

# HP Operations エージェント および HP Operations Smart Plug-ins for Infrastructure

Windows®、Linux、HP-UX、Solaris、AIX オペレーティングシステム向け  
ソフトウェアバージョン: 11.10

---

## インストールおよび設定ガイド

ドキュメントリリース日: 2012 年 9 月

ソフトウェアリリース日: 2012 年 9 月



## ご注意

### 保証

HP製品、またはサービスの保証は、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。ここに含まれる技術的、編集上の誤り、または欠如について、HPはいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

### 権利の制限

機密性のあるコンピュータソフトウェアです。これらを所有、使用、または複製するには、HPからの有効な使用許諾が必要です。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に関する書類、および商用アイテムの技術データは、FAR12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

### 著作権について

© Copyright 2010 - 2012 Hewlett-Packard Development Company, L.P.

### 商標について

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

Microsoft®、Windows®、およびWindows Vista®は、米国におけるMicrosoft Corporationの登録商標です。

UNIX®は、The Open Groupの登録商標です。

### 謝辞

本製品には、Eric Young (eay@cryptsoft.com)氏によって作成された暗号化ソフトウェアが含まれています。

本製品には、OpenSSL Toolkitで使用されるOpenSSL Project (<http://www.openssl.org/> (英語サイト))によって開発されたソフトウェアが含まれています。

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

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

本製品には 'zlib' 汎用圧縮ライブラリのインタフェースが使用されています。'zlib': Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

## ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

- ソフトウェアのバージョン番号は、ソフトウェアのバージョンを示します。
- ドキュメントリリース日は、ドキュメントが更新されるたびに更新されます。
- ソフトウェアリリース日は、このバージョンのソフトウェアのリリース期日を表します。

最新の更新のチェック、またはご使用のドキュメントが最新版かどうかの確認には、次のサイトをご利用ください。

<http://support.openview.hp.com/selfsolve/manuals>

このサイトを利用するには、HP Passportへの登録とサインインが必要です。HP Passport IDの取得登録は、次のWebサイトから行なうことができます。

<http://h20229.www2.hp.com/passport-registration.html>(英語サイト)

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

適切な製品サポートサービスをお申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、HPの営業担当にお問い合わせください。

## サポート

HPソフトウェアサポートオンラインWebサイトを参照してください。

<http://support.openview.hp.com>

HPソフトウェアが提供する製品、サービス、サポートに関する詳細情報をご覧ください。

HPソフトウェアオンラインではセルフソルブ機能を提供しています。お客様の業務の管理に必要な対話型の技術支援ツールに素早く効率的にアクセスいただけます。HPソフトウェアサポートWebサイトのサポート範囲は次のとおりです。

- 関心のある技術情報の検索
- サポートケースとエンハンスメント要求の登録とトラッキング
- 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 サポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部を除き、サポートのご利用には、HP Passportユーザとしてご登録の上、ログインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HP Passport IDの登録は、次の場所で行います。

<http://h20229.www2.hp.com/passport-registration.html>(英語サイト)

アクセスレベルに関する詳細は、以下のWebサイトにアクセスしてください。

[http://support.openview.hp.com/access\\_level.jsp](http://support.openview.hp.com/access_level.jsp)

---

## 目次

インストールおよび設定ガイド.....	1
目次.....	5
はじめに.....	8
インストールの計画.....	8
Operations エージェント の HPOM 管理 サーバーでの登録 (および Infrastructure SPI のインストール).....	11
HPOM for Windows 管理 サーバーへの登録.....	11
UNIX/Linux 管理 サーバーの HPOM での登録.....	14
Operations エージェント 配布 パッケージの削除.....	17
HP Operations エージェント をインストールするための前提条件.....	18
Windows の前提条件.....	18
Linux の前提条件.....	20
HP-UX の前提条件.....	22
Solaris の前提条件.....	23
AIX の前提条件.....	25
ノードのアップグレード.....	26
プレインストール タスク: クラスタ内の HPOM に HP Operations エージェント をインストールするには.....	29
HPOM コンソールからのインストール.....	30
ノードへの HP Operations エージェント の手動インストール.....	31
NAT 環境でのインストール後のタスク.....	36
非アクティブ モードでのエージェントのインストール.....	37
HP Operations エージェント の証明書の設定.....	41
インストールキーによる証明書要求.....	41
自動での証明書の要求.....	42
手動での証明書の配布.....	42
証明書の復元.....	44
高可用性 クラスタにおける HP Operations エージェント.....	46

---

安全な環境へのHP Operations エージェントの配布.....	52
プロキシの設定.....	53
プロキシ設定ファイルの構成.....	55
通信ブローカポートの設定.....	58
ローカル通信ポートの設定.....	61
複数のIPアドレスがあるノードの設定.....	61
プロキシを介したHTTPS通信の設定.....	62
安全性の高い環境における通信.....	62
リバースチャンネルプロキシの概要.....	64
アウトバウンドのみの環境における安全な通信の設定.....	66
設定ファイルによるRCP詳細の指定.....	68
複数のシステムに対するRCPの設定.....	69
RCPを介した通信の検証.....	70
2つのファイアウォールを介した通信.....	71
Performance Collection Componentのリモートからの設定.....	72
事前準備.....	72
OA-PerfCollComp-opcmsgポリシーの配布.....	73
Performance Collection Componentの設定.....	73
parmファイルの設定.....	73
HPOM for Windowsの場合.....	73
UNIX/Linux 9.10のHPOMの場合.....	74
alarmdefファイルの設定.....	74
HPOM for Windowsの場合.....	75
UNIX/Linux 9.10のHPOMの場合.....	75
HP Operations エージェントのリモートからの操作.....	76
HP Operations エージェントの監視.....	78
事前準備.....	78
自己監視ポリシー.....	79
自己監視ポリシーの配布.....	80
コンポーネントのステータス表示.....	81
Infrastructure SPIのみのインストール.....	82
HPOM for WindowsでのInfrastructure SPIsのコンポーネント.....	86

HPOM for UNIX での Infrastructure SPIs のコンポーネント.....	88
HP Operations エージェント のアンインストール.....	91
Infrastructure SPI のアンインストール.....	92

# 第1章

## はじめに

HP Operations エージェントはシステムの重要な要素のヘルス、パフォーマンス、可用性を示すメトリックを収集することにより、システムの監視を可能にします。HP Operations Manager (HPOM) は、単一のインタラクティブなコンソールを通じて複数のシステムを監視、管理するフレームワークを提供しますが、一方、個々のノードに配備された HP Operations エージェントは重要な情報を収集し、容易に監視プロセスを実施できるようにします。

HP Operations エージェントおよび *Infrastructure SPI 11.10* DVD メディアには、HP Operations Smart Plug-ins for Infrastructure (Infrastructure SPI) が収録されています。Infrastructure SPI を電子メディアからインストールする場合は、必ずすべてのノード プラットフォーム用の (およびプラットフォーム専用の ISO ファイルではない) メディアをダウンロードしてください。プラットフォーム専用の ISO ファイルには Infrastructure SPI が含まれていません。

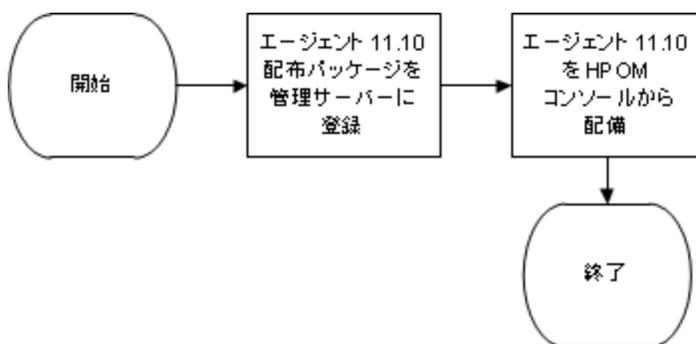
## インストールの計画

### HP Operations エージェント の HPOM 管理サーバーからリモートでのインストール

HPOM が導入された一元的な監視環境では、HP Operations エージェント 11.10 の配布パッケージを管理サーバーにインストールし、HPOM コンソールから複数の対象ノードに対してエージェント パッケージを一元的に配布できます。

これは、次のように行います。

1. HP Operations エージェント 11.10 配布パッケージを HPOM 管理サーバーに登録<sup>1</sup>します。  
HP Operations エージェント 配布パッケージを登録すると、Infrastructure SPI が自動的に HPOM 管理サーバーにインストールされます。Infrastructure SPI のインストールを省略するようにインストールを設定できます。
2. HPOM コンソールから HP Operations エージェント を一元的にインストールします。



### ノードへの HP Operations エージェント の手動インストール

管理対象ノードに手動でログオンすると、HP Operations エージェントおよび *Infrastructure SPI 11.10* から HP Operations エージェント をインストールすることができます。

<sup>1</sup>登録を行うと、確実に HP Operations エージェント 配布パッケージを配布サーバー (エージェントをノードに配布できるサーバー) の適切な場所に配置できます。

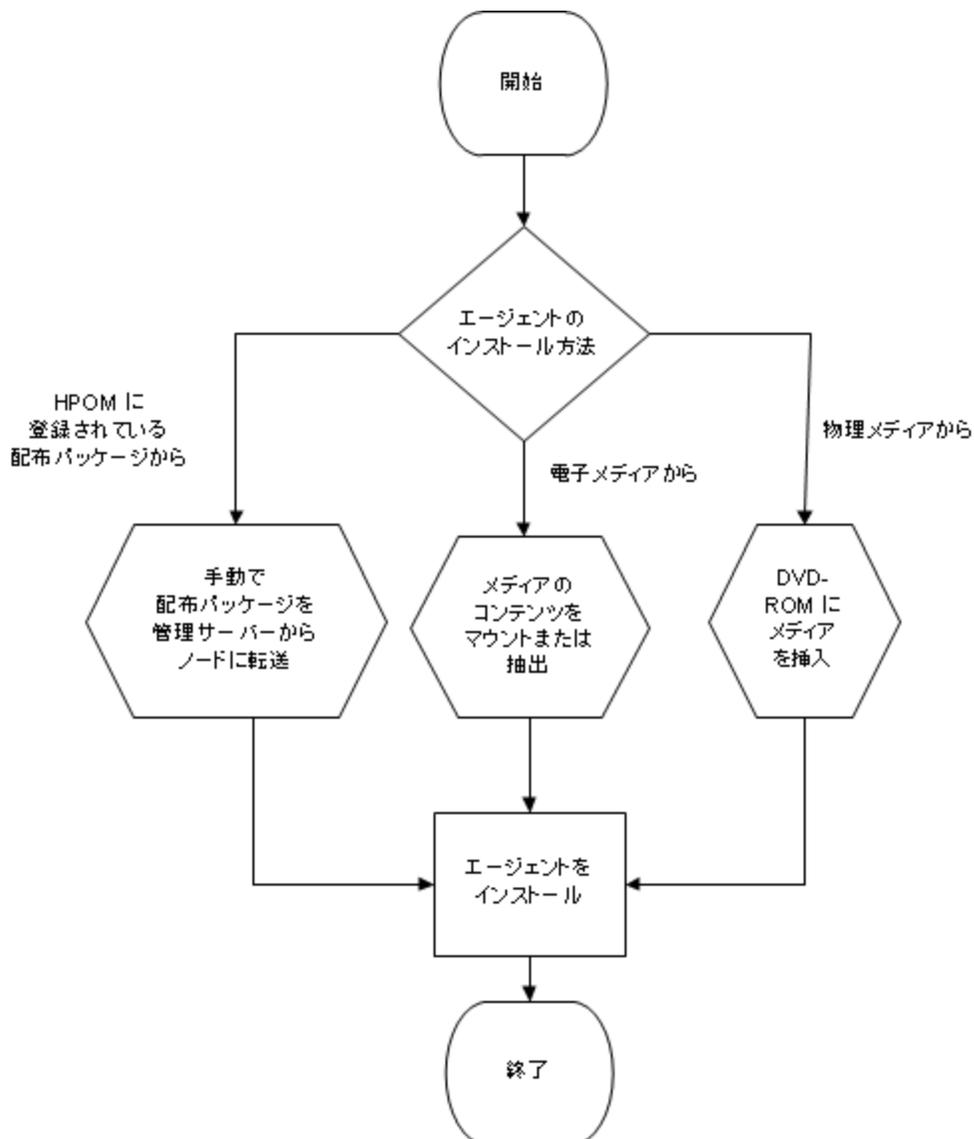
これは、次のように行います。

### 1. ノードを準備します。

次のいずれかを実行して、エージェントをインストールするための管理対象ノードを準備できます。

- *HP Operations エージェントおよびInfrastructure SPI 11.10* 物理メディアをDVDドライブに挿入します。
- *HP Operations エージェントおよびInfrastructure SPI 11.10* 電子メディアの内容をローカルディレクトリに抽出します。
- *HP Operations エージェントおよびInfrastructure SPI 11.10* 物理メディアをマウントします。
- 配布パッケージをHPOM管理サーバーから手動で転送します。

