNMP トラップを NNMi から受信するシステムです。</p> <p>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。</p> <ul style="list-style-type: none">• 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。 <p>注: NNMi 管理サーバーが NNMi アプリケーション フェイルオーバーに参加する場合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、453 ページの「アプリケーション フェイルオーバーと NNMi ノースバウンド インタフェース」を参照してください。</p>

表 45 Netcool/OMNIbus SNMP Probe の接続情報 (続き)

フィールド	説明
ポート	<p>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。</p> <p>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 <code>mttrapd.properties</code> ファイルを確認します。</p> <p>注: このポート番号は、NNMi コンソールの [通信の設定] フォームの [SNMP ポート] フィールドで設定した、NNMi が SNMP トラップを受信するためのポートと別にする必要があります。</p>
コミュニティ文字列	<p>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。</p> <p>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。</p> <p>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 <code>public</code> を使用します。</p>

統合コンテンツ

表 46 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 46 Netcool ソフトウェア用 NNMi 統合モジュールコンテンツ設定情報

フィールド	説明
インシデント	<p>インシデント転送の指定。</p> <ul style="list-style-type: none"> • 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。 <p>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、447 ページの「インシデント転送」を参照してください。</p>

表 46 Netcool ソフトウェア用 NNMi 統合モジュールコンテンツ設定情報

フィールド	説明
ライフサイクル状態の変化	<p>インシデント変更通知の仕様。</p> <ul style="list-style-type: none"> ● 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、448 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。
関連処理	<p>インシデント関連処理通知の仕様。</p> <ul style="list-style-type: none"> ● 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関連処理について、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関連関係ごとにトラップを 1 つ送信します。 ● グループ NNMi は、親インシデントに相関するすべての子インシデントをリストした相関処理ごとに、トラップを 1 つ送信します。 詳細については、449 ページの「インシデント関連処理通知」を参照してください。
削除	<p>インシデント削除の仕様。</p> <ul style="list-style-type: none"> ● 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、449 ページの「インシデント削除通知」を参照してください。

表 46 Netcool ソフトウェア用 NNMi 統合モジュールコンテンツ設定情報

フィールド	説明
NNMi コンソールアクセス	<p>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。</p> <p>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。</p> <p>NNMi コンソールが HTTP と HTTPS 両方の接続を承認するように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。</p>
Incident Filter(インシデント フィルタ)	<p>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。</p> <p>以下のオプションの 1 つを選択します。</p> <ul style="list-style-type: none"> • なし NNMi はすべてのイベントを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。 <p>インシデント フィルタを指定します。</p> <ul style="list-style-type: none"> • 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。 <p>詳細については、450 ページの「イベント転送フィルタ」を参照してください。</p>

転送先ステータス情報

表 47 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 47 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。
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。

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 9.00 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 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
- NNMi 8.00 からの Windows パスおよび環境変数

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 Server 2003:**

- %NnmInstallDir%: <drive>%Program Files%HP\HP BTO Software
- %NnmDataDir%: <drive>%Documents and Settings%All Users%Application Data%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、515 ページの「NNMi 8.00 からの Windows パスおよび環境変数」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、512 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、515 ページの「[NNMi 8.00 からの Windows パスおよび環境変数](#)」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 48 (Windows) または表 49 (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 48 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¥HP¥HP BTO Software¥bin
%NNM_CONF%	<ul style="list-style-type: none">• Windows Server 2008: C:¥ProgramData¥HP¥HP BTO Software¥conf• Windows Server 2003: C:¥Documents and Settings¥All Users¥Application Data¥HP¥HP BTO Software¥conf
%NNM_DATA%	<ul style="list-style-type: none">• Windows Server 2008: C:¥ProgramData¥HP¥HP BTO Software¥• Windows Server 2003: C:¥Documents and Settings¥All Users¥Application Data¥HP¥HP BTO Software¥
%NNM_DB%	<ul style="list-style-type: none">• Windows Server 2008: C:¥ProgramData¥HP¥HP BTO Software¥databases• Windows Server 2003: C:¥Documents and Settings¥All Users¥Application Data¥HP¥HP BTO Software¥databases
%NNM_JAVA%	C:¥Program Files¥HP¥HP BTO Software¥nonOV¥jdk¥b¥bin¥java.exe
%NNM_JAVA_DIR%	C:¥Program Files¥HP¥HP BTO Software¥java
%NNM_JAVA_PATH_SEP%	;
%NNM_JBOSS%	C:¥Program Files¥HP¥HP BTO Software¥nonOV¥jboss¥nms
%NNM_JBOSS_DEPLOY%	C:¥Program Files¥HP¥HP BTO Software¥nonOV¥jboss¥nms¥server¥nms¥deploy

表 48 Windows OS での環境変数のデフォルトの場所 (続き)

変数	Windows (例)
%NNM_JBOSS_LOG%	C:\Program Files\HP\HP BTO Software\nonOV\jboss\nms\server\nms\log
%NNM_JBOSS_ROOT%	C:\Program Files\HP\HP BTO Software\nonOV\jboss\nms
%NNM_JBOSS_SERVERCONF%	C:\Program Files\HP\HP BTO Software\nonOV\jboss\nms\server\nms
%NNM_JRE%	C:\Program Files\HP\HP BTO Software\nonOV\jdk\b
%NNM_LOG%	<ul style="list-style-type: none"> Windows Server 2008: C:\ProgramData\HP\HP BTO Software\log Windows Server 2003: C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\log
%NNM_LRF%	<ul style="list-style-type: none"> Windows Server 2008: C:\ProgramData\HP\HP BTO Software\shared\nnm\lrf Windows Server 2003: C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared\nnm\lrf
%NNM_PRIV_LOG%	<ul style="list-style-type: none"> Windows Server 2008: C:\ProgramData\HP\HP BTO Software\log Windows Server 2003: C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\log
%NNM_PROPS%	<ul style="list-style-type: none"> Windows Server 2008: C:\ProgramData\HP\HP BTO Software\shared\nnm\conf\props Windows Server 2003: C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared\nnm\conf\props
%NNM_SHARED_CONF%	<ul style="list-style-type: none"> Windows Server 2008: C:\ProgramData\HP\HP BTO Software\shared\nnm\conf Windows Server 2003: C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared\nnm\conf
%NNM_SHARE_LOG%	<ul style="list-style-type: none"> Windows Server 2008: C:\ProgramData\HP\HP BTO Software\log Windows Server 2003: C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\log

表 48 Windows OS での環境変数のデフォルトの場所 (続き)

変数	Windows (例)
%NNM_SNMP_MIBS%	C:\Program Files\HP\HP BTO Software\misc\%nnm%\snmp_mibs
%NNM_SUPPORT%	C:\Program Files\HP\HP BTO Software\support
%NNM_TMP%	<ul style="list-style-type: none"> Windows Server 2008: C:\ProgramData\HP\HP BTO Software\tmp Windows Server 2003: C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\tmp
%NNM_USER_SNMP_MIBS%	<ul style="list-style-type: none"> Windows Server 2008: C:\ProgramData\HP\HP BTO Software\shared\%nnm%\user-snmp-mibs Windows Server 2003: C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared\%nnm%\user-snmp-mibs
%NNM_WWW%	C:\Program Files\HP\HP BTO Software\www

表 49 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/databases
\$NNM_JAVA	/opt/OV/nonOV/jdk/b/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/b
\$NNM_LOG	/var/opt/OV/log
\$NNM_LRF	/var/opt/OV/shared/nnm/lrf
\$NNM_PRIV_LOG	/var/opt/OV/log

表 49 UNIX OS での環境変数のデフォルトの場所 (続き)

変数	HP-UX
\$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	/opt/OV/www

NNMi 8.00 からの Windows パスおよび環境変数

Windows OS では、NNMi ファイルへのデフォルト パスは、バージョン 8.00 と 8.01 (以上) では異なります。NNMi 8.00 より上の新バージョンの NNMi にアップグレードすると、新しいバージョンの NNMi は NNMi 8.00 で定義されたパスを使い続けます。この場合、NNMi インストール中に作成された環境変数の場所は以下ようになります。

- %NnmInstallDir%: <drive>%Program Files (x86)%HP OpenView
- %NnmDataDir%: <drive>%Program Files (x86)%HP OpenView\data

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。

```
"C:%Program Files (x86)%HP OpenView%bin%nmn.envvars.bat"
```

コマンドを実行した後で、表 50 で示す NNMi 環境変数を使用して頻繁に使用する NNMi ファイルの場所へ移動できます。



アップグレードのみの場合は、表 50 の情報を 512 ページの表 48 の情報より優先してください。

表 50 NNMi 8.00 Windows OS 環境変数のデフォルトの場所

変数	Windows (例)
%NNM_BIN%	C:%Program Files (x86)%HP OpenView%bin
%NNM_CONF%	C:%Program Files (x86)%HP OpenView\data%conf
%NNM_DATA%	C:%Program Files (x86)%HP OpenView\data
%NNM_DB%	C:%Program Files (x86)%HP OpenView\data%databases
%NNM_JAVA%	C:%Program Files (x86)%HP OpenView%nonOV%jdk%b%bin%java.exe
%NNM_JAVA_DIR%	C:%Program Files (x86)%HP OpenView%java

表 50 NNMi 8.00 Windows OS 環境変数のデフォルトの場所

変数	Windows (例)
%NNM_JAVA_PATH_SEP%	;
%NNM_JBOSS%	C:\Program Files (x86)\HP OpenView\nonOV\jboss\nms
%NNM_JBOSS_DEPLOY%	C:\Program Files (x86)\HP OpenView\nonOV\jboss\nms\server\nms\deploy
%NNM_JBOSS_LOG%	C:\Program Files (x86)\HP OpenView\nonOV\jboss\nms\server\nms\log
%NNM_JBOSS_ROOT%	C:\Program Files (x86)\HP OpenView\nonOV\jboss\nms
%NNM_JBOSS_SERVERCONF%	C:\Program Files (x86)\HP OpenView\nonOV\jboss\nms\server\nms
%NNM_JRE%	C:\Program Files (x86)\HP OpenView\nonOV\jdk\b
%NNM_LOG%	C:\Program Files (x86)\HP OpenView\data\log
%NNM_LRF%	C:\Program Files (x86)\HP OpenView\data\shared\nnm\lrf
%NNM_PRIV_LOG%	C:\Program Files (x86)\HP OpenView\data\log
%NNM_PROPS%	C:\Program Files (x86)\HP OpenView\data\shared\nnm\conf\props
%NNM_SHARE_LOG%	C:\Program Files (x86)\HP OpenView\data\log
%NNM_SHARED_CONF%	C:\Program Files (x86)\HP OpenView\data\shared\nnm\conf
%NNM_SNMP_MIBS%	C:\Program Files (x86)\HP OpenView\misc\nnm\snmp_mibs
%NNM_SUPPORT%	C:\Program Files (x86)\HP OpenView\support
%NNM_TMP%	C:\Program Files (x86)\HP OpenView\data\tmp
%NNM_USER_SNMP_MIBS%	C:\Program Files (x86)\HP OpenView\data\shared\nnm\user-snmp-mibs
%NNM_WWW%	C:\Program Files (x86)\HP OpenView\www