### 2. *HP Operations エージェントおよびInfrastructure SPI 11.10* メディアまたは配布パッケージで利用可能なインストーラプログラム (oainstall または oasetup) を使ってエージェントをインストールします。



### Infrastructure SPI のみのインストール

HP Operations エージェントおよび Infrastructure SPI 11.10 を使用すると、HPOM 管理サーバーには Infrastructure SPI だけをインストールできます。

これは、次のように行います。

1. HPOM 管理サーバーで設定ファイルを準備します。
2. HP Operations エージェントおよび Infrastructure SPI 11.10 メディアで利用可能なインストーラプログラム (`oainstall` または `oasetup`) で Infrastructure SPI をインストールします。

## 第2章

---

### Operations エージェント の HPOM 管理サーバーでの登録 (および Infrastructure SPI のインストール)

#### HPOM for Windows 管理サーバーへの登録

##### 前提条件

- 配布パッケージを登録しているときは配布ジョブを実行しないでください。  
アクティブな配布ジョブを表示するには
  1. コンソールツリーで、[ポリシー管理]を展開します。
  2. **[配布ジョブ]**をクリックします。アクティブな配布ジョブのリストが詳細ペインに表示されます。エージェント配布パッケージのインストール時にアクティブになっている配布ジョブがないことを確認する必要があります。エージェント配布パッケージの登録が完了するまで、配布ジョブを起動することはできません。
- Windows または AIX 用の HP Performance Agent 4.70 の配布可能パッケージが管理サーバーで利用できる場合、HP Operations エージェント 11.10 の配布パッケージを登録する前に、HP Performance Agent 4.72 の配布可能パッケージをインストールするか、HP Performance Agent 4.70 の配布可能パッケージを完全に削除する必要があります。
- ディスク容量:1 GB

##### 配布パッケージの登録<sup>1</sup>

1. 管理者権限で管理サーバーにログオンします。
2. 次のいずれかの作業を実行します。
  - 物理メディアを使って配布パッケージを登録する場合、*HP Operations エージェントおよび Infrastructure SPI 11.10* DVD を DVD-ROM ドライブに挿入します。
  - HP の Web サイトからインストールメディアをダウンロードします。HP の Web サイトには、それぞれのプラットフォーム固有の HP Operations エージェント 11.10 配布パッケージ用 .iso ファイルがあります。パッケージ固有の .iso ファイルをダウンロードすることも、すべてのプラットフォームの配布パッケージが含まれる .iso ファイルをダウンロードすることもできます。

Infrastructure SPI をインストールする場合、すべてのプラットフォーム用の配布パッケージが含まれる物理 DVD または .iso ファイルを使用します。プラットフォーム固有の .iso ファイルには、Infrastructure SPI が含まれていません。

3. オプション:Infrastructure SPI のインストールを省略するには、設定ファイルを作成します。

oainstall プログラムにより、配布パッケージの登録中に Infrastructure SPI が管理サーバーにインストールされます。このインストールには、Infrastructure SPI の (HP Reporter に必要な)レ

---

<sup>1</sup>登録を行うと、確実に HP Operations エージェント配布パッケージを配布サーバー (エージェントをノードに配布できるサーバー) の適切な場所に配置できます。

ポートと(Performance Managerに必要な)グラフのパッケージが含まれています。Infrastructure SPIのインストールを省略するには、次の手順に従います。

i. テキスト エディタで新しいファイルを作成します。

ii. 次の内容を追加します。

```
[agent.parameter]
REGISTER_AGENT=YES

[hpinfraspi.parameter]
InfraSPI=NO
InfraSPI_With_Graphs=NO
InfraSPI_With_Reports=NO
```

iii. ファイルを保存します。

4. メディアのルートから、次のコマンドを実行します。

**cscript oainstall.vbs -i -m**

このコマンドにより、すべてのプラットフォームのエージェント配布パッケージが管理サーバーに登録され、Infrastructure SPI がインストールされます。

Infrastructure SPI をインストールせずに手順 3 を完了するには、次のコマンドを実行します。

**cscript oainstall.vbs -i -m -spiconfig <config\_file>**

**ヒント:** 必要に応じて、選択したプラットフォームのみの配布パッケージに登録するように選択できます。ただし、プラットフォーム固有の配布パッケージに登録するコマンドでは Infrastructure SPI をインストールできません。

次のコマンドを実行して、1つのプラットフォームのみの配布パッケージをインストールします。

**cscript oainstall.vbs -i -m -p <platform>**

この例では、<プラットフォーム>に次のいずれかの値を使用します。

Windows の場合 :WIN

HP-UX の場合 :HP-UX

Linux の場合 :LIN

Solaris の場合 :SOL

AIX の場合 :AIX

1つのコマンドで複数のノード プラットフォームの配布パッケージに登録するには、複数の-p オプションをスペースで区切って使用します。

たとえば、次のようになります。

**cscript oainstall.vbs -i -m -p AIX -p SOL**

HPOM が高可用 (HA) クラスタにある場合

HPOM 高可用性 (HA) クラスタのアクティブ ノードで、前述の手順を実行します。

手順を完了したら、パッシブノードにフェールオーバーして、パッシブノードの  
%OvShareDir%server\installation ディレクトリに移動し、次のコマンドを実行します。

#### **cscript oainstall\_sync.vbs**

必要なオプションと引数を指定してインストールコマンドを実行すると、登録手順が始まります。登録プロセスの完了には、選択したパッケージの数に応じて、最大 20 分かかることがあります。

#### **確認**

1. 管理サーバーで、次の場所に移動します。

```
%ovinstalldir%bin\OpC\agtinstall
```

2. 次のコマンドを実行します。

#### **cscript oainstall.vbs -inv -listall**

このコマンドにより、管理サーバーにある利用可能な (アクティブな) 配布パッケージのリストが表示されます。

3. 配布パッケージをインストールしたプラットフォームを見つけます。アクティブバージョンに 11.10 と表示されていたら、インストールは成功です。

#### **ログファイル**

登録ログファイル (oainstall.log) は、次のディレクトリにあります。

```
%OvDataDir%shared\server\log
```

#### **パッケージの配置**

HP Operations エージェント パッケージを管理サーバーに登録すると、oainstall プログラムはすべての必要な配布パッケージを次のディレクトリに配置します。

```
%OvDataDir%shared\Packages\HTTPS
```

#### **配布パッケージのバックアップ**

管理サーバーにある配布パッケージを登録する場合、oainstall スクリプトは、古い配布パッケージのコピーを次のローカルディレクトリに保存します。

```
%OvShareDir%server\installation\backup\HPOpsAgt\<<OS>\<OA_
Version>\<ARCH>
```

アクティブな配布パッケージを表示するには、次のコマンドを実行します。

#### **cscript oainstall.vbs -inv**

システムにあるすべての配布パッケージ (アクティブまたはバックアップ) を表示するには、次のコマンドを実行します。

#### **cscript oainstall.vbs -inv -listall**

```
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Active Versions
=====
AIX      :PowerPC(64)      :11.10.033
HP-UX    :IPF32               :11.10.033
HP-UX    :PA-RISC            :11.10.033
LIN      :PowerPC(2.6)       :11.10.033
LIN      :x64(2.6)           :11.10.033
LIN      :x86(2.6)           :11.10.033
SOL      :SPARC           :11.10.033
SOL      :x86             :11.10.033
WIN      :x64             :11.10.033
WIN      :x86             :11.10.033

Backed-up Versions
=====
AIX      :PowerPC(32)     :08.60.005
AIX      :PowerPC(64)     :08.60.005
AIX      :PowerPC(32)     :11.00.044
AIX      :PowerPC(64)     :11.00.044
HP-UX    :IPF32           :08.60.005
HP-UX    :PA-RISC         :08.60.005
HP-UX    :IPF32           :11.00.044
HP-UX    :PA-RISC         :11.00.044
LIN      :IPF64(2.6)      :08.60.005
LIN      :x64(2.6)        :08.60.005
LIN      :x86(2.6)        :08.60.005
LIN      :IPF64(2.6)      :11.00.044
LIN      :PowerPC(2.6)    :11.00.044
LIN      :x64(2.6)        :11.00.044
LIN      :x86(2.6)        :11.00.044
SOL      :SPARC           :08.60.005
SOL      :x86             :08.60.005
SOL      :SPARC           :11.00.044
SOL      :x86             :11.00.044
WIN      :x64             :11.00.044
WIN      :x86             :11.00.044
WIN      :x64             :11.10.017
WIN      :x86             :11.10.017
WIN      :x64             :11.10.030
WIN      :x86             :11.10.030
WIN      :x64             :11.10.031
```

## UNIX/Linux 管理サーバーの HPOM での登録

### HPOM 管理サーバーでの配布パッケージの登録

注: 管理サーバーでは、少なくとも 1 GB のディスク領域を利用できる必要があります。

1. root で管理サーバーにログオンします。
2. 次のいずれかの作業を実行します。
  - 物理メディアを使って配布パッケージを登録する場合、*HP Operations エージェントおよび Infrastructure SPI 11.10 DVD* を DVD-ROM ドライブに挿入します。
  - HP の Web サイトからインストールメディアをダウンロードします。HP の Web サイトには、それぞれのプラットフォーム固有の HP Operations エージェント 11.10 配布パッケージ用 .iso ファイルがあります。パッケージ固有の .iso ファイルをダウンロードすることも、すべてのプラットフォームの配布パッケージが含まれる .iso ファイルをダウンロードすることもできます。.iso ファイルをダウンロードしたら、管理サーバーのローカルディレクトリにファイルの内容を抽出します。

3. オプション:Infrastructure SPI のインストールを省略するには、設定ファイルを作成します。

oainstall プログラムにより、配布パッケージの登録中に Infrastructure SPI が管理サーバーにインストールされます。このインストールには、Infrastructure SPI の (HP Reporter に必要な) レポートと (Performance Manager に必要な) グラフのパッケージが含まれています。Infrastructure SPI のインストールを省略するには、次の手順に従います。

- i. テキスト エディタで新しいファイルを作成します。

- ii. 次の内容を追加します。

```
[agent.parameter]
REGISTER_AGENT=YES

[hpinfraspi.parameter]
InfraSPI=NO
InfraSPI_With_Graphs=NO
InfraSPI_With_Reports=NO
```

- iii. ファイルを保存します。

4. メディアのルートから、次のコマンドを実行します。

**./oainstall.sh -i -m -p ALL**

このコマンドにより、すべてのプラットフォームのエージェント配布パッケージが管理サーバーに登録され、Infrastructure SPI がインストールされます。

Infrastructure SPI をインストールせずに手順 3 を完了するには、次のコマンドを実行します。

**./oainstall.sh -i -m -p ALL -spiconfig <config\_file>**

**ヒント:** 必要に応じて、選択したプラットフォームのみの配布パッケージをインストールするように選択できます。

次のコマンドを実行して、1つのプラットフォームのみの配布パッケージをインストールします。

**./oainstall.sh -i -m -p <platform>**

この例では、<プラットフォーム> に次のいずれかの値を使用します。

Windows の場合 :WIN

HP-UX の場合 :HP-UX

Linux の場合 :LIN

Solaris の場合 :SOL

AIX の場合 :AIX

1つのコマンドで複数のノードプラットフォームの配布パッケージをインストールするには、複数の -p オプションをスペースで区切って使用します。

たとえば、次のようになります。

```
./oainstall.sh -i -m -p AIX -p SOL
```

HPOM が高可用 (HA) クラスタにある場合

HPOM 高可用性 (HA) クラスタのアクティブ ノードで、前述の手順を実行します。

手順を完了したら、パッシブ ノードにフェールオーバーして、パッシブ ノードの `/var/opt/OV/shared/server/installation` ディレクトリに移動し、次のコマンドを実行します。

```
./oainstall_sync.sh
```