NNMi 9.00 およびウェルノウン ポート

表 51 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 51 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、 <i>nnmtrapconfig.ovpl</i> 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 51 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
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		複数サブネット アプリケーションのフェイルオーバーで使用する JGroups マルチキャスト 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 ovsmppd (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
45588	UDP	jgroups.udp.mcast_port	LAN アプリケーションのフェイルオーバーで使用する JGroups マルチキャスト ポート	nms-cluster.properties ファイルを変更します

表 52 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 52 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
162	UDP	SNMP トラップ ポート。トラップ転送、Northbound インターフェイス、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	複数サブネット アプリケーションのフェイルオーバーで使用する JGroups マルチキャスト 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

表 52 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
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
45588	UDP	LAN アプリケーションのフェイルオーバーで使用する JGroups マルチキャスト ポート	クライアントと サーバー
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weep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 インターフェイスを使用する 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 53 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 53 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。

問題点と解決策

データベース プールに使用可能な接続が *number* あります。

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。

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。

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。

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。

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。

ディスク場所 *location name* には *number%* の空き容量しかありません。

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。

平均的なシステム負荷は *number* です。

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。

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。

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。

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。

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。一度に開かれるファイルは 1,000 ファイルより少なくなることが期待されますが、特定の環境ではもっと多くのファイルが必要になる場合もあります。ただし、開いているファイル ハンドル数が増え続けている場合は、製品に問題があることを示す場合があります。

NNMi CPU の使用率は 100% です。

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。負荷の高いときにわずかな間に発生することがありますが、この警告メッセージが常時表示される場合は、負荷のためにシステムの処理能力が落ちている可能性があります。

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。

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 マネージャが単にメンテナンスのためにダウンしている場合は、オンラインに戻った時点で復元されますが、この数字が数十万件を超えるような場合は、手動でクリアしなければならないこともあります (サポートにお問い合わせください)。

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。

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。これが短時間表示される場合は心配には及びませんが、長時間表示される場合は、何らかの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。

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。

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。これは、システムに過剰な負荷がかかっているか、インストールされている SPI 数が多すぎることを示します。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。

メモリ領域 '*region name*' の使用率は *number*% です。

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。

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。

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 テクノロジー。Causal Engine RCA をトリガーするのは、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複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。

HP Network Node Manager i-suite Software

HP NNM i-suite Software とも呼ばれます。HP Network Node Manager i Software 製品 (NNMi) の周りに構築された HP ソフトウェア製品のファミリーです。HP NNM i-suite Software には、NNMi、NNMi Advanced、NNM iSPI for Performance、NNM iSPI for MPLS のような関連 iSPI が含まれます。

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

[HP Network Node Manager i-suite Software](#) 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ー用に、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 スイープ

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 プロブ テクニック。ルールベースの検出で有効化されている場合、NNMi は、設定 IP アドレス範囲について ping スイープを使用し、追加ノードを見つけることができます。サービス拒絶攻撃に ping スイ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ตอบสนอง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。nmtrapconfig.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。

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、モニタリングの設定、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かの【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。

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 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。

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。

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、管理対照ノードとの間で 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。「パブリック キー証明書」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。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、可用性またはパフォーマンス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weep 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。

最初の検出の後に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 アドレスまたはシステムオブジェクト ID (OID)。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。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、スパイラル検出 v1 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。根本原因の判定の結果、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が行われることがあります。

NNMi が RCA を使う方法の例を挙げると、管理対象ルーターに障害が発生し、NNMi 管理サーバーからルーターの別の側にある管理対象ノードが状態ポーリングクエリーに応答できなくなるというシナリオです。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 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。

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。

自動検出

ルールベースの検出を参照してください。

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または ICMP ping 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 [モニタリングの設定] 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。

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 StatePoller 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 クエリを使います。「障害ポーリング」も参照。

す

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。

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、コンテンツメント、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**」、「**ルールのベースの検出**」、および「**リストに基づいた検出**」も参照してください。

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、モニタリングの設定、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せん。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 / サーバー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 デバイスを經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 がモニタリング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、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以下の階層型ユーザー ロールがあります：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。「ユーザー アカウント」も参照。

り

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。

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。

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

ロール

ユーザーロールを参照してください。

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。

索引

符号

<resource_group>.cntl.log ファイル
 HP-UX, 228
 Linux, 228
/etc/hosts, 209

A

AlarmPoint

 Java Client, 371
 エージェント, 372
 クライアント, 372
 サーバー, 371

AlarmPoint 統合

 AlarmPoint Mobile Gateway
 概要, 373 to 374
 サポートされるバージョン, 373
 使用法, 374
 ドキュメント, 374
 トラブルシューティング, 375
 無効化, 375
 有効化, 374

AlarmPoint プラットフォーム

 概要, 370 to 371
 サポートされるバージョン, 371
 使用法, 372
 ドキュメント, 371
 トラブルシューティング, 373
 無効化, 373
 有効化, 371 to 372

APAgent (AlarmPoint), 372

APClient (AlarmPoint), 372

Application_A.log ファイル, 229

ARP キャッシュ, 61

Asset Manager と NNMi の統合

 使用法, 390
 トラブルシューティング, 390
 無効化, 390
 有効化, 390

Asset Manager 統合

 サポートされるバージョン, 390
 使用法, 390
 ドキュメント, 390
 トラブルシューティング, 390
 無効化, 390
 有効化, 390

B

BAC My BSM 統合

 概要, 391 to 392
 カスタム ポートレットの作成, 395 to 398
 シングル サインオン の設定, 398
 デフォルト モジュール, 392 to 393
 デモ ポートレット の設定, 394
 ドキュメント, 392
 トラブルシューティング, 398
 パラメータ, 400 to 401
 ポータル の説明, 391
 レポート のトラブルシューティング, 399

BAC 初期化ストリング, 109

BAC と NNMi の統合

 SSO の設定, 109 to 110

BAC と NNMi の統合、My BSM

 新しいポートレットの作成, 395 to 398
 概要, 391 to 392
 シングル サインオン の設定, 398
 デフォルト モジュール, 392 to 393
 デモ ポートレット の設定, 394
 ドキュメント, 392
 トラブルシューティング, 398
 パラメータ, 400 to 401

BAC 統合

 SSO の作成, 109 to 110

BIND, 209

BSM、「BSM トポロジ統合」を参照

BSM と NNMi の統合、トポロジ
サポートされるバージョン, 404
使用法, 405
説明, 403
ドキュメント, 404
トポロジフィルタ, 408
トラブルシューティング, 406
パラメータ, 406 to 409
変更, 405
無効化, 406
有効化, 404
利点, 403

BSM トポロジ統合
サポートされるバージョン, 404
使用法, 405
説明, 403
ドキュメント, 404
トポロジフィルタ, 408
トラブルシューティング, 406
パラメータ, 406 to 409
変更, 405
無効化, 406
有効化, 404
利点, 403

Business Availability Center、「BAC My BSM 統合」
を参照

Business Service Management、「BSM トポロジ統
合」を参照

C

CIA, 359

Cisco

スイッチ
階層, 39
ノードグループの定義, 38
ルーター
階層, 39
ノードグループの定義, 38

CiscoWorks LMS 統合

サポートされるバージョン, 378
使用法, 379
説明, 377
ドキュメント, 378
トラブルシューティング, 380
パラメータ, 381 to 382
変更, 380
無効化, 380
有効化, 378 to 379
利点, 377

Cisco。「CiscoWorks LMS 統合」を参照
CiscoWorks LAN Management Solution
「CiscoWorks LMS 統合」を参照

ClarusIPC Plus+ 統合

NNM iSPI for IP Telephony との
概要, 385 to 386
サポートされるバージョン, 386
使用法, 387
ドキュメント, 386
トラブルシューティング, 387
無効化, 387
有効化, 386

NNMi との

概要, 383 to 384
サポートされるバージョン, 384
使用法, 384
ドキュメント, 384
トラブルシューティング, 385
無効化, 384
有効化, 384

ClarusIPC Plus+ の統合

NNM iSPI for IP Telephony との
概要, 385 to 386
使用法, 387
トラブルシューティング, 387
無効化, 387
有効化, 386

NNMi との

概要, 383 to 384
使用法, 384
トラブルシューティング, 385
無効化, 384
有効化, 384

Clarus Systems ClarusIPC Plus+、「ClarusIPC
Plus+ 統合」を参照

Client、AlarmPoint Java, 371

cluster.exe コマンド, 206

cluster.log ファイル, 228

Cluster Manager プロセス, 174

Cluster Member プロセス, 174

cmcluster ファイル, 228

ワークスペース

状態ポーリングの設定, 74

状態ポーリングの評価, 76

CPU リリース, 79

D

diagnostics、NA の設定 , 416
DiskGroup_A.log ファイル , 229
DNS, 209

E

Event Configurator ウィンドウ、NNM 6.x/7.x, 355,
365
ext2 共有ディスク フォーマット
HA, 198

F

FORWARD フィールド、NNM 6.x/7.x イベント
設定 , 356
FQDN, 108

G

GUI。NNMi コンソールを参照
コンソール。NNMi コンソールを参照

H

HA_nnmhaserver.log ファイル , 228
haconfigure.log ファイル , 228
HA 下での NNMi の 8.11 へのアップグレード ,
217 to 220
HA クラスタ
IP アドレスの変更
NNMi, 208 to 211
NNMi のアップグレード , 217 to 220
アーキテクチャ , 191
概念 , 191
起動の問題
nmsdbmgr, 224
NNMi, 223
pmd, 224
共有データ , 205 to 206
サポート対象の製品 , 190
シナリオ , 193
設定
NNMi, 197 to 202
情報、NNMi, 197
スクリプト , 226
ファイル , 226
マンページ , 196
リファレンス ページ , 196

設定解除
NNMi, 212 to 215
設定のトラブルシューティング , 221
説明 , 189
前提条件 , 190
パッチ
NNMi, 216
ホスト名の変更
NNMi, 208 to 211
メンテナンス
NNMi, 208 to 211
アドオン iSPI, 211
メンテナンス モード , 208
用語 , 192
ライセンス , 207

HA クラスタの設定解除
NNMi, 212 to 215
HA クラスタのメンテナンス , 208
HA クラスタ用の NNMi の再有効化 , 223
高可用性クラスタ 「HA クラスタ」を参照
HA 設定 , 226
HA 用のクラスタ アーキテクチャ , 191
HA 用のメンテナンス モード , 208
HA リソース グループ
起動できない , 222
設定
NNMi, 197
説明 , 192
停止
NNMi, 214
hostname コマンド , 209
HP Asset Manager、「Asset Manager 統合」を参照
HP BSM、「BSM トポロジ統合」を参照
HP Business Service Management、「BSM トポロジ
統合」を参照
HP Network Automation、「NA 統合」を参照
HPOM 統合、エージェント実装
サポートされるバージョン , 461
HPOM と NNMi の統合
Web サービス実装
インシデントの同期 , 476
概要 , 475
使用法 , 481
統合動作 , 490

ドキュメント, 477
トラブルシューティング, 483 to 487
パラメータ, 488 to 493
変更, 482
無効化, 483
有効化, 479
利点, 476

エージェント実装

概要, 460
使用法, 465
ドキュメント, 461
トラブルシューティング, 468 to 470
パラメータ, 471 to 474
変更, 466
無効化, 467
利点, 460

HPOM 統合

Web サービス実装

インシデントの同期, 476
概要, 475
使用法, 481
動作, 490
ドキュメント, 477
トラブルシューティング, 483 to 487
パラメータ, 488 to 493
変更, 482
無効化, 483
有効化、UNIX, 479
有効化、Windows, 477
利点, 476

エージェント実装

エージェントのインストール順序, 31
概要, 460
使用法, 465
ドキュメント, 461
トラブルシューティング, 468 to 470
パラメータ, 471 to 474
変更, 466
無効化, 467
有効化, 461
利点, 460

HP Operations Manager、「HPOM 統合」を参照

HP Performance Insight, 31

HP ProCurve Manager Plus、「PCM Plus 統合」を参照

HP ServiceGuard

HP-UX, 190
Linux, 190

HP ServiceGuard

HA リソース グループ, 192

HP SIM、「SIM 統合」を参照

HP Systems Insight Manager、「SIM 統合」を参照

HP Universal Configuration Management

Database、「UCMDB 統合」を参照

HP-UX

HP ServiceGuard, 190

NIS, 209

nnmharg.ovpl スクリプト, 227

アクティブ サーバー, 174

仮想ホスト, 198

共有ディスクの設定, 206

共有ディスク フォーマット

Ha, 198

ログ ファイル, 228

HP ルート分析管理システム、「RAMS MPLS WAN

統合」を参照

HTTPS プロトコル

デフォルト ポート, 517

I

IBM Tivoli Netcool/OMNIBus、「Netcool ソフトウェア用 NNMi 統合モジュール」を参照

ICMP

State Poller, 47

アドレス モニタリング, 73

トラフィックの無効化, 47

プロトコル, 43

要求, 53

ipNoLookup.conf ファイル, 319

IP アドレス

HA 用に変更

NNMi, 208 to 211

NNMi 管理サーバーの変更, 276

範囲, 62 to 65

iSPI

NNM iSPI for Performance レポートの URL, 395

アプリケーション フェイルオーバー, 180

HP NNM iSPI NET。「iSPI」を参照

NNM iSPI NET。「iSPI」を参照

SPI。「iSPI」を参照

IWS、HPOM, 475

J

Java Client、AlarmPoint, 371

Java Runtime Environment、インストールする、
358

jboss

アプリケーション サーバー、173
ディレクトリ、245

jbossServer.log ファイル

HP-UX, 228
Linux, 228
Solaris, 229
UNIX, 224
Windows

HA の設定、228
pmd のトラブルシューティング、224

L

Launcher、NNM 6.x/7.x, 364

ldap.properties ファイル、134

LDAP、NNMi との統合、113

license.txt ファイル

アクティブなクラスター ノード、209
管理サーバー、276

LicFile.txt ファイル

licenses.txt のアップデート、207
バックアップする
NNMi データ、246
プライマリ クラスター ノード、199

Linux

HP ServiceGuard, 190
NIS, 209
nnmharg.ovpl, 227
仮想ホスト、198
共有ディスクの設定、206
共有ディスク フォーマット
HA, 198

lvm2 共有ディスク フォーマット
HA, 198

lwssofmconf.xml file, 107, 109, 147

M

messages* ログ ファイル

Linux, 228
Solaris, 229

MIB II 変数、74

MIB ブラウザ

NNM 6.x/7.x, 364
URL 例、360

Microsoft Cluster Services

HA リソース グループ、192
ダイナミック ディスク、206

Microsoft クラスタ サービス

HA クラスタ、190
nnmhamscs.vbs スクリプト、227

Microsoft フェールオーバー クラスタリング

HA クラスタ、190
HA リソース グループ、192
ダイナミック ディスク、206

Mount_A.log ファイル、229

MTTR, 440

My BSM、「BAC My BSM 統合」を参照

N

NA インシデント アクションの表示、417

NA インベントリへの NNMi デバイスのインポート、
419

NA、インベントリへの NNMi デバイスのイン
ポート、419

NA と NNMi の統合

概要、411 to 413
使用法、415 to 420
ドキュメント、413
トラブルシューティング、420
パラメータ、423 to 424
変更、420
無効化、420
有効化、413 to 415
利点、412

NA 統合

NNMi コネクタ、413
URL アクション、415
概要、411 to 413
サポートされるバージョン、412
使用法、415 to 420
動作、424
ドキュメント、413
トラブルシューティング、420
パラメータ、423 to 424
変更、420
無効化、420
有効化、413 to 415
利点、412

Netcool/OBNIbus と NNMi の統合

- 概要, 495
- サポートされるバージョン, 496
- 使用法, 500
- ドキュメント, 497
- トラブルシューティング, 502 to 503
- パラメータ, 504 to 508
- 変更, 501
- 無効化, 501
- 利点, 496

Netcool ソフトウェア用 NNMi 統合モジュール

- 概要, 495
- 使用法, 500
- ドキュメント, 497
- トラブルシューティング, 502 to 503
- パラメータ, 504 to 508
- 変更, 501
- 無効化, 501
- 利点, 496

netmon.cmstr ファイル, 316

netmon.noDiscover ファイル, 328

NetScout Systems nGenius Performance Manager、
nGenius Performance Manager 統合を参照

Network Automation、「NA 統合」を参照

nGeniusNNM8.zip ファイル, 441

nGenius Performance Manager と NNMi の統合

- 使用法, 442
- トラブルシューティング, 440 to 442
- 無効化, 442
- 有効化, 441

nGenius Performance Manager 統合

- サポートされるバージョン, 441
- 使用法, 442
- ドキュメント, 441
- トラブルシューティング, 440 to 442
- 無効化, 442
- 有効化, 441

NIS, 209

nmsdbmgr.log ファイル

- HP-UX, 228
- Linux, 228
- Solaris, 229
- Windows, 228

nmsdbmgr サービス

- 起動の問題, 224
- ディスク フェイルオーバー, 224

NNM 6.x/7.x

NNMi からのデータ収集, 313 to 315

NNMi との統合

- イベント転送, 354 to 358
- テスト, 361 to 364
- トラブルシューティング, 364
- リモート ビューの起動, 358 to 361

NNMi へのアップグレード

- OVW マップ, 344 to 346
- SNMP, 315 to 321
- イベント, 337 to 343
- オプション, 310 to 312
- カスタム スクリプト, 347
- 検出, 321 to 331
- ステータス モニタリング, 331 to 337
- 提案するパス, 285, 287, 295, 309
- フェーズ, 310
- ホーム ベース コンテナ ビュー, 346 to 347

イベント ノードリストの設定, 356

イベント モニタリングのカスタマイズ, 306

管理ステーション, 361 to 363

ステータス モニタリング, 304

動的ビュー, 359

ネットワーク検出, 301

ビュー, 358

NNM 6.x/7.x イベント ビュー, 364

NNM 6.x/7.x からのアップグレード

- OVW マップ, 344 to 346
- アップグレードの割合を管理, 353
- イベント, 337 to 343
- オプション, 310 to 312
- カスタム スクリプト, 347
- 検出, 321 to 331
- ステータス モニタリング, 331 to 337
- 提案するパス, 285, 287, 295, 309
- フェーズ, 310
- ホーム ベース コンテナ ビュー, 346 to 347

NNM 6.x/7.x 管理ステーション設定の保存, 357

NNM 6.x/7.x と NNMi の統合

- イベント転送, 354 to 358
- テスト, 361 to 364
- トラブルシューティング, 364
- リモート ビューの起動, 358 to 361