必要なオプションと引数を指定してコマンドを実行すると、登録手順が開始します。登録プロセスの完了には、選択したパッケージの数に応じて、最大 20 分かかることがあります。

### 確認

1. 管理サーバーで、次の場所に移動します。

```
/opt/OV/bin/OpC/agtinstall
```

2. 次のコマンドを実行します。

```
./oainstall.sh -inv -listall
```

このコマンドにより、管理サーバーにある利用可能な (アクティブな) 配布パッケージのリストが表示されます。

3. 配布パッケージをインストールしたプラットフォームを見つけます。アクティブバージョンに 11.10 と表示されていたら、インストールは成功です。

### ログファイル

登録ログファイル (`oainstall.log`) は、次のディレクトリにあります。

```
/var/opt/OV/shared/server/log
```

### パッケージの配置

HP Operations エージェント パッケージを管理サーバーに登録すると、`oainstall` プログラムはすべての必要な配布パッケージを次のディレクトリに配置します。

```
/var/opt/OV/share/databases/OpC/mgd_node/vendor
```

### 配布パッケージのバックアップ

管理サーバーにある配布パッケージを登録する場合、`oainstall` スクリプトは、古い配布パッケージのコピーを次のローカルディレクトリに保存します。

```
/var/opt/OV/shared/server/installation/backup/HPOpsAgt/<OS>/<OA_
Version>/<ARCH>
```

アクティブな配布パッケージを表示するには、次のコマンドを実行します。

```
./oainstall.sh -inv
```

システムにあるすべての配布パッケージ (アクティブまたはバックアップ) を表示するには、次のコマンドを実行します。

```
./oainstall.sh -inv -listall
```

## Operations エージェント 配布パッケージの削除

1. UNIX/Linux の場合:管理サーバーに管理者でログオンし、`%ovinstalldir%bin\OpC\agtinstall` ディレクトリに移動します。  
Windows の場合:管理サーバーにrootでログオンし、`/opt/OV/bin/OpC/agtinstall` ディレクトリに移動します。
2. 次のコマンドを実行して、削除する配布パッケージの正しいバージョン番号をメモに記録します。

*Windows の場合*

```
cscript oainstall.vbs -inv -listall
```

*UNIX/Linux の場合*

```
./oainstall.sh -inv -listall
```

3. 次のコマンドを実行します。

*Windows の場合*

```
cscript oainstall.vbs -r -m -v <version> -p <platform>
```

*UNIX/Linux の場合*

```
./oainstall.sh -r -m -v <version> -p <platform>
```

ここで、`<version>` は削除するエージェント 配布パッケージのバージョンです。

`-p` オプションでは、管理サーバーから削除する HP Operations エージェントのプラットフォーム固有のパッケージを指定します。プラットフォーム情報を引数の形式でこのオプションに指定するには、次のリストを使用します。

- Linux:LIN
- Solaris:SOL
- HP-UX:HP-UX
- AIX:AIX
- Windows:WIN
- すべてのプラットフォーム:ALL

このオプションと引数には大文字と小文字の区別があります。

HP Operations エージェント 11.10 配布パッケージを削除すると、(使用可能な場合) インストーラプログラムは、配布パッケージの最も新しいバックアップバージョンを管理サーバーに復元します。

## 第3章

---

# HP Operations エージェント をインストールするための前提条件

## Windows の前提条件

### ユーザー

HP Operations エージェントを Windows ノードにインストールするには、管理者権限を持つユーザーを使用する必要があります。このユーザーは、デフォルトのシステム共有 (**Programs Files** フォルダが設定されているディスク) にアクセスできる権限に加え、以下の追加権限を持つ必要があります。

- ローカル Administrators グループのメンバシップ
- ADMIN\$ 共有 への書き込みアクセス
- レジストリの読み取りアクセス
- 「サービスとしてログオン」の権限
- サービスの開始および停止権限

### 必要なソフトウェア

**Windows インストーラ 4.5 以降:** Windows インストーラソフトウェアは、Microsoft Windows オペレーティングシステムに含まれています。HP Operations エージェントのインストーラプログラムでは、システム上にこのソフトウェアコンポーネントのバージョン 4.5 が存在する必要があります。

**Windows Script Host:** Windows Script Host がシステムで有効化されている必要があります。HP Operations エージェントのインストーラプログラムでは、Windows Script Host が有効である必要があります。Windows Script Host が有効かどうかをチェックするには、以下の手順に従います。

1. Windows システムにログオンします。
2. [スタート] メニューから、[ファイル名を指定して実行] を開きます。
3. [ファイル名を指定して実行] で、**regedit** と入力して **Enter** キーを押します。[レジストリエディタ] ウィンドウが開きます。
4. [レジストリエディタ] ウィンドウで、**[HKEY\_LOCAL\_MACHINE] > [SOFTWARE] > [Microsoft]** の順に展開し、**[Windows Script Host]** をクリックします。
5. 右側のペインで [Enabled] キーを探します。
6. [Enabled] が存在する場合は、そのキーをダブルクリックして [Value Data] が 1 にセットされていることを確認します。Windows Script Host が無効の場合、[Enabled] キーの [Value Data] は 0 にセットされています。
7. [Enabled] が存在しない場合は、問題なく Windows Script Host は有効であると見なすことができます。

### 必要なサービス

エージェントをインストールする前に、以下のサービスが稼働していることを確認します。

- Event Log
- Remote Procedure Call (RCP)
- Plug and Play
- Security Accounts Manager
- Net Logon
- Remote Registry
- サーバー
- Workstation

上記サービスが稼働していることを確認するには、以下の手順に従います。

1. 管理権限でシステムにログオンします。
2. [スタート]メニューから、[ファイル名を指定して実行]を開きます。
3. [ファイル名を指定して実行]で、**services.msc**と入力して **Enter** キーを押します。[サービス]ウィンドウが開きます。
4. [サービス]ウィンドウで、上記の各サービスのステータスが[開始]かどうかをチェックします。いずれかのサービスのステータスが[開始]以外の場合は、サービスを右クリックし、次に[開始]をクリックします。

#### ディスク容量

##### 新規インストールの場合

インストールディレクトリ用

350 MB

データディレクトリ用

50 MB

##### 旧エージェントソフトウェアからのアップグレードの場合

インストールディレクトリ用

100 MB

データディレクトリ用

50 MB

#### 推奨されるソフトウェアとサービス

**WMI インターセプタ ポリシー:**Windows Management Instrumentation インターセプタ ポリシーまたは Measurement Threshold ポリシーを配布して WMI イベントおよびクラスを監視する場合や、ノードで自動サービス検出を実行する場合、システムで WMI サービスを利用可能にする必要があります。

**SNMP MIB 監視:**エージェントシステム上の SNMP MIB (Management Information Base) 内のオブジェクトを監視したい場合は、システムに必ず SNMP エージェント (MIB-I および MIB-II 準拠) をインストールします。

**HPOM アクションツールのノード**で HPOM アクションおよびツールを起動する場合、NT LM Security Support Provider サービスが稼働している必要があります。

#### **Windows Server 2008 上の Hyper-V に適用される追加要件**

仮想システムを監視できるように、以下の修正プログラムを適用します。

<http://support.microsoft.com/kb/950050>

メトリックの BYLS クラスをログに記録できるように、以下の修正プログラムを適用します。

<http://support.microsoft.com/KB/960751>

## Linux の前提条件

### ユーザー

HP Operations エージェントを Linux ノードにインストールするには、root 権限を持つユーザーを使用する必要があります。

**注:** Linux ノードでは root ユーザーを使用せずに HP Operations エージェントをインストールすることはできないので、HPOM コンソールからリモートで vSphere Management Assistant (vMA) ノードにエージェントをインストールすることはできません (root ユーザーがデフォルトで無効になっているため)。

### 必要なソフトウェア

HP Operations エージェントをインストールするには、以下のランタイムライブラリとパッケージが必要となります。

- glibc-2.3.4-2.36.i686.rpm
- C++ ランタイム
  - カーネルバージョン 2.6 のシステムの場合  
**/usr/lib/libstdc++.so.5**
  - カーネルバージョン 2.6 の Itanium システムの場合  
**/usr/lib/libstdc++.so.6**
- curses ランタイムライブラリ  
**/usr/lib/libncurses.so.5**
- x64 システムの場合:
  - libgcc-3.4.6-8.i386.rpm
  - libstdc++-3.4.6-8.i386.rpm

HPOM for Windows コンソールからリモートでエージェントをインストールしたい場合は、システムに OpenSSH 5.2 以降がインストールされていることを確認します。

### ディスク容量

#### 新規インストールの場合

インストールディレクトリ用 (**/opt/OV** および **/opt/perf**):

350 MB

データディレクトリ用 (**/var/opt/OV** および **/var/opt/perf**):

350 MB

#### アップグレードの場合

インストールディレクトリ用 (`/opt/OV` および `/opt/perf`):

100 MB

データディレクトリ用 (`/var/opt/OV` および `/var/opt/perf`):

350 MB

**注:** インストールディレクトリまたはデータディレクトリに十分な容量がない場合、`ln -s` コマンドを使用して、インストールディレクトリまたはデータディレクトリから同じシステムの別の場所に対してシンボリックリンクを設定できます。

たとえば、`/opt/OV` ディレクトリから `/new` ディレクトリに対してシンボリックリンクを設定する場合は、次のようにします。

```
ln -s /new /opt/OV
```

#### 推奨されるソフトウェアとサービス

**SNMP MIB 監視:** エージェントシステム上の SNMP MIB (Management Information Base) 内のオブジェクトを監視したい場合は、システムに必ず SNMP エージェント (MIB-I および MIB-II 準拠) をインストールします。

3. **xglance:** xglance ユーティリティを使用するには、システムに以下のコンポーネントが存在する必要があります。
4. Open Motif ツールキット 2.2.3 (Red Hat Enterprise Linux 5.x、および SUSE Linux Enterprise Server 10.x を除く x86\_64 と Itanium 環境の Linux プラットフォームでは、Open Motif ツールキットの 32 ビットバージョンと関連ライブラリが存在する必要があります)。

#### vMA ノードの追加要件

- portmap サービスが開始されていることを確認します。
- vMA のフロッピー ディスクドライブを無効にします。
- vMA の RAM サイズを 1 GB に増やします。
- ファイアウォールを経由した vMA ノードとの通信を可能にします。

エージェントはポート 383 を使用し、ファイアウォールを経由して他のシステムとの通信を円滑に実施します。このポート 383 の通信トラフィックを受け入れるように、vMA ノードを設定する必要があります。これを実行するには、以下のコマンドを実行します。

```
■ sudo iptables -I RH-Firewall-1-INPUT 3 -p tcp -m tcp --dport 383 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
```

```
■ sudo service iptables save
```

変更が有効になっていることを確認するには、次のコマンドを実行します。

```
sudo vi /etc/sysconfig/iptables
```

vi エディタにより、`/etc/sysconfig` ディレクトリの `iptables` ファイルが開かれます。iptables ファイルの中に、以下の行が存在することを確認します。

```
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 383 --tcp-flags  
SYN,RST,ACK SYN -j ACCEPT
```

**注:** デフォルトでは、vMA (Linux) ノードの root ユーザーは無効になっています。そのため、エージェントを HPOM コンソールからリモートで vMA ノードに配布することはできません。HP Operations エージェントのインストーラプログラム (oainstall スクリプト) にも root 権限が必要です。そのため、エージェントを手動で vMA ノードにインストールする前に、sudo コマンドを使用して root ユーザーに切り替える必要があります。

## HP-UX の前提条件

### ユーザー

HP Operations エージェントを HP-UX ノードにインストールするには、root 権限を持つユーザーを使用する必要があります。

### 必要なソフトウェア

HP-UX で、以下のパッチがインストールされていることを確認します。

- HP-UX 11.23. の場合、PHKL\_36853、PHCO\_38149 (または後継パッチ)
- HP-UX 11i v1. の場合、PHNE\_27063 (または後継パッチ)
- HP-UX 11i v1. の場合、PHCO\_24400 s700\_800 11.11 libc 累積パッチ (または後継パッチ)
- HP-UX 11.11 PA-RISC. の場合、PHCO\_38226 (または後継パッチ)
- HP-UX 11.31. の場合、PHCO\_36530 (または後継パッチ)
- HP-UX 11i v1. の場合、パフォーマンスツールが VERITAS Volume Manager 3.2 と連携して機能するには、以下のパッチが必要となります。
  - PHKL\_26419 for HP-UX B.11.11 (11.11) (または後継パッチ)
  - PHCO\_26420 for HP-UX B.11.11 (11.11) (または後継パッチ)