NNM 6.x/7.x 動的ビューを起動, 364

NNM 6.x/7.x を追加

- 管理ステーション, 356
- ビュー, 360

nnm.envvars.bat コマンド, 512 to 515

nnm.envvars.sh コマンド, 512
 nnmbackup.ovpl
 説明, 243
 nnmbackupembdb.ovpl
 説明, 243
 nnmcluster コマンド, 177
 nnmcommconf.ovpl コマンド, 52
 nnmconfigexport.ovpl
 NNM 6.x/7.x 管理ステーション設定の保存, 357
 SNMPv3 資格情報, 36
 設定の XML への出力, 272
 nnmconfigimport.ovpl コマンド, 272
 nnmcontainerlist.csv ファイル, 346
 nnmdatareplicator.conf ファイル, 226
 nnmdatareplicator.ovpl こまんど, 206
 nnmdatareplicator.ovpl すくりふと, 227
 nnm Dumpevents コマンド, 364
 nnmhaclusterinfo.ovpl スクリプト, 226
 nnmhaconfigure.ovpl
 コマンド, 224
 nnmhaconfigure.ovpl すくりふと, 226
 nnmhadisk.ovpl コマンド
 nmsdbmgr のトラブルシューティング, 224
 設定ファイルの複製, 205
 トラブルシューティング, 224
 nnmhadisk.ovpl スクリプト, 227
 nnmhamonitor.ovpl スクリプト, 227
 nnmhamscs.vbs スクリプト, 227
 nnmharg.ovpl スクリプト, 227
 nnmhargconfigure.ovpl こまんど, 222
 nnmhargconfigure.ovpl すくりふと, 227
 nnmhastart.ovpl スクリプト, 227
 nnmhastartrg.ovpl スクリプト, 227
 nnmhastop.ovpl スクリプト, 227
 nnmhastoprg.ovpl スクリプト, 227
 nnmhaunconfigure.ovpl スクリプト, 226
 NNMi 9.00 へのアップグレード, 283
 NNMi Oracle データの移行, 293
 Red Hat Linux 5.2 または 5.3 への移行, 289
 同じ NNMi 管理サーバー, 285
 機能面の相違点, 295, 296
 サポート対象のアップグレード, 283
 設定面の相違点, 295
 別の NNMi 管理サーバー, 287
 nnmimport.bat コマンド, 420
 nnmimport.sh コマンド, 420
 NNMi iSPI for Metrics、「iSPI」を参照
 NNMi クイックスタート設定ウィザード, 21
 NNMi コンソール
 HPOM からのアクセス
 Web サービス実装, 476
 エージェント実装, 460
 Netcool イベント ビューアからのアクセス, 496
 NNM 6.x/7.x インシデント設定を確認する, 357
 URL, 395
 サインオフ, 107
 トランザクションベースの更新, 36
 NNMi 初期化ストリング, 109
 NNMi 設定移動の準備, 271
 NNMi に AlarmPoint Mobile Gateway を統合
 概要, 373 to 374
 使用法, 374
 トラブルシューティング, 375
 無効化, 375
 有効化, 374
 NNMi に AlarmPoint を統合
 概要, 370 to 371
 使用法, 372
 トラブルシューティング, 373
 無効化, 373
 有効化, 371 to 372
 NNMi に CiscoWorks LMS を統合
 サポートされるバージョン, 378
 使用法, 379
 説明, 377
 ドキュメント, 378
 トラブルシューティング, 380
 パラメータ, 381 to 382
 変更, 380
 無効化, 380
 有効化, 378 to 379
 利点, 377
 NNMi に PCM Plus を統合
 使用法, 426
 トラブルシューティング, 426
 無効化, 426
 有効化, 426

NNMi に SIM を統合

- サポートされるバージョン, 430
- 使用法, 432
- 説明, 430
- ドキュメント, 430
- トラブルシューティング, 433
- パラメータ, 433 to 435
- 変更, 432
- 無効化, 432
- 有効化, 430 to 431
- 利点, 430

NNMi に SNMP トラップ レシーバを統合

- 概要, 444
- 使用法, 447
- ドキュメント, 445
- トラブルシューティング, 451
- パラメータ, 454 to 458
- 変更, 450
- 無効化, 451
- 有効化, 445
- 利点, 444

NNMi に UCMDB を統合

- サポートされるバージョン, 438
- 使用法, 438
- 説明, 437
- ドキュメント, 438
- トラブルシューティング, 438
- パラメータ, 438
- 変更, 438
- 無効化, 438
- 利点, 437

NNMi ノースバウンド インタフェース

- 概要, 444
- 使用法, 447
- ドキュメント, 445
- トラブルシューティング, 451
- パラメータ, 454 to 458
- 変更, 450
- 無効化, 451
- 有効化, 445
- 利点, 444

NNMi の移動

- 管理サーバー, 271
- 設定, 272
- 設定および組み込みデータベース, 272

NNMi へのアクセス, 108

nnmlicense.ovpl コマンド

- HA クラスタでの NNMi ライセンス, 207 to 209
- NNM 製品, 207
- 管理サーバーの変更, 276

nnmloadseeds.ovpl コマンド, 63

nnmofficialfqdn.ovpl コマンド, 108

nnmresetembdb.ovpl

- 説明, 244

nnmrestore.ovpl

- 説明, 243

nnmrestoreembdb.ovpl

- 説明, 243

nnmsetofficialfqdn.ovpl コマンド, 108

nnmtopodump.ovpl コマンド, 347

NOC, 317

NOC_Demo_Portal_iSPIPerf.xml ファイル, 392 to 394

NOC_Demo_Portal.xml ファイル, 392 to 394

No Device Profile, 321

Nortel

- スイッチ
 - 階層, 39
 - ノード グループの定義, 38
- ルーター
 - 階層, 39
 - ノード グループの定義, 38

northbound インタフェース、NNMi northbound インタフェースを参照

nslookup コマンド, 197

O

oid_to_sym file, 321

OLDsyslog.log ファイル, 228

OM、「HPOM 統合」を参照

om.hp.ov.nms.cluster* パラメータ, 178

OpenView アプリケーション サーバー、NNM 6.x/7.x, 359

Operations Manager、「HPOM 統合」を参照

Oracle データベースと HA, 203

OV_Message イベント、NNM 6.x/7.x, 363

ov.conf ファイル

- HA 設定, 226
- nmsdbmgr のトラブルシューティング, 224

ovaddr コマンド、NNM 6.x/7.x, 359

ovalarm の URL 例, 360
ovas、NNM 6.x/7.x, 359
ovdumpevents コマンド、NNM 6.x/7.x, 364
ovet*.log ファイル
 HP-UX, 228
OV jovw の URL 例, 360
OV Launcher の URL 例, 360
ovspmd.log ファイル
 HP-UX, 228
 Linux, 228
 Solaris, 229
 Windows, 228
ovspmd サービス、トラブルシューティング, 223
ovstart コマンド
 アプリケーション サーバー, 177 to 180
 トラブルシューティング, 223
ovstop コマンド
 アプリケーション フェイルオーバー, 177 to 180
 トラブルシューティング, 223
 フェイルオーバーを行わせないように
 HA 下での NNMi の 8.11 へのアップグレード
 , 218
 HA クラスタでの NNMi の停止, 211, 216
ovtopodump コマンド、NNM 6.x/7.x, 362
ovtopofix コマンド、NNM 6.x/7.x, 362
ovwId、ノード詳細、使用している, 361
ovw、NNM 6.x/7.x, 364
OVW、NNM 6.x/7.x からのアップグレード,
 344 to 346
OV アプリケーション サーバー、NNM 6.x/7.x, 359

P

PCM Plus 統合
 サポートされるバージョン, 426
 使用法, 426
 ドキュメント, 426
 トラブルシューティング, 426
 無効化, 426
 有効化, 426
PC、管理対象としない, 55
Performance Insight, 31
PERL5LIB、環境変数, 344

ping プロトコル
 スニープ, 59
 デバイスの検索, 43
 要求, 74
pmd の起動の問題, 224
postgres.log ファイル
 HP-UX, 228
 Linux, 228
 Solaris, 229
 Windows, 228
Postgres データベース, 174

R

RAMS MPLS WAN と NNMi の統合
 使用法, 428
 トラブルシューティング, 428
 パラメータ, 428
 無効化, 428
 有効化, 428
RAMS MPLS WAN 統合
 サポートされるバージョン, 427
 使用法, 428
 ドキュメント, 428
 トラブルシューティング, 428
 パラメータ, 428
 無効化, 428
 有効化, 428
recovery.conf ファイル, 178
remsh コマンド, 190
Report Presenter の URL 例, 360

S

sendMsg.ovpl コマンド、NNM 6.x/7.x, 361 to 363
SIM 統合
 サポートされるバージョン, 430
 使用法, 432
 説明, 430
 ドキュメント, 430
 トラブルシューティング, 433
 パラメータ, 433 to 435
 変更, 432
 無効化, 432
 有効化, 430 to 431
 利点, 430
SLA, 73

SNMP

- Data Presenter, 360
- MIB ディレクトリ, 245, 246
- NNMi へのアップグレード, 315 to 321
- 監視, 74
- コミュニティ文字列, 45
- コンポーネント稼働状態, 74
- 設定
 - アクセス, 315 to 321
 - 設定の調整, 53
 - 通信の問題, 64
 - デバイス アクセス, 52
 - ノードの設定, 51
 - バージョンの優先, 46
 - プロトコル, 43
 - 無効化
 - 通信, 50
 - トラフィック, 47
 - 要求, 53

snmpout.txt ファイル, 316

snmptrap コマンド、NNM 6.x/7.x, 363

SNMP 情報のアップグレード, 315 to 321

Solaris

- NIS+, 209
- nnmharg.ovpl スクリプト, 227
- nnmhargconfigure.ovpl
 - コマンド, 222
 - スクリプト, 227
- Veritas Cluster Server, 190
- 仮想ホスト
 - NNMi, 198
 - 共有ディスクの設定, 206
 - 共有ディスク フォーマット
 - Ha, 198

ssh コマンド, 190

SSO

- BAC My BSM 統合の設定, 398
- BAC 統合に作成, 109 to 110
- アクセス, 108

State Poller

- ICMP, 47
- 概念, 67 to 68
- 確認する
 - 稼働状態統計, 78
 - 通信設定, 52
- 計画作成, 68 to 74
- 設定, 74 to 76
- 設定の評価, 76 to 78
- 調整, 78 to 79

syslog.log ファイル, 228

T

tar ファイル, 247

Top-N CPU 使用率ポートレット, 393

Top-N メモリ使用率ポートレット, 393

traceroute コマンド, 50

trapd.conf の編集, 356

trapd.conf ファイル、編集する, 356

trapd.conf を手動で編集する, 356

U

UCMDB 統合

- サポートされるバージョン, 438
- 使用法, 438
- 説明, 437
- ドキュメント, 438
- トラブルシューティング, 438
- パラメータ, 438
- 変更, 438
- 無効化, 438
- 利点, 437