Itanium で実行されている HP-UX システムでは、libunwind ライブラリを利用できます。

HP-UX 11i v1 システムが複数のプロセッサで構成されており、PRM Group が APP\_ メトリックを記録するために parm ファイル内で log application=prm スイッチを使用している場合、以下のパッチをインストールする必要があります。

PHKL\_28052 (または後継パッチ)

HP-UX 11i v1 以降では、パフォーマンスツールは Instant Capacity on Demand (iCOD) と連携して動作します。iCOD データを正しく報告するには、以下の pstat カーネルパッチがインストールされている必要があります (iCOD がシステムにインストールされていない場合は、このカーネルパッチはインストールしないでください)。

PHKL\_22987 for HP-UX B.11.11 (11.11) (または後継パッチ)

HP GlancePlus は HP Operations エージェントのこのバージョンに含まれており、Process Resource Manager (PRM) バージョン C.03.02 と連携して動作します。

HP-UX 11.11 以降で EMC PowerPath v2.1.2 または v3.0.0 が稼働する場合は、最新の EMC パッチがインストールされている必要があります。

- EMC PowerPath v2.1.2 リリースの場合は、以下のパッチを使用します。  
EMCpower\_patch213 HP.2.1.3\_b002 (または後継パッチ)
- EMC PowerPath v3.0.0 リリースの場合は、以下のパッチを使用します。  
EMCpower\_patch301 HP.3.0.1\_b002 (または後継パッチ)

#### ディスク容量

##### 新規インストールの場合

インストールディレクトリ用 (/opt/OV および /opt/perf):

400 MB

データディレクトリ用 (/var/opt/OV および /var/opt/perf):

550 MB

##### アップグレードの場合

インストールディレクトリ用 (/opt/OV および /opt/perf):

400 MB

データディレクトリ用 (/var/opt/OV および /var/opt/perf):

550 MB

**注:** インストールディレクトリまたはデータディレクトリに十分な容量がない場合、ln -s コマンドを使用して、インストールディレクトリまたはデータディレクトリから同じシステムの別の場所に対してシンボリックリンクを設定できます。  
たとえば、/opt/OV ディレクトリから /new ディレクトリに対してシンボリックリンクを設定する場合は、次のようにします。  
**ln -s /new /opt/OV**

#### 推奨されるソフトウェアとサービス

**SNMP MIB 監視:** エージェントシステム上の SNMP MIB (Management Information Base) 内のオブジェクトを監視したい場合は、システムに必ず SNMP エージェント (MIB-I および MIB-II 準拠) をインストールします。

## Solaris の前提条件

#### ユーザー

HP Operations エージェントを Solaris ノードにインストールするには、root 権限を持つユーザーを使用する必要があります。

#### 必要なソフトウェア

HP Operations エージェントを Solaris ノードにインストールする前に、以下のパッチ (または後継パッチ) がインストールされていることを確認します。

オペレーティングシステムのバージョン	プラットフォーム	必要なパッチ
10	32 ビット (x86)	<ul style="list-style-type: none"> <li>• 118345-03 SunOS 5.10_x86:ld &amp; libc.so.</li> <li>• 119964-03 SunOS 5.10_x86 Shared library patch for C++_x86</li> <li>• 120754-01 SunOS 5.10_x86 libmtsk</li> </ul>
	64 ビット (SPARC/x64)	<ul style="list-style-type: none"> <li>• 117461-04 Linker</li> <li>• 120753-01 libmtsk</li> <li>• 119963-19 SunOS 5.10:Shared library patch for C++</li> </ul>

さらに、以下のパッケージが利用できることを確認します。

SUNWlibC

SUNWlibms

SUNWmfrun

SUNWxwplt

#### ディスク容量

#### 新規インストールの場合

インストールディレクトリ用 (/opt/OV および /opt/perf):

350 MB

データディレクトリ用 (/var/opt/OV および /var/opt/perf):

350 MB

#### アップグレードの場合

インストールディレクトリ用 (/opt/OV および /opt/perf):

100 MB

データディレクトリ用 (/var/opt/OV および /var/opt/perf):

350 MB

**注:** インストールディレクトリまたはデータディレクトリに十分な容量がない場合、ln -s コマンドを使用して、インストールディレクトリまたはデータディレクトリから同じシステムの別の場所に対してシンボリックリンクを設定できます。

たとえば、/opt/OV ディレクトリから /new ディレクトリに対してシンボリックリンクを設定する場合は、次のようにします。

```
ln -s /new /opt/OV
```

#### 推奨されるソフトウェアとサービス

**SNMP MIB 監視:** エージェント システム上の SNMP MIB (Management Information Base) 内のオブジェクトを監視したい場合は、システムに必ず SNMP エージェント (MIB-I および MIB-II 準拠) をインストールします。

## AIX の前提条件

### ユーザー

HP Operations エージェント を AIX ノードにインストールするには、root 権限を持つユーザーを使用する必要があります。

### 必要なソフトウェア

- HP GlancePlus が正しく機能するには、**libC.a** ライブラリが必要となります。このライブラリは、AIX オペレーティングシステムの光磁気媒体に存在する **xlC.rte** パッケージにバンドルされています。
- 通信デーモンでは、**bos.perf.libperfstat** パッケージが必要となります。
- HPOM for Windows コンソールからリモートでエージェントをインストールしたい場合は、システムに OpenSSH 5.2 以降がインストールされていることを確認します。

### ディスク容量

#### 新規インストールの場合

インストールディレクトリ用 (**/usr/lpp/OV** および **/usr/lpp/perf**):

350 MB

データディレクトリ用 (**/var/opt/OV** および **/var/opt/perf**):

350 MB

#### アップグレードの場合

インストールディレクトリ用 (**/usr/lpp/OV** および **/usr/lpp/perf**):

350 MB

データディレクトリ用 (**/var/opt/OV** および **/var/opt/perf**):

350 MB

**注:** インストールディレクトリまたはデータディレクトリに十分な容量がない場合、**ln -s** コマンドを使用して、インストールディレクトリまたはデータディレクトリから同じシステムの別の場所に対してシンボリックリンクを設定できます。

たとえば、**/usr/lpp/OV** ディレクトリから **/new** ディレクトリに対してシンボリックリンクを設定する場合は、次のようにします。

```
ln -s /new /usr/lpp/OV
```

### 推奨されるソフトウェアとサービス

**SNMP MIB 監視:** エージェント システム上の SNMP MIB (Management Information Base) 内のオブジェクトを監視したい場合は、システムに必ず SNMP エージェント (MIB-I および MIB-II 準拠) をインストールします。

**xglance:** xglance ユーティリティを使用するには、システムに以下のコンポーネントが存在する必要があります。

- Open Motif 2.1 以降
- X11 Revision 6 (X11R6)

クロスパーティション メトリックを収集/記録するには、xmservd または xmtopas デーモンが使用可能である必要があります。xmtopas は、perfagent.tools ファイルセットの一部です。xmservd は、Performance Toolbox for AIX コンポーネント (ライセンスが必要なソフトウェアプログラム) にバンドルされています。

## ノードのアップグレード

### 11.00 よりも前のエージェントのアップグレード

HP Operations エージェント、HP Performance エージェント、HP GlancePlus の旧バージョン (11.00 よりも前) を HP Operations エージェント 11.10 にアップグレードできます。次のバージョンは直接 HP Operations エージェント 11.10 にアップグレードできます。

- HP Operations エージェント: 8.53, 8.60
- HP Performance エージェント: 4.70, 5.00
- HP GlancePlus: 4.70, 5.00

特定のバージョンより古いエージェント ソフトウェアがインストールされていると、HP Operations エージェント 11.10 のインストールは失敗します。8.53 より古い HP Performance エージェント、4.70 より古い HP Performance エージェント、4.70 より古い HP GlancePlus がインストールされたノードに HP Operations エージェント 11.10 をインストールする場合は、事前に以下のいずれかを実施します。

- HP Operations エージェント 11.10 にアップグレード可能なバージョンにエージェント ソフトウェアをアップグレードする。

これは、アップグレードで推奨される方法です。この場合、必要なパッケージとポリシーが確実にノードに残されます。

- エージェント ソフトウェアを完全に削除する。

この場合、ポリシーとインストールメンテーション ファイルがノードから削除される場合があります。HP Operations エージェント 11.10 へのアップグレードが完了したら、必要なポリシーとインストールメンテーション ファイルを必ずノードに再配布してください。

### 既存エージェントのバージョンの確認

*Windows の場合*

1. 管理者権限を使用して、ノードにログオンします。
2. HP Operations エージェントのバージョンをチェックします。
3. コマンド プロンプトを開きます。
4. 次のコマンドを実行します。

```
opcagt -version
```

コマンドの出力が A.8.53 より低いバージョンを示す場合は、HP Operations エージェント 11.10 のインストール前に、まず、バージョン 8.53 または 8.60 にアップグレードする必要があります (または、インストールされているバージョンを完全に削除してください)。

5. HP Performance エージェント のバージョンをチェックします。

- a. コマンド プロンプトを開きます。

- b. 次のコマンドを実行します。

```
perfstat -v
```

コマンドの出力として、HP Performance エージェント のさまざまなコンポーネントのバージョンが表示されます。**ovpa.exe** コンポーネントのバージョンが C.04.70 より低い場合は、HP Operations エージェント 11.10 のインストール前に、まず、バージョン 4.70 または 5.00 にアップグレードする必要があります (または、インストールされているバージョンの HP Performance エージェント を完全に削除してください)。

#### UNIX/Linux の場合

1. root 権限を使用して、ノードにログオンします。
2. HP Operations エージェントのバージョンをチェックします。
3. コマンド プロンプトを開きます。
4. 次のコマンドを実行します。

```
opcagt -version
```

コマンドの出力が A.8.53 より低いバージョンを示す場合は、HP Operations エージェント 11.10 のインストール前に、まず、バージョン 8.53 または 8.60 にアップグレードする必要があります (または、インストールされているバージョンを完全に削除してください)。

5. HP Performance エージェント のバージョンをチェックします。

- a. コマンド プロンプトを開きます。

- b. 次のコマンドを実行します。

```
perfstat -v
```

コマンドの出力として、HP Performance エージェント のさまざまなコンポーネントのバージョンが表示されます。**ovpa** コンポーネントのバージョンが C.04.70 より低い場合は、HP Operations エージェント 11.10 のインストール前に、まず、バージョン 4.70 または 5.00 にアップグレードする必要があります (または、インストールされているバージョンの HP Performance エージェント を完全に削除してください)。

6. HP GlancePlus のバージョンをチェックします。

- a. コマンド プロンプトを開きます。

- b. 次のコマンドを実行します。

```
perfstat -v
```

コマンドの出力として、HP Performance エージェント と HP GlancePlus のさまざまなコンポーネントのバージョンが表示されます。**glance** コンポーネントのバージョンが C.04.70 より低い場合は、HP Operations エージェント 11.10 のインストール前に、まず、バージョン 4.70 または 5.00 にアップグレードする必要があります (または、インストールされているバージョンの HP GlancePlus を完全に削除してください)。

#### HP Operations エージェント 11.10 によるデータの収集/保存

古いバージョンの HP Operations エージェント (11.00 よりも前) は、約 50 のメトリックの形式でシステムパフォーマンスデータを、組み込みパフォーマンスコンポーネント (EPC) に保存します。このコンポーネントは、**coda** と呼ばれます。HP Performance エージェント は、500 を超えるシステムパフォーマンスメトリックを収集し (**scope** コレクタを使用)、ログファイルベースのストレージメカニズムを利用してデータを保存します。バージョン 11.10 の HP Operations エージェント は、HP Performance エージェント のデータ収集/保存メカニズムを採用しているため、より多くのメトリックセットを収集し、メトリックデータをログファイルベースのデータストアに保存します。ただし、外部プログラムや HPOM ポリシー内での EPC への参照は、scope コレクタとログファイルベースのデータストアに向けられます。これにより、過去に配布したすべてのポリシーと統合は、古いバージョンの HP Operations エージェント (11.00 よりも前) から HP Operations エージェント 11.10 にアップグレードした後も、中断なくシームレスに機能し続けます。