Universal Configuration Management Database、
「UCMDB 統合」を参照

UNIX

HA 設定

ファイル, 226

ipNoLookup.conf コマンド

検出からアドレスを除外, 328

LicFile.txt ファイル

HA クラスタ ライセンスのインストール, 207

プライマリ HA クラスタ ノードの設定, 199

netmon.cmstr コマンド, 316

nnm8EventForwardDestinations.txt ファイル,
355

nnm.envvars.sh コマンド, 512

nnmtrapd ログ ファイル, 224

pmd ログ ファイル, 224

remsh コマンド, 190

sendMsg.ovpl コマンド, 363

ssh コマンド, 190

trapd.conf ファイル, 356

環境変数

インストール, 22

管理, 514

共有ディスクのディレクトリ, 205

ディスク グループ
NNMi, 198
ポート番号, 360
ボリューム グループ
NNMi, 199
マウントポイント
NNMi, 199

URL

NNM iSPI for Performance レポート, 395
NNMi コンソール, 395
選択が必要, 361
選択を必要としない, 360

URL アクセス、SSO, 108

UUID、ノード詳細、使用している, 361

V

Veritas Cluster Server, 190
HA リソース グループ, 192
nmmharg.ovpl スクリプト, 227

Volume_A.log ファイル, 229

vxfs 共有ディスク フォーマット
HA, 198

W

Web サーバー
AlarmPoint, 371
ポート, 360

Windows

HA 設定
スクリプト, 226
ファイル, 226
LicFile.txt ファイル
HA クラスタ ライセンスのインストール, 207
プライマリ HA クラスタ ノードの設定, 199
Microsoft Cluster Services, 190
Microsoft フェールオーバー クラスタリング, 190
netmon.cmstr コマンド, 316
netmon.noDiscover コマンド, 328
nmm8EventForwardDestinations.txt ファイル,
355
nmm.envvars.bat コマンド, 512 to 515
nmmhargconfigure.ovpl コマンド, 222
nmmtrapd ログ ファイル, 224
pmd ログ ファイル, 224
sendMsg.ovpl コマンド, 363
trapd.conf ファイル, 356
仮想ホスト
NNMi, 198

環境変数
アプリケーション フェイルオーバー, 174
インストール, 22
管理, 512 to 515
共有ディスクの設定, 206
共有ディスクのディレクトリ, 205
共有ディスク フォーマット
HA, 198
ポート番号, 360
マウントポイント
NNMi, 199

X

XML ファイル, 42, 272

xnmevents コマンド、NNM 6.x/7.x, 355

XServer, 356

あ

アーキテクチャ、HA クラスタ, 191

アクション
NA 統合, 415

アクション、NA 統合
インシデント, 416
インシデントの表示, 417
追加, 415

アクション メニュー, 364

アクセス資格認定
コミュニティ文字列, 45
設定, 44

アクティブ
サーバー, 173
プロトコル, 50

アップグレード ツール
データ インポート

nmmconnect.ovpl, 330
nmmdiscof.cfg.ovpl, 328
nmmincidentcfg.ovpl, 338
nmmloadnodegroups.ovpl, 345, 347
nmmloadseeds.ovpl, 324, 330
nmmmibmigration.ovpl, 338, 350
nmmtrapdMerge.ovpl, 340, 351
nmmtrapload.ovpl, 338, 351
restoreMigration.ovpl, 314, 350
snmpCapture.ovpl, 316, 346, 351

データ収集
archiveMigration.ovpl, 314, 348
captureLocale.ovpl, 348
createMigrationDirs.ovpl, 314, 348
hostnolookup.ovpl, 348

- nnmetmapmigration.ovpl, 350
- nnmmapmigration.ovpl, 344, 349
- nnmmigration.ovpl, 319, 321, 348
- nnmtopodump.ovpl, 347, 349
- ovmapdump.ovpl, 349
- ovmibmigration.ovpl, 349
- ovwdbDump.ovpl, 349
- snmpCapture.ovpl, 349
- trapdConfNodes.ovpl, 349

- アドレス、管理サーバー
 - 確認する, 52
 - 変更, 276
 - 優先, 47

- アプリケーション
 - アラート生成, 369
 - サーバー、AlarmPoint, 371
 - フェイルオーバー
 - iSPI, 180
 - NNMi の設定, 175 to 177
 - インシデント, 180
 - 機能, 177 to 180
 - セットアップ, 174
 - 統合アプリケーション, 182
 - マルチサブネットでの設定, 187
 - 例, 179

- アプリケーションアラート アラーム カテゴリ、
NNM 6.x/7.x, 358

- アプリケーションステータス インシデント カテゴリ、
358

- アプリケーションフェイルオーバーのセットアップ、
174

- アラート生成アプリケーション, 369

- アラーム、NNM 6.x/7.x
 - カテゴリ, 357
 - 動的ビューを起動, 364
 - マッピング, 357 to 358

い

- イベント
 - NNM 6.x/7.x からのアップグレード, 337 to 343
 - OV_Message、NNM 6.x/7.x, 363
 - インタフェース停止 / 開始のテスト イベント生成
, 362
 - 監視
 - 概念, 308
 - カスタマイズ, 306
 - 削減, 356
 - 転送
 - 確認する, 361
 - 管理サーバー, 354

- イベント設定ウィンドウ、NNM 6.x/7.x, 354

- イベント モニタリングのカスタマイズ, 306

- インシデント

- HPOM への転送

- Web サービス実装, 475

- エージェント実装, 460

- NA アクションの表示, 417

- Netcool/OMNIbus への転送, 496

- NNM 6.x/7.x を NNMi コンソールで確認する,
357

- SNMP トラップ レシーバへの転送, 444

- 概念, 81 to 87

- カテゴリ, 358

- 計画作成, 88

- 更新の同期

- HPOM Web サービス実装, 476

- 設定, 89

- 設定の評価, 89

- 調整, 89

- フィルタ, 491 to 493

- ブラウザ, 353

- インシデント Web サービス、HPOM, 475

- [インシデントの設定] フォーム

- 設定の確認, 357

- インシデントの転送

- HPOM へ

- Web サービス実装, 475

- エージェント実装, 460

- Netcool/OMNIbus への転送, 496

- SNMP トラップ レシーバ, 444

- インシデント ワークスペース, 361

- インストール

- AlarmPoint Java Client, 371

- HA クラスタ用のライセンス, 207

- HP Performance Insight, 31

- Java Runtime Environment, 358

- パブリック キー証明書, 95

- インタフェース

- HA 設定の仮想ホスト ネットワーク

- NNMi, 198

- 開始 / 停止テスト イベント生成, 362

- 監視, 69

- グループ

- 確認する, 76

- 事前設定, 72

- 設定, 74

- フィルタリング, 41

- 目的, 37

設定, 41
モデル, 36
モニタリングの設定, 75
インタフェース開始/停止のテスト イベント生成, 362
[インタフェース グループ] フォーム, 71
[インタフェース グループ] ワークスペース, 71
[インタフェースの設定] フォーム, 79
インタラクティブ モード、アプリケーション フェイ
ルオーバー, 177
インベントリ、NA への NNMi デバイスのイン
ポート, 419

う

ウィザード、NNMi クイックスタート設定, 21
ウィンドウ、システム情報, 78

え

エラー アラーム カテゴリ、NNM 6.x/7.x, 358

お

オブジェクト グループ、定義の作成, 72
オプション、NNM 6.x/7.x からのアップグレード,
310 to 312
オフライン バックアップ, 244
オンライン バックアップ, 244

か

解決、名前の制限, 319
階層、ノード グループ, 39
概念
HA, 191
イベント モニタリング, 308
インシデント, 81 to 87
検出, 303
状態ポーリング, 67 to 68
ステータス モニタリング, 306
設定, 35
通信, 44
外部リレーショナル データベース, 243
拡張モニタリング, 69
確認
モニタリングの設定, 76 to 77

確認する

NNM 6.x/7.x インシデント設定, 357
SNMP 用に設定されたノード, 51
State Poller
稼働状態統計, 78
通信設定, 52
イベント転送, 361
インタフェース グループ, 76
管理 IP アドレス, 52
順序番号, 75
通信設定, 52
デバイスについての SNMP アクセス, 52
デフォルト設定, 76
ネットワーク
接続, 64
モニタリングの設定, 76
ノード グループ, 76
カスタム インシデント属性, 359
カスタム スクリプト、NNM 6.x/7.x からのアップグ
レード, 347
仮想 IP アドレスのサポート, 190
仮想ホスト、HA 設定
ネットマスク
NNMi, 198
ネットワーク インタフェース
NNMi, 198
短い名前
NNMi, 197
カテゴリのマッピング, 357
環境、テスト, 21
環境変数
UNIX
インストール, 22
管理, 514
Windows
アプリケーション フェイルオーバー, 174
インストール, 22
管理, 512 to 515
概要, 511
監視
イベント
概念, 308
カスタマイズ, 306
インタフェース, 75
拡張, 69
ステータス
概念, 306
設定, 304

- 設定, 77
 - 設定, 41
 - バッチ処理, 74
 - ネットワーク
 - 設定の確認, 76
 - ノード, 79
 - ノードの設定, 75
- 管理
 - アドレス
 - 確認する, 52
 - 優先, 47
 - サーバー
 - AlarmPoint Java Client のインストール, 371
 - NNM 6.x/7.x イベントの転送, 354
 - NNMi の移動, 271
 - ステーション
 - NNM 6.x/7.x エンティティを作成, 359
 - NNM 6.x/7.x をトポロジに追加, 356
 - 設定を保存, 357
- 管理ステーション フォーム, 359
- 関連ドキュメント, 24

き

- キー、パブリック, 95
- 基幹、ネットワーク, 55
- ルール、自動検出
 - 順序, 58
 - 評価, 65 to 66
- ルールベース検出
 - 概要, 57
 - 有効化, 65
- 起動
 - HA メンテナンス後
 - NNMi, 211
 - HA リソース グループ, 222
- 起動の問題
 - nmsdbmgr, 224
 - NNMi, 223
 - pmd, 224
- 基本共有ディスク フォーマット
 - HA, 198
- キャッシュ、ARP, 61
- 共存
 - HP Operations Manager エージェント, 31
 - HP Performance Insight, 31
- 共有 HA データ, 205 to 206
- 共有される設定データ, 246

- 共有ディスク
 - サポート, 190
 - 設定, 206
 - データ, 205
 - データ ファイルのコピー, 197
 - ファイル, 224
 - マウント解除
 - NNMi, 214
- 共有ディスクのマウント解除
 - NNMi, 214
- 共有ファイル システムのタイプ、HA 設定
 - NNMi, 198