#### **coda のバージョンの確認**

システムで使用できる coda のバージョンが 10.50.215 から 10.50.245 の場合は、HP Reporter や HP Performance Insight などのデータ分析ツールを使って coda データのバックアップを作成することをお勧めします。coda のバージョンを確認するには、ログディレクトリ (Windows では %ovdatadir%\log、UNIX/Linux では /var/opt/OV/log) にある **coda.txt** ファイルを開き、coda のバージョン (Starting CODA 文の横) を確認します。

#### **Solaris SPARC 管理対象ノードがある Solaris SPARC 管理サーバーでのアップグレード**

Solaris SPARC HPOM 管理サーバーを使用し、HP Software Security Core (HPOvSecCo) コンポーネントバージョン 06.20.050 を搭載する HP Operations エージェント 8.60 が管理サーバーにインストールされている場合、環境内にあるすべての Solaris SPARC 管理対象ノード上のエージェントをバージョン 11.10 にアップグレードし、管理サーバーのエージェントをバージョン 11.10 にアップグレードする必要があります。アップグレードしないと、管理サーバーのエージェントをバージョン 11.10 にアップグレードするまで、(エージェント 8.60 がインストールされている) Solaris SPARC ノードと (エージェント 11.10 がインストールされている) 管理サーバー間の通信が失敗します。

さらに、環境にある SPARC 管理対象ノード上のエージェントをバージョン 11.10 にアップグレードする前に、管理サーバーにホットフィックス QCCR1A97520 を適用する必要があります。

SPARC ノードで SPARC HPOM 管理サーバーを使用する場合、以下の手順を実行します。

1. root 権限で管理サーバーにログオンします。
2. 次のコマンドを実行して、管理サーバー上の HP Software Security Core (OvSecCo) コンポーネントのバージョンを確認します。

```
strings /opt/OV/lib/libOvSecCore.so | grep FileV
```

コマンド出力に HPOvSecCo のバージョンが 06.20.050 と表示されたら、ホットフィックス QCCR1A97520 を管理サーバーに適用します (このホットフィックスを取得するには HP サポートにお問い合わせください)。他のバージョンが表示される場合は、アップグレードを続行します。

このホットフィックスを適用すると、HP Operations エージェント 11.10 が搭載された SPARC ノードが、HPOvSecCo コンポーネントバージョン 06.20.050 を搭載する SPARC 管理サーバーと通信できるようになります。SPARC 管理サーバーにこのホットフィックスをインストールしないと、管理サーバー上のエージェントをバージョン 11.10 にアップグレードするまで、HP Operations エージェント 11.10 が搭載された SPARC ノードは SPARC 管理サーバーと通信できません。

次のコマンドを実行して、管理サーバー上の HPOvSecCo コンポーネントのバージョンが 06.20.077 にアップグレードされていることを確認します。

```
strings /opt/OV/lib/libOvSecCore.so | grep FileV
```

コマンド出力に HPOvSecCo コンポーネントのバージョンが 06.20.077 と表示されます。

## プレインストールタスク: クラスタ内の HPOM に HP Operations エージェントをインストールするには

高可用性 (HA) クラスタ環境にインストールした場合、クラスタ内のアクティブなシステムが他のシステムにフェールオーバーするときに、HP Operations エージェントはフェールオーバーしません。ただし、HP Operations エージェントにより、クラスタ内で稼働するクラスタ対応アプリケーションを監視することができます。

HP Operations エージェントは、クラスタに属するすべてのノードにインストールする必要があります。エージェントをクラスタにインストールする場合、追加の手順や特別な設定は一切必要ありません。しかし、クラスタ内で稼働する HPOM 管理サーバーにエージェントをインストールするには、追加の設定手順が必要となります。

### HPOM for Windows の場合

1. HPOM データベースが起動され稼働していることを確認します。
2. 管理権限でアクティブな管理サーバーにログオンします。
3. 以下のコマンドを実行し、アクティブノードを保守停止モードに設定します。

```
ovownodeutil -outage_node -unplanned -node_name <ノードのFQDN>
```

4. [「HPOM コンソールからのインストール」\(30ページ\)](#) または [「ノードへの HP Operations エージェントの手動インストール」\(31ページ\)](#) の指示に従って、アクティブサーバーにエージェントをインストールします。
5. クラスタ内の各ノードでステップ 4 とステップ 5 を実行します。

### 上記形式の説明

<ノードのFQDN> は、アクティブノードの完全修飾ドメイン名です。

### UNIX/Linux の HPOM の場合

1. root 権限でアクティブな管理サーバーにログオンします。
2. ノードを保守モードに設定し、アクティブノードの HA リソースグループの監視を無効にします。  
アクティブノードで、以下のコマンドを実行します。

```
/opt/OV/sbin/ovharg -monitor <HA リソースグループ名> disable
```

### 上記形式の説明

<HA リソースグループ名> は、HPOM 管理サーバーの HA リソースグループです。

3. [「HPOM コンソールからのインストール」\(30ページ\)](#) または [「ノードへの HP Operations エージェントの手動インストール」\(31ページ\)](#) の指示に従って、アクティブサーバーにエージェントをインストールします。  
インストール時に共有ディスクがマウントされていないことを確認してください。
4. クラスタ内の各ノードでステップ 2 とステップ 3 を実行します。

## 第4章

---

### HPOM コンソールからのインストール

**注:** (`root` ユーザーがデフォルトで無効になっている) vSphere Management Assistant (vMA) ノードのインストールにはこの方法を使用しないでください。vMA ノードにはエージェントを手動でインストールしてください。

ノードで他の HP ソフトウェアをホストする場合、エージェントをインストールする前に製品のプロセスがすべて停止していることを確認してください。エージェントのインストールが完了した後に、プロセスを開始できます。

#### HPOM for Windows の場合

HPOM コンソールから管理対象ノードに HP Operations エージェントをインストールするには、*HPOM for Windows* のオンラインヘルプの「リモート エージェントのインストール」のトピックに従います。

#### UNIX/Linux の HPOM の場合

UNIX/Linux 上の HPOM から管理対象ノードに HP Operations エージェントをインストールするには、*HPOM for UNIX/Linux* オンラインヘルプの「New Agent Installation」のトピックに従います。

## 第5章

### ノードへの HP Operations エージェント の手動インストール

#### タスク 1: インストールを準備する

HP Operations エージェント をインストールする前に、*HP Operations エージェント* および *Infrastructure SPI 11.10* メディアをノードに抽出するか、マウントする必要があります。

または、エージェント配布パッケージを HPOM 管理サーバーから手動で転送することもできます。

#### Windows 管理サーバーから配布パッケージを転送するには

1. ノードが管理対象ノードとして追加されていることを、HPOM コンソールで確認します。
2. 管理サーバーにディレクトリを作成し、そのディレクトリに移動します。
3. 次のコマンドを実行します。

```
ovpmutil dnl pkg Operations-agent /pnn <ノードのFQDN>
```

この場合、<ノードのFQDN> は、ノードの完全修飾ドメイン名です。

ノードの配布パッケージは、現在のディレクトリにダウンロードされます。

4. このディレクトリを管理サーバーからノードの一時ディレクトリに転送します。

#### UNIX/Linux 管理サーバーから配布パッケージを転送するには

1. 管理サーバーにログオンし、次に以下のディレクトリに移動します。

```
/var/opt/OV/share/databases/OpC/mgd_  
node/vendor/<vendor>/<arch>/<ostype>/A.11.10.000
```

上記形式の説明

<ベンダー>: オペレーティングシステムのベンダーの名前。

<アーキテクチャ>: ノードのアーキテクチャ。

<OS タイプ>: ノードのオペレーティングシステム。

以下の表は、<ベンダー>/<アーキテクチャ>/<OS タイプ>の使用可能な組み合わせのリストを示しています。

オペレーティングシステム	アーキテクチャ	選択可能な組み合わせ
Windows	Itanium	ms/ipf64/win2k3
Windows	x86_64	ms/x64/win2k3
Windows	x86	ms/x86/winnt
Linux	Itanium	linux/ipf64/linux26
Linux	x86_64	linux/x64/linux26

オペレーティングシステム	アーキテクチャ	選択可能な組み合わせ
Linux	x86	linux/x86/linux26
Linux	PowerPC (64 ビット)	linux/powerpc/linux26
HP-UX	Itanium	hp/ipf32/hpux1122
HP-UX	PA-RISC	hp/pa-risc/hpux1100
Solaris	SPARC	sun/sparc/solaris7
Solaris	x86	sun/x86/solaris10
AIX	PowerPC (32 ビット)	ibm/rs6000/aix5
AIX	PowerPC (64 ビット)	ibm/rs6k64/aix5

- RPC\_BBC ディレクトリの内容 (A.11.10.000 ディレクトリに存在) をノードの一時ディレクトリに転送します。

#### オプション: プロファイル ファイルの準備

##### プロファイル ファイルについて

インストール (手動インストール) 中にプロファイルファイルを使用して、デフォルト以外の設定を使用して実行するようにエージェントをプログラムできます (通信ポート、イベント インターセンクタ、ライセンス タイプなど)。プロファイルファイルは、マニュアルに示されている手順に従って、手動で作成する必要があります。

- エージェントをインストールするシステムで新しいファイルを作成して、そのファイルをテキスト エディタで開きます。
- デフォルト以外の値を使用する場合は、次の構文を入力して、エージェント変数を設定します。

```
set <namespace>:<variable>=<value>
```

上記形式の説明

<namespace> は設定変数の名前空間です

<variable> は設定する変数です

<value> は変数に割り当てる値です

- ローカルディレクトリにファイルを保存します。

##### インストール中に設定できる主な機能

- エージェント ユーザー:** インストール時に、エージェントを実行するユーザーを設定できます。MODE 変数を使用すると、システムを実行中にエージェントが使用できるデフォルト以外のユーザーを選択できます。

root 以外のユーザーや権限のないユーザーを使用して実行するようにエージェントを設定するには、次の内容を追加します。

**set eaagt:MODE=NPU**

root 以外のユーザーや権限のないユーザーを使用して Operations Monitorin Component だけを実行するようにエージェントを設定するには、次の内容を追加します (他のエージェントは root または Local System で実行されます)。

**set eaagt:MODE=MIXED**

さらに、同様の方法で変数一式を設定し、デフォルト以外のユーザーでエージェントを実行できるようにする必要があります。詳細については、『HP Operations エージェント ユーザーガイド』の「インストール中のエージェント ユーザーの設定」のセクションを参照してください。

- **ライセンス:** (HPOM コンソールを使用せずに) エージェントをノードにインストールする場合、インストール後に評価ライセンスは自動で有効にはなりません。インストール時にプロファイルファイルでライセンス固有の変数を設定し、必要な使用ライセンス (LTU) を適用できます。

たとえば、HP Operations OS Inst Adv SW LTU を永続的に適用する場合、次の内容を追加します。

**set eaagt.license:HP\_Operations\_OS\_Inst\_Adv\_SW\_LTU=PERMANENT**

インストール時にプロファイルファイルを使用してライセンスを適用する方法の詳細については、『HP Operations エージェント ライセンスガイド』を参照してください。

**タスク 2:HP Operations エージェント をインストールする**

**注:** ノードで他の HP ソフトウェアをホストする場合、エージェントをインストールする前に製品のプロセスがすべて停止していることを確認してください。エージェントのインストールが完了した後に、プロセスを開始できます。

1. root または管理者としてノードにログオンします。
2. HP Operations エージェントおよび Infrastructure SPI 11.10 メディアからインストールする場合は、以下の手順に従います。
  - a. メディアのルートに移動します。
  - b. プロファイルファイルを使用せずにインストールするには、次のコマンドを実行します。

Windows の場合:

```
cscript oainstall.vbs -i -a -s <management_server> [-cs <certificate_server>][-install_dir <install_directory> -data_dir <data_directory>]
```

UNIX/Linux の場合:

```
./loainstall.sh -i -a -s <management_server> [-cs <certificate_server>]
```