く

- クイックスタート設定ウィザード, 21
- 組み込みデータベース
 - バックアップおよびリストアする, 249
 - リレーショナル, 243
- クラスタ ノード、HA の設定
 - NNMi
 - セカンダリ, 201
 - プライマリ, 199 to 201
- クラスタ マネージャ、アプリケーション フェイルオーバーのモード, 177
- グループ
 - インタフェース
 - フィルタリング, 41
 - 目的, 37
 - ディスク
 - HA 用の NNMi, 198
 - ノード, 37
 - ボリューム
 - HA 用の NNMi, 199

け

- 計画作成
 - インシデント, 88
 - 状態ポーリング, 68 to 74
 - 通信, 48
 - ポーリング間隔, 73
- 検出
 - NNM 6.x/7.x
 - からのアップグレード, 321 to 331
 - 比較, 301
 - 再スタート, 42
 - 重要概念, 303
 - スイッチ, 65
 - スパイラル, 55

トランザクションベースの更新、例外, 36
ノードを削除, 64
パフォーマンス, 53
評価
 ルールベース検出, 65 to 66
 リストベース検出, 64
方法
 ルールベース検出, 57 to 58
 リストベース検出, 57
ルーター, 65

こ

恒久ライセンスのパスワード, 209

コマンド

cluster.exe, 206
hostname, 209
nnm.envvars.bat, 512 to 515
nnm.envvars.sh, 512
nnmcluster, 177
nnmcommconf.ovpl, 52
nnmconfigexport.ovpl
 NNM 6.x/7.x 管理ステーション設定の
 保存, 357
 SNMPv3 資格情報, 36
 設定の XML への出力, 272
nnmconfigimport.ovpl, 272
nnmdatareplicator.ovpl, 206
nnmdumpevents, 364
nnmhaconfigure.ovpl, 224
nnmhadisk.ovpl
 nmsdbmgr のトラブルシューティング, 224
 設定ファイルの複製, 205
nnmhargconfigure.ovpl, 222
nnmimport.bat, 420
nnmimport.sh, 420
nnmlicense.ovpl
 HA クラスタでの NNMi ライセンス,
 207 to 209
 管理サーバーの変更, 276
nnmloadseeds.ovpl, 63
nnmofficialfqdn.ovpl, 108
nnmsetofficialfqdn.ovpl, 108
nnmtopodump.ovpl, 347
nslookup, 197
ovaddr, 359
ovspmd, 223
ovstart
 アプリケーション フェイルオーバー,
 177 to 180
 トラブルシューティング, 223

ovstop
 アプリケーション フェイルオーバー,
 177 to 180
 トラブルシューティング, 223
 フェイルオーバーを行わせないように, 211,
 216, 218
ovtopodump, 362
ovtopofix, 362
remsh, 190
sendMsg.ovpl, 361 to 363
snmptrap, 363
ssh, 190
traceroute, 50
xnmevents, 355

コマンドスクリプト、NA の設定, 416

コマンドラインセキュリティ, 108

コマンドライン モード、アプリケーション フェイル
オーバー, 177

コミュニティ文字列
 アクセス資格認定, 45
 複数, 50

コンテインメント、ノード グループ, 39

コンテナ ビュー、NNM 6.x/7.x からのアップグレー
ド, 346 to 347

コンポーネント稼働状態モニタリング, 74 to 79

コンポーネント登録ファイル, 246

[コンポーネントの例外別 Top-N デバイス] ポート
レット, 393

さ

サーバー

AlarmPoint, 371
jboss, 173
アクティブ, 173

サービス レベル契約条項, 73

再試行

値, 50
設定, 44
調整, 53

再スタート

HA メンテナンス後
NNMi, 211
検出, 42

削減

イベント, 356
デフォルト コミュニティ文字列, 53
認証不合格, 53

削除

- 検出されたノード, 64
- ライセンス キー, 276

作成

- NNMi ポートレット, 395 to 398

作成者属性, 36

作成中

- NNM 6.x/7.x 管理ステーション エンティティ, 359
- オブジェクト グループ定義, 72
- 再使用可能なノード グループ, 73

サポートされるバージョン

- HA 製品, 190
- 統合されたアプリケーション
 - AlarmPoint, 371
 - AlarmPoint Mobile Gateway, 373
 - Asset Manager, 390
 - BAC My BSM, 392
 - BSM トポロジ, 404
 - CiscoWorks LMS, 378
 - ClarusIPC Plus+ と NNMi, 384
 - ClarusIPC Plus+ と NNM iSPI for IP Telephony, 386
 - HPOM エージェント実装, 461
 - NA, 412
 - Netcool/OMNIBus, 496
 - nGenius Performance Manager, 441
 - PCM Plus, 426
 - RAMS、MPLS WAN, 427
 - SIM, 430
 - UCMDB, 438
- ハードウェアとソフトウェア, 29

し

シード、ルールベース検出, 57

資格認定、アクセス

- コミュニティ文字列, 45
- 設定, 44

しきい値アラーム カテゴリ、NNM 6.x/7.x, 358

システム

- オブジェクト ID 範囲
 - 自動検出, 62
 - 評価, 66
- 共有ファイル タイプ、HA 設定
 - NNMi, 198
- デバイス対応マトリックス, 29
- リリース, 79

事前設定

- インタフェース グループ, 72
- ノード グループ, 73

自動検出ルールの順序, 58

シナリオ

- HA クラスタ, 193

主要操作マップ ポートレット, 393

順序属性

- 自動検出ルール, 58
- ベストプラクティス, 36

順序番号、確認, 75

順序、評価, 68

詳細、ノード, 361

状態、不整合なレイヤー 2 接続の特定, 417

証明書、パブリック キー, 95

初期化ストリング

- BAC, 109
- NNMi, 109

シングルサインオン、「SSO」を参照

す

スweep、ping, 59

スイッチ

- 階層, 39
- 検出, 65
- デフォルト, 66
- ノード グループの定義, 38

スクリプト

- HA 設定, 226
- NNM 6.x/7.x からのアップグレード, 347
- nnmhaclusterinfo.ovpl, 226
- データのリストア, 246
- バックアップ, 244 to 245

スタンバイ システム, 174

ステータス

- インシデント カテゴリ, 358

監視

- NNM 6.x/7.x からのアップグレード, 331 to 337
- 概念, 306
- 設定, 304
- ポーリング
 - 開始, 77
 - パフォーマンスの評価, 77 to 78

ステータス アラーム カテゴリ、NNM 6.x/7.x, 358

ステータス インシデント カテゴリ, 358

ステータス ポーリングの開始, 77

スパイラル検出, 55

せ

制限のある環境, 21

製品、HA, 190

セカンダリ HA クラスタ ノード

設定

NNMi, 201

設定情報, 197

接続、ネットワークを確認する, 64

設定

BAC My BSM

ポートレット, 394

HA クラスタ

NNMi, 197 to 202

HA クラスタ ノード、セカンダリ

NNMi, 201

HA クラスタ ノード、プライマリ

NNMi, 199 to 201

HA 情報

NNMi, 197

HA のトラブルシューティング, 221

NA diagnostics, 416

NNM 6.x/7.x

イベントの転送, 354

ビューを追加, 360

NNMi 移動の準備, 271

NNMi の移動, 272

SNMP

アクセス, 315 to 321

アクセス資格認定, 44

アプリケーション フェイルオーバー, 173

インシデント, 89

インシデント カテゴリ, 358

インタフェース

監視, 75

グループ, 74

概念, 35

監視, 77

ルールベース検出, 62

共有データ, 246

共有ディスク, 206

再試行, 44

状態ポーリング, 74 to 76

スクリプト、HA クラスタ, 226

設定, 41

タイムアウト, 44

通信, 51, 52

通信に意味のあるデフォルト, 48

デフォルトの確認, 76

トランザクションベースの更新, 36

ネットワーク モニタリングの確認, 76 to 77

ノード, 49

監視, 75

グループ, 74

比較

イベント モニタリングのカスタマイズ, 306

ステータス モニタリング, 304

ネットワーク検出, 301

ファイル

HA クラスタ, 226

HA 用のレプリケーション, 206

ポーリングの例, 69

保存

NNM 6.x/7.x 管理ステーション, 357

既存, 36

モニタリングのバッチ処理, 74

やり直し, 42

リストベース検出, 63

領域, 48

レベル, 44

ワークスペース, 359

設定アラーム カテゴリ、NNM 6.x/7.x, 358

設定、動作

HPOM 統合、Web サービス実装, 490

NA 統合, 424

設定の評価

検出, 64

通信, 51

設定のやり直し, 42

設定のリセット, 42

設定を評価する

インシデント, 89

状態ポーリング, 76 to 78

前提条件

HA クラスタ用の NNMi, 190

ソフトウェア, 29

ハードウェア, 29

そ

属性

作成者, 36

順序, 36

そのまま使用できる

BAC My BSM モジュール, 394

インシデントへの NA 統合変更, 416
ポーリング動作, 69

ソフトウェア
対応, 29
要件, 27

た

タイムアウト
値, 50
設定, 44
調整, 53
ネットワーク, 44

タスク フロー モデル, 35

ち

チェックリスト、ポーリング, 68

調整

インシデント, 89
状態ポーリング, 78 to 79
通信, 53

つ

追加のノード パック ライセンスを購入する, 64

通信

概念, 44
計画作成, 48
設定, 51, 52
設定の確認, 52
設定の評価, 51
設定領域, 48
調整, 53

通信設定に意味のあるデフォルト, 48

て

データ

共有
設定, 246
ディスク, 205
収集、State Poller, 74
収集の確認, 77
バックアップする
組み込みデータベースのみ, 249
スクリプト, 244 to 245
方針, 248 to 249
リストアする
組み込みデータベースのみ, 249
スクリプト, 246

データの収集
ステータス ポーリング
確認する, 77
データの選択, 74

データのリストア
組み込みデータベース, 249
スクリプト, 246

データ バックアップ
イベント領域, 245
設定領域, 244
トポロジ領域, 245

データベース

Postgres, 174
組み込みをバックアップする, 249
組み込みをリストアする, 249
トポロジ, 67
リセット, 42

データベース、組み込み
NNMi の移動, 272

データをバックアップする
組み込みデータベースのみ, 249
スクリプト, 244 to 245
方針, 248 to 249

デーモン モード、アプリケーション フェイルオー
バー, 177

停止

HA フェイルオーバーを行わせないように
NNMi, 211
HA リソース グループ
NNMi, 214

ディスク

共有
データ ファイルのコピー, 197
ディレクトリ, 205
グループ、HA 設定, 198
フェイルオーバー, 224

ディレクトリ サービス、NNMi との統合, 113

ディレクトリ サービス、NNMi ユーザー情報, 113

ディレクトリ サービス内の NNMi ロール, 113

ディレクトリ サービス内のパスワード, 113

ディレクトリ サービス内のユーザー名, 113

ディレクトリ。「場所」を参照

テスト

NNM 6.x/7.x
統合, 361
トラップ, 363

- 通信設定, 51
 - ラグタイム, 50
- テスト環境, 21
- デバイス
 - NA への NNMi のインポート, 419
 - SNMP アクセス, 52
 - フィルタ, 40
 - プロファイル
 - 概念, 40
 - 状態ポーリング, 73
- デバイスを検出から除外, 58
- デフォルト
 - BAC My BSM モジュール, 392 to 393
 - HTTPS ポート, 517
 - 意味のある、通信, 48
 - ルールベース検出, 62
 - 検出, 55
 - コミュニティ文字列, 53
 - スイッチ, 66
 - 設定, 41
 - 設定の確認, 76
 - ルーター, 66
- 転送、イベント
 - NNM 6.x/7.x から NNMi 管理サーバーへ, 354
 - 確認する, 361
- 転送先リストファイル, 355
- 転送されたインシデント、HPOM のトラブルシューティング
 - Web サービス実装, 483 to 486
 - エージェント実装, 468 to 470
- 転送されたインシデント、Netcool ソフトウェア用 NNMi 統合モジュールのトラブルシューティング, 502 to 503

と

- 同期、HPOM のトラブルシューティング、Web サービス実装, 486
- 統合
 - アプリケーション フェイルオーバー, 182
- 統合モジュール、HPOM, 475
- 動作
 - そのまま使用できるポーリング, 69
- 動作の設定
 - HPOM 統合、Web サービス実装, 490
 - NA 統合, 424

動的

- ディスク, 206
- ビュー
 - NNM 6.x/7.x, 359
 - NNMi, 364

ドキュメント

- AlarmPoint Mobile Gateway 統合, 374
- AlarmPoint 統合, 371
- Asset Manager 統合, 390
- BAC My BSM 統合, 392
- BSM トポロジ統合, 404
- CiscoWorks LMS 統合, 378
- ClarusIPC Plus+ 統合
 - NNM iSPI for IP Telephony との, 386
 - NNMi との, 384
- HPOM 統合
 - Web サービス実装, 477
 - エージェント実装, 461
- NA 統合, 413
- nGenius Performance Manager 統合, 441
- PCM Plus 統合, 426
- RAMS MPLS WAN 統合, 428
- SIM 統合, 430
- UCMDB 統合, 438
- 関連, 24
- ハードウェアとソフトウェアの要件、NNMi, 29
- 場所, 309

トポロジ

- NNM 6.x/7.x 管理ステーション, 356
- 概要 URL 例, 360
- データベース, 67
- 領域データ, 245

トポロジ フィルタ、BSM トポロジ統合, 408

ドメイン ネーム サービス, 209

トラストストア
出力例, 97

トラップ、NNM 6.x/7.x システムに対するテスト, 363

トラフィック
制御, 50
無効化, 47

トラフィックの制御, 50

トラブルシューティング

- AlarmPoint Mobile Gateway 統合, 375
- AlarmPoint 統合, 373
- Asset Manager 統合, 390
- BAC 統合, 398
- BSM トポロジ統合, 406

- CiscoWorks LMS 統合 , 380
- ClarusIPC Plus+ 統合
 - NNM iSPI for IP Telephony との , 387
 - NNMi との , 385
- HA 設定 , 221
- HPOM 統合、エージェント実装
 - 転送されたインシデント , 468 to 470
- HPOM 統合、Web サービス実装
 - 転送されたインシデント , 483 to 487
 - 同期 , 486
 - ファイアウォール , 487
 - メッセージブラウザ , 486
- NA 統合 , 420
- Netcool ソフトウェア用 NNMi 統合モジュール , 502 to 503
- nGenius Performance Manager 統合 , 440 to 442
- NNMi ノースバウンド インタフェース , 451
- PCM Plus 統合 , 426
- RAMS MPLS WAN 統合 , 428
- SIM 統合 , 433
- UCMDB 統合 , 438
- 検出
 - 自動検出 , 65 to 66

な

- 名前解決、制限 , 319
- 名前解決の制限 , 319

に

- 認証不合格、削減 , 53
- 認証プロファイル
 - 複数 , 50

ね

- ネットマスク、HA 設定の仮想ホスト NNMi, 198
- ネットワーク
 - アクセスの無効化 , 47
 - 確認する
 - 接続 , 64
 - 設定 , 76
 - 監視
 - 設定 , 76
 - 動作 , 69
 - ノード , 79
 - 基幹 , 55
 - 検出
 - NNM 6.x/7.x, 301
 - 評価 , 64 to 66

- 負荷 , 79

- ネットワーク インタフェース、HA 設定の仮想ホスト NNMi, 198
- ネットワーク運営センター , 317
- ネットワーク情報サービス , 209
- ネットワーク ステータス ポートレット , 393
- ネットワーク待ち時間 , 44

の

- ノード
 - HA クラスタのセカンダリの設定 NNMi, 201
 - HA クラスタのプライマリの設定 NNMi, 199 to 201
 - SNMP 設定 , 51
 - 監視 , 79
 - 削除する、検出した , 64
 - 詳細 , 361
 - 設定 , 41, 49
 - モニタリングの設定 , 75
 - レベルのフィルタリング , 356

- ノード インベントリ ビュー , 356

- ノード グループ
 - インタフェース グループ , 41
 - 階層 , 39
 - 確認する , 76
 - 事前設定 , 73
 - ステータス , 41
 - 設定 , 74
 - 定義 , 38
 - デバイス フィルタ , 40
 - 非 SNMP デバイス , 70
 - フィルタリング , 37
 - メンバーシップ , 39

- ノード グループのステータス ポートレット , 393

- ノード グループの定義 , 38

- [ノード グループ] フォームフォーム , 71

- [ノード グループ] フォームワークスペース , 71

- [ノードの設定] フォーム , 79

は

- バージョン
 - SNMP 優先 , 46
 - 情報ファイル , 246
- バージョン、サポートされる HA 製品 , 190

バージョン、サポート対象

統合されたアプリケーション

- AlarmPoint, 371
- AlarmPoint Mobile Gateway, 373
- Asset Manager, 390
- BAC My BSM, 392
- BSM トポロジ, 404
- CiscoWorks LMS, 378
- ClarusIPC Plus+ と NNMi, 384
- ClarusIPC Plus+ と NNM iSPI for IP Telephony, 386
- HPOM エージェント実装, 461
- NA, 412
- Netcool/OMNIbus, 496
- nGenius Performance Manager, 441
- PCM Plus, 426
- RAMS、MPLS WAN, 427
- SIM, 430
- UCMDB, 438

ハードウェアとソフトウェア, 29

バージョン比較

カスタマイズ

- イベント モニタリング, 306
- ステータス モニタリング, 304
- ネットワークの検出, 301

ハードウェア

- 対応, 29
- 必要な, 27

場所

- ipNoLookup.conf, 319
- jboss 配備ディレクトリ, 245
- LicFile.txt ファイル, 246
- netmon.cmstr, 316
- netmon.noDiscover, 328
- nGeniusNNM8.zip, 441
- SNMP MIB (UNIX), 246
- SNMP MIB (Windows), 245
- trapd.conf, 356

環境変数

- インストール, 22
- 管理, 512 to 515

ドキュメント, 309

- AlarmPoint Mobile Gateway 統合, 374
- AlarmPoint 統合, 371
- Asset Manager 統合, 390
- BAC My BSM 統合, 392
- BSM トポロジ統合, 404
- CiscoWorks LMS 統合, 378
- ClarusIPC Plus+ と NNMi の統合, 384
- ClarusIPC Plus+ 統合と NNM iSPI for IP Telephony, 386

- HPOM 統合、エージェント実装, 461

- HPOM 統合、Web サービス実装, 477

- NA 統合, 413

- nGenius Performance Manager 統合, 441

- PCM Plus 統合, 426

- RAMS MPLS WAN 統合, 428

- SIM 統合, 430

- UCMDB 統合, 438

- パス、NNM 6.x/7.x からのアップグレード, 285, 287, 295, 309

- パスワード、恒久ライセンス, 209

- パソコン、管理対象としない, 55

- パフォーマンス インシデント カテゴリ, 358

- パフォーマンス、ステータス ポーリング, 77

- パブリック キー証明書、インストール, 95

- パブリック キー証明書の取得, 95

パラメータ

- BAC My BSM 統合, 400 to 401

- BSM トポロジ統合, 406 to 409

- CiscoWorks LMS 統合, 381 to 382

- HPOM 統合

- Web サービス実装, 488 to 493

- エージェント実装, 471 to 474

- NA 統合, 423 to 424

- Netcool ソフトウェア用 NNMi 統合モジュール, 504 to 508

- NNMi ノースバウンド インタフェース, 454 to 458

- RAMS MPLS WAN 統合, 428

- SIM 統合, 433 to 435

- UCMDB 統合, 438

- アプリケーション フェイルオーバー, 178

- 範囲、IP アドレス, 65

ひ

- 非 SNMP デバイス ノード グループ, 70

ビュー

- NNMi から動的を起動, 364

- 追加の NNM 6.x/7.x を設定, 360

- 評価の順序, 68

ヒント

- IP アドレス範囲, 65

- システム ID 範囲, 66

- ヒント、設定

- シード済み検出, 63

- 自動検出, 62

ふ

ファイアウォール

- HPOM のトラブルシューティング、Web サービス実装, 487
- トラフィックの制御, 50
- ネットワーク アクセスの無効化, 47

ファイル

- <resource_group>.cntl.log, 228
- HA 設定
 - スクリプト, 226
 - ファイル, 226
- ipNoLookup.conf, 319
- jbossServer.log, 224
- ldap.properties, 134
- license.txt
 - アクティブなクラスタ ノード, 209
 - 管理サーバー, 276
- LicFile.txt
 - HA クラスタ, 207
 - 場所, 246
 - バックアップする, 199
- lwssofmconf.xml, 107, 109, 147
- netmon.cmstr, 316
- netmon.noDiscover, 328
- nGeniusNNM8.zip, 441
- nmsdbmgr.log, 228
- nnmcontainerlist.csv, 346
- nnmdatareplicator.conf, 226
- NOC_Demo_Portal_iSPIPerf.xml, 392 to 394
- NOC_Demo_Portal.xml, 392 to 394
- oid_to_sym, 321
- OLDsyslog.log, 228
- ov.conf
 - HA 設定, 226
 - nmsdbmgr のトラブルシューティング, 224
- ovspmd.log, 228
- postgres.log, 228
- recovery.conf, 178
- snmpcapture.out, 316, 346
- snmpout.txt, 316
- syslog.log, 228
- tar, 247
- trapd.conf, 356
- XML, 272
- 共有ディスク, 224
- クラスタ ノードで更新されない, 221
- コンポーネント登録, 246
- システムタイプ
 - NNMi, 198
- 転送先リスト, 355
- バージョン情報, 246
- バックアップする, 243
- レプリケーション, 206