- c. プロファイルファイルを使用してインストールするには、次のコマンドを実行します。

Windows の場合:

```
cscript oainstall.vbs -i -a -agent_profile <path>\<profile_file> -s <management_server>
[-cs <certificate_server>] [-install_dir <install_directory> -data_dir <data_directory>]
```

UNIX/Linux の場合:

```
./loainstall.sh -i -a -agent_profile <path>/<profile_file> -s <management_server> [-cs
<certificate_server>]
```

**ヒント:** Windows の場合、.vbs スクリプトを実行しないときには、代わりに以下の手順に従います。

- メディアのルート ディレクトリから、packages\WIN ディレクトリに移動します。

- ノードのアーキテクチャに応じて、適切なディレクトリに移動します (x64 プラットフォームの場合は Windows\_X64、x86 プラットフォームの場合は Windows\_X86)。

Microsoft Visual C++ Redistributable Package がシステムにインストールされていない場合は、Microsoft Visual C++ Redistributable Package 用の実行可能ファイル (このディレクトリに存在) を実行します。

- 次のコマンドを実行します。

```
oasetup -install -management_server <management_server> [-certificate_
server <certificate_server>] [-install_dir <install_directory> -data_dir <data_
directory>]
```

または

```
oasetup -install -management_server <management_server> [-certificate_
server <certificate_server>] -agent_profile <path>\<profile_file> [-install_dir
<install_directory> -data_dir <data_directory>]
```

3. エージェント配布パッケージを HPOM 管理サーバーから手動で転送した場合には、以下の手順に従います。

a. 配布パッケージを格納したノードのディレクトリに移動します。

b. 次のコマンドを実行します。

Windows の場合:

```
oasetup -install -management_server <management_server> [-certificate_server
<certificate_server>][-install_dir <install_directory> -data_dir <data_directory>]
```

UNIX/Linux の場合:

i. **chmod u+x oasetup.sh**

ii. **./loasetup.sh -install -management\_server <management\_server> [-certificate\_server <certificate\_server>]**

プロファイルファイルを使用してインストールするには、-install の後に、-agent\_profile <path>\<profile\_file> を追加します。

上記形式の説明

<管理サーバー>: 管理サーバーの FQDN。

<証明書サーバー>: 証明書サーバーの FQDN。

<インストールディレクトリ>: すべてのパッケージとバイナリファイルをノードに配置するためのパス。

<データ ディレクトリ>: すべてのデータと設定ファイルをノードに配置するためのパス。

<path> はプロファイル ファイルへのパスです。

<profile\_file> はプロファイル ファイルの名前です。

**ヒント:** `oainstall` と `oasetup` プログラムは、インストールプロセスをトレースするオプションを提供します。エージェントのインストールが失敗し、失敗の原因を検出できない場合は、トレースオプションを付けてインストーラを実行すると、トレースファイルを生成することができます。生成されたトレースファイルは、詳細な分析のために HP サポートに送付することができます。

インストールプロセスをトレースするには、次の追加オプションを指定して前述のコマンドを実行してください。

#### **-enabletrace ALL**

たとえば、次のようになります。

```
./oainstall.sh -i -a -agent_profile /root/profile/profile_file -s  
test_system1.domain.com -enabletrace ALL
```

トレースファイル(.trc という拡張子)は、次の場所にあります。

#### *Windows の場合*

%ovdatadir%Temp

#### *UNIX/Linux の場合*

/var/opt/OV/tmp

HPOM 管理サーバーにエージェントをインストールする場合、インストール後にすべての HPOM プロセスを再起動する必要があります。

#### パッケージの配置

HP Operations エージェントをスタンドアロンサーバーにインストールすると、インストーラプログラムでは必要なすべてのパッケージとファイルを以下の場所に配置します。

- Windows の場合:
  - %ovinstalldir%
  - %ovdatadir%
- HP-UX、Linux、Solaris の場合:
  - /opt/OV
  - /opt/perf
  - /var/opt/OV
  - /var/opt/perf
- AIX の場合
  - /usr/lpp/OV
  - /usr/lpp/perf

- /var/opt/OV
- /var/opt/perf

#### インストールログファイル

インストーラによってインストールログファイル(oainstall.log)が次のディレクトリに配置されます。

- Windows の場合: %ovdatadir%\log
- UNIX/Linux の場合: /var/opt/OV/log

#### インストールの確認

HP Operations エージェントをインストールしたら、インストールログファイル(oainstall.log)の内容を確認します。インストールが成功している場合は、ファイルにはエラーがなく、ファイルの最後の方に次のメッセージが表示されています。

```
HP Operations agent installation completed successfully
```

## NAT 環境でのインストール後のタスク

ネットワークアドレス変換 (NAT) 環境にあるノードにエージェントをインストールする場合は、ノードの追加時に HPOM で使用された IP アドレスを使用するように、ノード上のエージェントを設定する必要があります。

HPOM に設定された IP アドレスを使用するようにエージェントを設定するには、以下の手順を実行します。

1. root 権限または管理権限でノードにログオンします。
2. 以下のディレクトリに移動します。

#### Windows の場合

```
%ovinstalldir%bin
```

#### HP-UX、Linux、Solaris の場合

```
/opt/OV/bin
```

#### AIX の場合

```
/usr/lpp/OV/bin
```

3. 次のコマンドを実行します。

```
ovconfchg -ns eaagt -set OPC_IP_ADDRESS <IP アドレス>
```

この <IP アドレス> は、管理対象ノードのリストにノードを追加するときに HPOM に設定した、ノードの IP アドレスです。

4. 以下のコマンドを実行してエージェントを再起動します。
  - a. ovc -kill
  - b. ovc -start

## 第6章

---

### 非アクティブモードでのエージェントのインストール

#### 非アクティブモードについて

管理対象ノードにローカルにインストールしている最中、エージェント インストーラをプログラムして、コンポーネントを設定せずに、必要なファイルとパッケージだけをノードに配置するように選択できます。その結果、エージェントの実行は自動的に開始されず、非アクティブのままになります。後で、インストーラプログラムをもう一度使用して、エージェントを設定して開始する必要があります。

この方法を使用する利点は、HP Operations エージェント が非アクティブモードでインストールされているシステムのイメージのクローンを作成できることです。事前にインストールされている HP Operations エージェント でシステムのクローンを作成すると、管理対象ノードのリストにシステムを追加した後で、システムにエージェントをインストールする必要がありません。

#### HP Operations エージェント を非アクティブモードでインストールする

インストールの非アクティブモードを使用すると、インストール後にエージェントの操作が開始されません。

HP Operations エージェントをインストールするには

1. root または管理者としてノードにログオンします。
2. *HP Operations エージェント* および *Infrastructure SPI 11.10* メディアからインストールする場合は、以下の手順に従います。
  - a. メディアのルートに移動します。
  - b. 次のコマンドを実行します。

*Windows* の場合:

```
cscript oainstall.vbs -i -a -defer_configure [-install_dir <install_directory> -data_dir <data_directory>]
```

*UNIX/Linux* の場合:

```
./loainstall.sh -i -a -defer_configure
```

上記形式の説明

<インストールディレクトリ>: すべてのパッケージとバイナリファイルをノードに配置するためのパス。

<データディレクトリ>: すべてのデータと設定ファイルをノードに配置するためのパス。

#### 後でエージェントを設定する

エージェントをアクティブモードに設定するには、HP Operations エージェント の設定詳細 (HPOM 管理サーバーおよび証明書サーバーの情報など) を指定して設定する必要があります。oainstall プログラムの `-configuration` オプションを使用すると、このタスクを実行できます。

エージェントの運用を開始したいときは、以下の手順に従います。

1. 以下のディレクトリに移動します。

Windows 64 ビット ノードの場合:

```
%ovinstalldir%bin\win64\OpC\install
```

その他の Windows ノードの場合:

```
%ovinstalldir%bin\OpC\install
```

HP-UX、Linux、Solaris ノードの場合:

```
/opt/OV/bin/OpC/install
```

AIX ノードの場合:

```
/usr/lpp/OV/bin/OpC/install
```

2. 次のコマンドを実行します。

Windows の場合

```
cscript oainstall.vbs -a -configure -s <management_server> [-cs <certificate_server>]
```

または

```
oasetup -configure -management_server <management_server> [-certificate_server <certificate_server>]
```

UNIX/Linux の場合

```
./oainstall.sh -a -configure -s <management_server> [-cs <certificate_server>]
```

HPOM for Windows 管理サーバーからのエージェントのリモートでの設定

-defer\_configure オプションを指定して HP Operations エージェントをインストールした場合、エージェントが HPOM 管理サーバーと連携して動作するように、後で設定する必要があります。ノードのエージェントはローカルで設定するか、または HPOM for Windows 管理サーバーからリモートで設定することができます。

エージェントをリモートで設定するには

1. SSH クライアントを設定します。

**注:** HPOM for Windows では、サードパーティ製 SSH クライアントソフトウェア PuTTY が提供されています。ここでは、PuTTY SSH クライアントの設定手順について説明します。PuTTY は HP のソフトウェアではありません。このソフトウェアは保証なしで提供されています。したがって、PuTTY の使用または性能に関するすべての損害は、お客様の責任となります。

2. 管理サーバーの %ovinstalldir%\contrib\OVOW\PuTTY ディレクトリから、PLINK.EXE、PSCP.EXE、および runplink.cmd ファイルを、PATH 環境変数に含まれている任意のディレクトリにコピーします。たとえば、管理サーバーが C:\Program Files\HP\HP BTO Software にインストールされている場合は、次のディレクトリにファイルをコピーします。C:\Program Files\HP\HP BTO Software\bin
3. ユーザーを作成します。エージェントをリモートでインストールする際に、HPOM はノードに対する管理アクセス権を持つユーザーの資格情報を必要とします。次のリストは、ノードのオペレーティングシステムに応じて必要となる具体的な権限を示しています。

- Windows
  - ADMIN\$ 共有 への書き込みアクセス (ユーザーはローカル Administrators グループのメンバーであること)
  - レジストリの読み取りアクセス
  - 「サービスとしてログオン」の権限 ([資格情報の設定] リストで [ユーザー/パスワード] を選択する場合にのみ必要)
- UNIX/Linux
  - ファイルを転送するためにノード上のSSHにログインする権限、およびインストールコマンドを実行する権限

#### 4. エージェントを設定します。

*Windows 64 ビット ノードの場合*

```
ovdeploy -cmd "%ovinstalldir%\bin\win64\OpC\install\oasetup -configure -management_server <management_server> -certificate_server <certificate_server>" -node <node_name> -fem winservice -ostype Windows -user <node_user> -pw <node_passwd>
```

*それ以外のWindows ノードの場合*

```
ovdeploy -cmd "%ovinstalldir%\bin\OpC\install\oasetup -configure -management_server <management_server> -certificate_server <certificate_server>" -node <node_name> -fem winservice -ostype Windows -user <node_user> -pw <node_passwd>
```

*HP-UX、Linux、Solaris ノードの場合*

```
ovdeploy -cmd "/opt/OV/bin/OpC/install/oainstall.sh -a -configure -srv <management_server> -cs <certificate_server>" -node <node_name> -fem ssh -ostype UNIX -user <node_user> -pw <node_passwd>
```

*AIX ノードの場合*

```
ovdeploy -cmd "/usr/lpp/OV/bin/OpC/install/oainstall.sh -a -configure -srv <management_server> -cs <certificate_server>" -node <node_name> -fem ssh -ostype UNIX -user <node_user> -pw <node_passwd>
```

上記形式の説明

<管理サーバー>: 管理サーバーの完全修飾ドメイン名。

<証明書サーバー>: 証明書サーバーの完全修飾ドメイン名。このパラメータはオプションです。-cs オプションを指定しなかった場合は、管理サーバーがノードの証明書サーバーになります。

<ノード名>: ノードの完全修飾ドメイン名。

<ノードのユーザー>: ノードでエージェントを設定可能なユーザー。作成されたユーザーです。

<ノードのパスワード>: 上記ユーザーのパスワード。



## 第7章

---

### HP Operations エージェント の証明書 の設定

暗号化を伴う SSL (Secure Socket Layer) プロトコルを使用してネットワーク通信を円滑に実施するには、すべての管理対象ノードに証明書をインストールする必要があります。証明書により、ノードは管理サーバーや他のノードと安全に通信を行うことができます。

管理サーバーはノードに証明書を発行し、認証局として機能することができます。各管理対象ノードは、管理サーバーから次の証明書を取得する必要があります。

**固有のノード証明書。**ノードは、この証明書を管理サーバーや他のノードに送信することで自身を証明します。

**管理サーバーの信頼済み証明書のコピー。**ノードが管理サーバーからの通信を承認するのは、対象の管理サーバーの信頼済み証明書を保有している場合に限られます。

複数の管理サーバーが存在している環境では、他のすべての管理サーバーに関する信頼済み証明書のコピーがノードに存在する必要があります。

HPOM 管理環境で、ノードが証明書を使用して安全に通信するには、エージェントをノードにインストールした後で証明書をインストールする必要があります。

### インストールキーによる証明書要求

証明書要求を暗号化するために、インストールキーを使用することができます。管理サーバー上でインストールキーを生成し、それをノードに転送することができます。

インストールキーを使用して証明書を要求する前に、ノードで HP Operations エージェントが稼働していることを確認してください。エージェントは起動時に、証明書要求を送信します。その後、インストールキーを用いて証明書を要求すると、管理サーバー上の元の証明書要求が新しい証明書要求で上書きされます。エージェントのインストールでデフォルトを使用するか、または `ovconfchg` ユーティリティを使用することにより、`sec.cm.client` 名前空間の `CERTIFICATE_DEPLOYMENT_TYPE` パラメータに `manual` をセットし、初回の証明書要求を抑制することができます。

インストールキーで証明書を要求するには

1. HPOM Administrators グループに属するアカウントを使用し、管理サーバーにログインします。
2. コマンド プロンプト (シェル) を開きます。
3. 次のコマンドを実行します。

*HPOM for Windows の場合*

```
ovowcsacm -genInstKey [-file <file_name>] [-pass <password>]
```

*HPOM for UNIX、または UNIX/Linux における HPOM の場合*

```
opccsacm -genInstKey [-file <file_name>] [-pass <password>]
```

上記形式の説明

<ファイル名>:インストールキー ファイルの名前。

<パスワード>:このパスワードは、後でノードに証明書を要求する際に必要になります。このオプションは省略できます。

このコマンドにより、インストールキーが生成されます。

**注:** <ファイル名>には完全なパスを指定します。完全なパスでない場合、証明書は現在の作業ディレクトリに格納されます。-file オプションを指定しない場合、証明書は <データディレクトリ>\shared\server\certificates に格納されます。

4. 生成されたファイルを安全な方法でノードに移動します。インストールキーはいずれのノードに対しても有効です。
5. ノードのインストールに使用したアカウントで、ノードにログインします。
6. コマンドプロンプト (シェル)を開きます。
7. UNIX/Linux ノードでは、必ず PATH 変数に <インストールディレクトリ>/bin ディレクトリに対するパスが含まれるようにします。
8. 次のコマンドを実行します。

```
ovcert -certreq -instkey <ファイル名>
```

管理サーバーは要求を許可します。この処理は、自動または手動で行われるように設定できます。その後、管理サーバーはノードに証明書を送信します。

高可用クラスタに存在するエージェントノードでは、次のコマンドを実行します。

```
ovc -restart ovconfd
```

## 自動での証明書の要求

HPOM コンソールからエージェントをノードに配布すると、ノードは自動で管理サーバーに証明書を要求します。ノードは鍵を使用して、証明書要求を暗号化します。

次に管理サーバーは、証明書要求を許可します。この処理は、自動で行われるように設定することができます。要求を許可すると、管理サーバーは証明書をノードに送信します。管理サーバーが証明書要求を拒否した場合、以下のコマンドを管理対象ノードで実行し、再度要求を送信することができます。

```
ovcert -certreq
```

管理サーバーエージェントで証明書の要求が許可されたら、高可用クラスタに存在するエージェントノードで、次のコマンドを実行します。

```
ovc -restart ovconfd
```

安全性が高い環境では、証明書配布のタイプを手動に設定し、自動での証明書要求を無効にすることができます。その場合、インストールキーを使用して証明書を要求するか、または証明書を手動で配布する必要があります。

## 手動での証明書の配布

ノードは自動的に、証明書要求を管理サーバーに送信することができます。証明書をノードに手動でインストールしたい場合は、ノード上の (sec.cm.client 名前空間の) CERTIFICATE\_DEPLOYMENT\_TYPE 変数に MANUAL をセットします。

手動で証明書を配布するには

1. HPOM Administrators グループに属するアカウントを使用し、管理サーバーにログインします。
2. コマンド プロンプト (シェル) を開きます。
3. ノードがHPOM コンソールの管理対象ノード リストに追加されていることを確認します。
4. 次のコマンドを実行します。

*HPOM for Windows の場合*

```
ovowcsacm -issue -name <node_name> [-file <file_name>] [-coreid <OvCoreId>] [-pass <password>]
```

*HPOM for UNIX の場合*

```
opccsacm -issue -file <file_name> [-pass <password>] -name <node_name> [-coreid <OvCoreId>]
```

**注:** <ファイル名>には完全なパスを指定します。完全なパスでない場合、証明書は現在の作業ディレクトリに格納されます。-file オプションを指定しない場合、証明書は <データディレクトリ>\shared\server\certificates に格納されます。

上記形式の説明

<ノード名>:ノードのFQDN、またはIPアドレス。

<OV コアID>:ノードのコアID。エージェントがすでにインストールされているノードのコアIDを取得するには、管理サーバーで以下の手順を実行します。

*HPOM for UNIX、または UNIX/Linux における HPOM の場合*

次のコマンドを実行します。

```
opcnode -list_id node_list=<ノード名>
```

*HPOM for Windows の場合*

コンソールツリーでノードを右クリックし、次に **[プロパティ]** をクリックします。ノード プロパティ ダイアログボックスが開きます。ノード プロパティ ダイアログボックスで、[全般] タブに移動し、**[詳細設定]** をクリックします。[詳細設定] ダイアログボックスが開き、ノードのコアIDが表示されます。

<ファイル名>:コマンドにより生成される証明書ファイルの名前。このオプションを指定しない場合、コマンドは以下のディレクトリにデフォルトのファイル名「<ノード名>-<OvCoreId>.p12」でファイルを作成します。

*HPOM for UNIX、または UNIX/Linux における HPOM の場合*

```
/var/opt/OV/temp/OpC/certificates
```

*HPOM for Windows の場合*

```
%OvShareDir%server\certificates
```

5. 生成されたファイルを安全な方法でノードに移動します。インストールキーはいずれのノードに対しても有効です。
6. エージェントがまだノードにインストールされていない場合は、インストールします。プロファイルファイルベースのインストールを使用し、CERTIFICATE\_DEPLOYMENT\_TYPE 変数に manual をセットします。また、管理サーバーで生成されたものと同じ OvCoreID を使用します

(sec.cm.client 名前空間の CERTIFICATE\_SERVER\_ID に管理サーバーで生成された ID をセットします)。

7. ノードでコマンド プロンプト (シェル) を開きます。
8. ノードでエージェントが稼働している場合、以下のコマンドを実行します。

```
ovc -stop
```

9. 生成されたファイルから証明書をインポートするには、以下のコマンドを実行します。

```
ovcert -importcert -file <ファイル名>
```

10. 以下のコマンドをノードで実行します。

```
ovc -start
```

証明書をインポートしたら、高可用クラスタに存在するエージェント ノードで、次のコマンドを実行します。

```
ovc -restart ovconfd
```

## 証明書の復元

ノードで証明書を紛失した場合は、再度作成する必要があります。既存の証明書をファイルにバックアップしている場合は、証明書に不具合が生じたときにそれを復元することができます。証明書をバックアップするには、以下の手順に従います。

1. root 権限または管理権限でノードにログオンします。
2. コマンド プロンプト (シェル) を開きます。
3. 次のコマンドを実行します。

```
ovcm -exportcacert -file <file_name> [-pass <password>]
```

4. このコマンドにより、管理サーバーの証明書が -file オプションで指定したファイルにバックアップされます。
5. 次のコマンドを実行します。

```
ovcert -exporttrusted [-ovrg <server>] -file <file_name>
```

6. ここで <サーバー> は、管理サーバーが HA クラスタにインストールされている場合、HA リソースグループ名となります。

このコマンドにより、管理サーバーの信頼済み証明書が -file オプションで指定したファイルにバックアップされます。

7. 以下のコマンドを実行し、ノード証明書のエイリアスを決定します。

```
ovcert -list [-ovrg <server>]
```

ノード証明書のエイリアスは長い文字列であり、出力の Certificates セクションの下に表示されます。たとえば、次のようになります。

```
+-----+
| Keystore Content | +-----+
-----+
```

```
| Certificates:| cdc7b5a2-9dd6-751a-1450-eb556a844b55 (*) | +-----+
-----+
| Trusted Certificates: |
| CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55 | +-----+
-----+
```

8. 次のコマンドを実行します。

**ovcert -exportcert -file <file\_name> -alias <alias> [-pass <password>]**

このコマンドにより、ノード証明書が -file オプションで指定したファイルにバックアップされます。

管理サーバー証明書を復元するには、以下のコマンドを実行します。

**ovcm -importcacert -file <file\_name> [-pass <password>]**

信頼済み証明書を復元するには、以下のコマンドを実行します。

**ovcert -importtrusted -file <file\_name>**

ノード証明書を復元するには、以下のコマンドを実行します。

**ovcert -importcert -file <file\_name> [-pass <password>]**

## 第8章

---

### 高可用性クラスタにおける HP Operations エージェント

HP Operations エージェントを使用して、高可用性 (HA) クラスタ内でノードを監視することができます。HA クラスタ内でクラスタ対応アプリケーションを監視するには、以下のガイドラインに従ってエージェントを配備する必要があります。

クラスタ内のすべてのノードは、HPOM コンソールの管理対象ノードのリストに存在する必要があります。

HP Operations エージェントは、HA クラスタ内のすべてのノードにインストールする必要があります。

ノードで MAX\_RETRIES\_FOR\_CLUSTERUP 変数 (conf.cluster 名前空間の下) を整数値に設定する必要があります。プロファイルファイルベースのインストールを使用すると、インストール時において、すべてのノードに適切な値の変数を確実に設定できます。

**仮想ノード。** HPOM for UNIX 8.3x、HPOM on UNIX/Linux 9.1x、または HPOM for Windows 9.00 でノードを使用する場合は、仮想ノードという概念を利用することができます。仮想ノードは、共通のリソースグループでリンクされた物理ノードのグループです。リソースグループの変更に基づいて、エージェントは自動的に物理ノード上のポリシーを有効化または無効化することができます。

仮想ノード機能は、HPOM for Windows 8.1x では利用できません。

HA クラスタ内でノードを監視するには、すべての物理ノードにではなく、仮想ノードにのみ監視ポリシーを配布します。したがって、クラスタ対応アプリケーションの監視を開始する前に、HPOM コンソールで HA クラスタに仮想ノードを作成することが重要です。

次に、HPOM コンソールで仮想ノードを作成するためのガイドラインを示します。

- 仮想ノードは、物理ノード自体とすることはできません。
- 仮想ノードは、DHCP、自動配布、および証明書をサポートしません。
- エージェントを仮想ノードにインストールすることはできません。

#### HA クラスタ内のノードの監視

HP Operations エージェントを設定し、HA クラスタ内のノードで稼働するクラスタ対応アプリケーションを監視することができます。

HA クラスタ内のノード上のクラスタ対応アプリケーションを監視するには、以下の手順に従います。

1. (Microsoft Cluster Server クラスタのみ) 監視対象リソースを含むリソースグループに、ネットワーク名と IP アドレスリソースの両方が含まれることを確認します。
2. クラスタ対応アプリケーションを監視するために必要となるポリシーを特定します。
3. クラスタ対応アプリケーションを記述する XML ファイルを作成し、その名前を **apminfo.xml** にします。
4. このファイルは、監視対象となるリソースグループを定義し、リソースグループとアプリケーションインスタンスをマッピングするために使用されます。
5. **apminfo.xml** ファイルの形式は次のとおりです。