ファイル システムのタイプ、HA 設定, 198

フィルタ

- インシデント, 491 to 493
- デバイス, 40
- ノード レベルの設定, 356

フィルタリング

- インタフェース グループ, 41
- ノード グループ, 37

フェーズ、NNM 6.x/7.x からのアップグレード, 310

フェイルオーバー

- アプリケーション
 - iSPI, 180
 - NNMi の設定, 175 to 177
 - 機能, 177 to 180
 - セットアップ, 174
 - 統合製品, 182
 - マルチサブネットでの設定, 187
 - 例, 179
- ディスク, 224

フォーム

- インシデントの設定
 - NNM 6.x/7.x インシデント設定を確認する, 357
- インタフェース グループ, 71
- 監視の設定
 - 状態ポーリングの高度化, 67
 - 状態ポーリングの調整, 79
- 管理ステーション, 359
- ノード グループ, 71

不合格、認証削減, 53

不整合な状態のレイヤー 2 接続の特定, 417

不整合な状態、レイヤー 2 接続, 417

部分バックアップ, 244

プライマリ HA クラスタ ノード

- 設定
 - NNMi, 199 to 201
- 設定情報
 - NNMi, 197

ブラウザ、インシデント, 353

不利点、リストベース検出, 57 to 58

プリンタ、管理対象としない, 55

フロー モデル、タスク, 35

プロセス

- Cluster Manager, 174
- Cluster Member, 174

- プロトコル
 - アクティブ, 50
 - 通信, 43
 - ポーリング, 47
- プロファイル、デバイス
 - 概念, 40
 - 状態ポーリング, 73
- プロファイル、認証
 - 複数, 50
- へ
- ページ、HA リファレンス, 196
- ベストプラクティス
 - NNMi 設定移動の準備, 271
 - No Device Profile, 321
 - 概要, 21
 - 既存の設定を保存, 36
 - 作成者属性, 36
 - 作成中
 - オブジェクトグループ定義, 72
 - 再使用可能なノードグループ, 73
 - 順序属性, 36
 - 順序番号の確認, 75
 - 順序番号のダブルチェック, 51
 - 短いポーリング間隔, 73
 - モニタリング設定のバッチ処理, 74
 - 優先される管理アドレス, 47
- 変更
 - BSM トポロジ統合, 405
 - CiscoWorks LMS 統合, 380
 - HPOM 統合
 - Web サービス実装, 482
 - エージェント実装, 466
 - NA 統合, 420
 - Netcool ソフトウェア用 NNMi 統合モジュール, 501
 - NNMi 管理サーバー
 - IP アドレス, 276
 - 概要, 271
 - NNMi ノースバウンド インタフェース, 450
 - SIM 統合, 432
 - UCMDB 統合, 438
- 変数、MIB II, 74
- 変数、環境
 - UNIX
 - MANPATH, 30
 - インストール, 22
 - 管理, 514

- Windows
 - NNMi 8.00, 515
 - アプリケーション フェイルオーバー, 174
 - インストール, 22
 - 管理, 512
 - 概要, 511

ほ

- ポータル、BAC My BSM
 - 説明, 391
- ポート番号、Web サーバー, 360
- ポートレット、BAC My BSM
 - NNMi の作成, 395 to 398
 - NNMi のトラブルシューティング, 398
 - 設定, 394
- ホーム ベース、NNM 6.x/7.x, 364
- ポーリング
 - 間隔の計画作成, 73
 - ステータス
 - 開始, 77
 - 調整, 78 to 79
 - パフォーマンスの評価, 77
 - 設定の例, 69
 - そのまま使用できる動作, 69
 - チェックリスト, 68
 - プロトコル, 47
- ポイント、マウント
 - NNMi, 199
- 方針、バックアップ, 248 to 249
- ホスト、HA 設定用の仮想
 - NNMi, 197
- ホスト名、HA 用に変更
 - NNMi, 208 to 211
- ボリュームグループ、HA 設定, 199
- ま
- 毎週のデータ バックアップ, 248
- マウントポイント
 - NNMi, 199
- 待ち時間、ねっとわーく, 44
- 末端ノード、管理対象としない, 55
- マンページ、HA, 196
- み
- 短い名前、HA 設定の仮想ホスト
 - NNMi, 197

む

無効化

- AlarmPoint Mobile Gateway 統合, 375
- AlarmPoint 統合, 373
- Asset Manager 統合, 390
- BSM トポロジ統合, 406
- CiscoWorks LMS 統合, 380
- ClarusIPC Plus+ 統合
 - NNM iSPI for IP Telephony との, 387
 - NNMi との, 384
- HPOM 統合
 - Web サービス実装, 483
 - エージェント実装, 467
- NA 統合, 420
- Netcool ソフトウェア用 NNMi 統合モジュール, 501
- nGenius Performance Manager 統合, 442
- NNMi ノースバウンド インタフェース, 451
- PCM Plus 統合, 426
- RAMS MPLS WAN 統合, 428
- SIM 統合, 432
- SNMP, 50
- UCMDB 統合, 438
 - トラフィック, 47
 - ネットワーク アクセス, 47

め

- メッセージブラウザ、HPOM のトラブルシューティング、Web サービス実装, 486
- メモリー リソース, 79
- メリット
 - BSM トポロジ統合, 403
 - CiscoWorks LMS 統合, 377
 - HPOM 統合
 - Web サービス実装, 476
 - エージェント実装, 460
 - NA 統合, 412
 - Netcool ソフトウェア用 NNMi 統合モジュール, 496
 - NNMi ノースバウンド インタフェース, 444
 - SIM 統合, 430
 - UCMDB 統合, 437
 - ルールベース検出, 57
 - リストベース検出, 57
- メンバーシップ、ノード グループ, 39

も

- モード、アプリケーション フェイルオーバーのクラスター マネージャ, 177
- 文字列、コミュニティ
 - アクセス資格認定, 45
 - 複数, 50
- モデル
 - タスクフロー, 35
 - ユーザー インタフェース, 36
- モニタリング
 - 設定
 - 確認する, 76 to 77
- モニタリング設定のバッチ処理, 74
- [モニタリングの設定] フォーム, 67, 71, 79
- フォーム
 - ステータス ポーリングの調整, 79
 - 説明, 67
 - ポーリングの種類と間隔の設定, 71
- 問題、HA の起動
 - nmsdbmgr, 224
 - NNMi, 223
 - pmd, 224

ゆ

- ユーザー インタフェース モデル, 36

有効化

- AlarmPoint Mobile Gateway 統合, 374
- AlarmPoint 統合, 371 to 372
- Asset Manager 統合, 390
- BSM トポロジ統合, 404
- CiscoWorks LMS 統合, 378 to 379
- ClarusIPC Plus+ 統合
 - NNM iSPI for IP Telephony との, 386
 - NNMi との, 384
- HPOM 統合、エージェント実装, 461
- HPOM 統合、Web サービス実装
 - Linux, 479
 - UNIX, 479
 - Windows, 477
- NA 統合, 413 to 415
- nGenius Performance Manager 統合, 441
- NNMi ノースバウンド インタフェース, 445
- PCM Plus 統合, 426
- RAMS MPLS WAN 統合, 428
- SIM 統合, 430 to 431
 - ルールベース検出, 65

優先

- SNMP のバージョン, 46
- 管理アドレス, 47

よ

要件、ハードウェアとソフトウェア, 29

用語

- HA, 192
- アプリケーション フェイルオーバー, 173

予防的データ バックアップ, 249

ら

ライセンス

- HA クラスタ, 207
- 限度, 58
- 購入する、追加のノード パック, 64
- ディレクトリの場所, 246
- 内容, 56

ライセンス キー、NNM iSPI NET, 417

ラグ タイム、テスト, 50

り

リストベース検出, 64

- 概要, 57
- 評価, 64

リソース グループ、HA
NNMi, 197

リリース、システム, 79

利点

- BSM トポロジ統合, 403
- CiscoWorks LMS 統合, 377
- HPOM 統合
 - Web サービス実装, 476
 - エージェント実装, 460
- NA 統合, 412
- Netcool ソフトウェア用 NNMi 統合モジュール, 496
- NNMi ノースバウンド インタフェース, 444
- SIM 統合, 430
- UCMDB 統合, 437
- ルールベース検出, 57
- リストベース検出, 57

リファレンス ページ、HA, 196

領域

- トポロジ, 245

領域、設定, 48

リリースノート, 29

リレーショナル データベース、バックアップする, 243

る

ルーター

- 階層, 39
- 監視, 69
- 検出, 65
- デフォルト, 66
- ノード グループの定義, 38

ルールベース検出

- 評価, 65 to 66

れ

例

- HPOM 統合、Web サービス実装
 - インシデント フィルタ, 492
- SNMP 情報, 316
- アプリケーション フェイルオーバー, 179
- コンテナ ビューの設定, 346
- ノード グループの設定, 75
- ポーリング設定, 69

レイヤー 2 接続、不整合な状態の特定, 417

レプリケーション、設定ファイル, 206

レベル、設定, 44

レポート、BAC My BSM のトラブルシューティング, 399

ろ

ログ ファイル

- HA クラスタ
- 更新されない, 221

わ

ワークスペース

- インシデント, 361
- インタフェース グループ, 71
- 設定
 - NNM 6.x/7.x 管理ステーションを設定, 359
 - 状態ポーリングの設定, 74
 - 状態ポーリングの評価, 76
- ノード グループ, 71