**注:** `apminfo.xml` ファイルのパッケージ タグの間では、改行は使用できません。

```
T
<?xml version="1.0" ?>
<APMClusterConfiguration>
  <application>
    <Name>クラスタ対応アプリケーションの名前。</Name>
    <Instance>
      <Name>最初のインスタンスのアプリケーション名。インスタンス名はコマンドの起動/停止に使用され、メッセージ内でこのインスタンスを指定するために使用する名前に相当します。</Name>
      <Package>アプリケーションの最初のインスタンスが稼働するリソース グループ。</Package>
    </Instance>
    <Instance>
      <Name>2 番目のインスタンスのアプリケーション名。</Name>
      <Package>アプリケーションの 2 番目のインスタンスが稼働するリソース グループ。</Package>
    </Instance>
  </Application>
</APMClusterConfiguration>
```

### apminfo.xml の DTD

```
<!ELEMENT APMClusterConfiguration (Application+)>
<!ELEMENT Application (Name, Instance+)>
<!ELEMENT Name (#PCDATA)>
<!ELEMENT Instance (Name, Package)>
<!ELEMENT Package (#PCDATA)>
```

### 例

以下の例では、リソースグループの名前は SQL-Server であり、ネットワーク名 (またはインスタンス名) は CLUSTER04 です。

```
<?xml version="1.0" ?>
<APMClusterConfiguration>
  <application>
    <Name>dbspi_mssqlserver</Name>
    <Instance>
      <Name>CLUSTER04</Name>
      <Package>SQL-Server</Package>
```

```
</Instance>
```

```
</Application>
```

```
</APMClusterConfiguration>
```

6. クラスタ内の各ノードに対する完成した **apminfo.xml** ファイルを、以下のディレクトリに保存します。

Windows の場合 :%OvDataDir%conf\conf\

UNIX/Linux の場合 :/var/opt/OV/conf/conf/

7. クラスタ対応となるポリシーを記述する XML ファイルを作成します。ファイル名は、<アプリケーション名>.apm.xml という形式に従う必要があります。<アプリケーション名> は、**apminfo.xml** ファイル内の <Application><Name> タグの内容と同一である必要があります。<アプリケーション名>.apm.xml ファイルには、[「高可用性クラスタにおける HP Operations エージェント」\(46ページ\)](#) で特定したポリシーの名前が含まれます。

8. <アプリケーション名>.apm.xml ファイルを作成する際には、以下の形式を使用します。

```
<?xml version="1.0" ?>
```

```
<APMApplicationConfiguration>
```

```
<Application>
```

```
<Name>クラスタ対応アプリケーションの名前 (apminfo.xml ファイルの <Application><Name> と一致する必要があります)。</Name>
```

```
<Template>クラスタ対応となる最初のポリシー。</Template>
```

```
<Template>クラスタ対応となる2番目のポリシー。</Template>
```

```
<startCommand>アプリケーションのインスタンスが起動したときに常にエージェントが実行するオプションのコマンド。</startCommand>
```

```
<stopCommand>アプリケーションのインスタンスが停止したときに常にエージェントが実行するオプションのコマンド。</stopCommand>
```

```
</Application>
```

```
</APMApplicationConfiguration>
```

**注:** オペレーティングシステムで提供されていないプログラムを起動する場合は、startCommand および stopCommand タグ内で、プログラムのファイル拡張子を指定する必要があります。

たとえば、次のようになります。

```
<startCommand>test_command.sh</startCommand>
```

```
<startCommand>dbspicol.exe ON $instanceName</startCommand>
```

停止/起動コマンドでは、以下の変数を使用できます。

変数	説明
\$instanceName	(<Instance><Name> に一覧表示されている) 起動/停止しているインスタンスの名前。
\$instancePackage	(<Instance><Package> に一覧表示されている) 起動/停止しているリソースグループの名前。
\$remainingInstances	このアプリケーションの残りのインスタンス数。
\$openViewDirectory	エージェントのコマンド ディレクトリ。

### 例

**dbspi\_mssqlserver.apm.xml** という以下のサンプルファイルでは、Smart Plug-in for Databases が Microsoft SQL Server 用のポリシーを設定する方法を示しています。

```
<?xml version="1.0" ?>
<APMApplicationConfiguration>
  <application>
    <Name>dbspi_mssqlserver</Name>
    <Template>DBSPI-MSS-05min-Reporter</Template>
    <Template>DBSPI-MSS-1d-Reporter</Template>
    <Template>DBSPI-MSS-05min</Template>
    <Template>DBSPI-MSS-15min</Template>
    <Template>DBSPI-MSS-1h</Template>
    <Template>DBSPI-MSS6-05min</Template>
    <Template>DBSPI-MSS6-15min</Template>
    <Template>DBSPI-MSS6-1h</Template>
    <Template>DBSPI Microsoft SQL Server</Template>
    <StartCommand>dbspicol.exe ON $instanceName</StartCommand>
    <StopCommand>dbspicol.exe OFF $instanceName</StopCommand>
  </Application>
</APMApplicationConfiguration>
```

9. クラスタ内の各ノードに対する完成した `<app_name>.apm.xml` ファイルを、以下のディレクトリに保存します。

Windows の場合: `%OvDataDir%\bin\instrumentation\conf`

UNIX/Linux の場合: `/var/opt/OV/bin/instrumentation/conf`

10. リソースグループが存在する物理ノードはすべて管理対象ノードであることを確認します。
11. 次のコマンドを実行し、すべての物理ノードにある XML ファイルの構文をチェックします。

- Windows の場合 :`%OvInstallDir%\bin\ovappinstance -vc`  
HP-UX、Linux、Solaris の場合 :`/opt/OV/bin/ovappinstance -vc`  
AIX の場合 :`/usr/lpp/OV/bin/ovappinstance -vc`
- オプション:マルチホーム環境下のホストなど一部の物理ノードでは、標準のホスト名がクラスタ構成内のノード名と異なる場合があります。この場合、エージェントはリソースグループの現在の状態を正しく判定することができません。クラスタ構成内で認識されているホスト名を使用するように、エージェントを設定してください。
- クラスタ構成内で認識されている物理ノードの名前を取得します。

**ovclusterinfo -a**

- クラスタ構成内で認識されているノードの名前を使用するように、エージェントを設定します。

**ovconfchg -ns conf.cluster -set CLUSTER\_LOCAL\_NODENAME <名前>**

この場合、<名前> は **ovclusterinfo -a** の出力に記載されたノードの名前です。

- 以下のコマンドを実行し、すべての物理ノード上のエージェントを再起動します。

**ovc -stop**

**ovc -start**

HPOM for Windows 8.1x を使用している場合、クラスタ対応アプリケーションを監視するために ([「高可用性クラスタにおける HP Operations エージェント」\(46ページ\)](#)) で特定したポリシーを、HA クラスタのすべての物理ノードに配布します。

他のタイプの管理サーバーの場合、クラスタ対応アプリケーションを監視するために ([「高可用性クラスタにおける HP Operations エージェント」\(46ページ\)](#)) で特定したポリシーを、クラスタに作成した仮想ノードに配布します。

### エージェント ユーザー

デフォルトでは、HP Operations エージェントは定期的にはリソースグループのステータスをチェックします。UNIX および Linux ノードの場合、エージェントは通常、root ユーザーのみが実行できるクラスタアプリケーション固有のコマンドを使用します。Windows ノードの場合、エージェントはコマンドを実行する代わりに API を使用します。

エージェントのユーザーを変更した場合、エージェントはクラスタコマンドを正常に実行するために必要な権限を持たなくなる場合があります。この場合は、クラスタコマンドの実行時にエージェントがセキュリティプログラム (sudo、.do など) を使用するように設定する必要があります。

非 root アカウントで稼働するエージェントがクラスタコマンドを実行できるように設定するには、以下の手順に従います。

- 以下のコマンドを実行して、エージェントを停止します。

**ovc -kill**

- 以下のコマンドを入力し、エージェントがセキュリティプログラムを使用するように設定します。

**ovconfchg -ns ctrl.sudo -set OV\_SUDO <セキュリティプログラム>**

この場合、<セキュリティプログラム> はエージェントに使用させるプログラムの名前です (/usr/local/bin/.do など)。

- 以下のコマンドを実行して、エージェントを起動します。

```
ovc -start
```

## 第9章

### 安全な環境への HP Operations エージェント の配布

HP Operations エージェントと HPOM 管理サーバーは HTTPS プロトコルを使用し、ネットワークを通じて互いに通信を行います。管理サーバーはエージェント ノードとの接続を開設し、ポリシーの配布、アクションの起動などのタスクを実行します。

HP Operations エージェント ノードは管理サーバーとの接続を開設し、メッセージと応答を送信します。

デフォルトでは、エージェント ノードと管理サーバーのオペレーティングシステムは、ローカル通信ポートを割り当てます。しかし、エージェントと管理サーバーは両方とも、インバウンド通信に通信ブローカコンポーネントを使用します。通信ブローカコンポーネントはデフォルトで、ポート 383 を使用してデータを受信します。したがって実際には、ノードと管理サーバーは以下の 2 セットのポートを使用します。

オペレーティングシステムがアウトバウンド通信に割り当てたポート

通信ブローカがインバウンド通信に使用するポート

安全性が高いファイアウォールベースのネットワークでは、管理サーバーとエージェント ノード間の通信は、ファイアウォール設定の制約のために失敗する場合があります。このようなシナリオでは、追加の設定タスクを実行し、管理サーバーと管理対象ノード間の双方向通信を設定することができます。

#### 設定に関する計画

- ネットワークでファイアウォールを介した双方向の HTTPS 接続が許可されているが、何らかの制限が設けられている場合は、HPOM の次の設定オプションを使用してそれらの制限に対応することができます。
- ネットワークにおいて、アウトバウンド接続が特定のローカルポートにのみ許可されている場合、特定のローカルポートを使用するよう HPOM を設定します。
- ネットワークにおいて、インバウンド接続が特定の宛先ポートにのみ許可され、ポート 383 には許可されていない場合、別の通信ブローカポートを設定できます。
- ネットワークにおいて、ファイアウォールを介した接続の開設が特定のプロキシシステムにのみ許可されている場合、これらのプロキシを介して HPOM 通信をリダイレクトさせることができます。
- ネットワークにおいて、ファイアウォールを介した管理サーバーからのアウトバウンド HTTPS 接続のみが許可されており、ノードからのインバウンド接続がブロックされる場合は、リバースチャネルプロキシ (RCP) の設定を行います。

#### 事前準備

Windows ノードでのみ HP Operations エージェントを使用している場合は、このセクションをスキップしてください。

ほとんどの設定作業は `ovconfchg` ユーティリティを使用して行いますが、このユーティリティは以下のディレクトリに存在します。

HP-UX、Linux、Solaris の場合

`/opt/ov/bin`

AIX の場合

`/usr/lpp/OV/bin`

システムのあらゆる場所から `ovconfchg` コマンド (および他のエージェント特有のコマンド) を実行するには、`bin` ディレクトリをシステムの `PATH` 変数に追加する必要があります。Windows システムでは、`bin` ディレクトリは `PATH` 変数に自動的に追加されています。`bin` ディレクトリを UNIX/Linux システムの `PATH` 変数に追加するには、以下の手順に従います。

次のいずれかを実行します。

HP-UX、Solaris、Linux ノードでは、以下のコマンドを実行します。

```
export PATH=/opt/OV/bin:$PATH
```

AIX ノードでは、以下のコマンドを実行します。

```
export PATH=/usr/lpp/OV/bin:$PATH
```

これで `PATH` 変数に、指定した場所がセットされました。システムの任意の場所から、エージェント特有のコマンドを実行できるようになりました。

## プロキシの設定

別のネットワーク上の管理サーバーおよびノードから、プロキシを通じて接続をリダイレクトすることができます。

管理サーバーはプロキシサーバーとの接続を開設し、ポリシーとインストールメンテーションの配布、ハートビートポーリング、またはアクションの起動などを行います。プロキシサーバーは、管理サーバーに代わってノードへの接続を開設し、両者間の通信を転送します。

ノードはプロキシサーバーとの接続を開設し、メッセージとアクション応答の送信などを行います。プロキシサーバーは、ノードに代わって管理サーバーへの接続を開設します。

また以下のように、より複雑な環境でプロキシを介して通信をリダイレクトすることも可能です。

各管理サーバーとノードは、異なったプロキシサーバーを使用して互いに通信を行うことができます。

管理サーバーとノードを設定し、接続する必要があるホストに応じて正しいプロキシを選択することが可能です。

以下の図は、複数のプロキシを介した管理サーバーとノード間の接続を示しています。

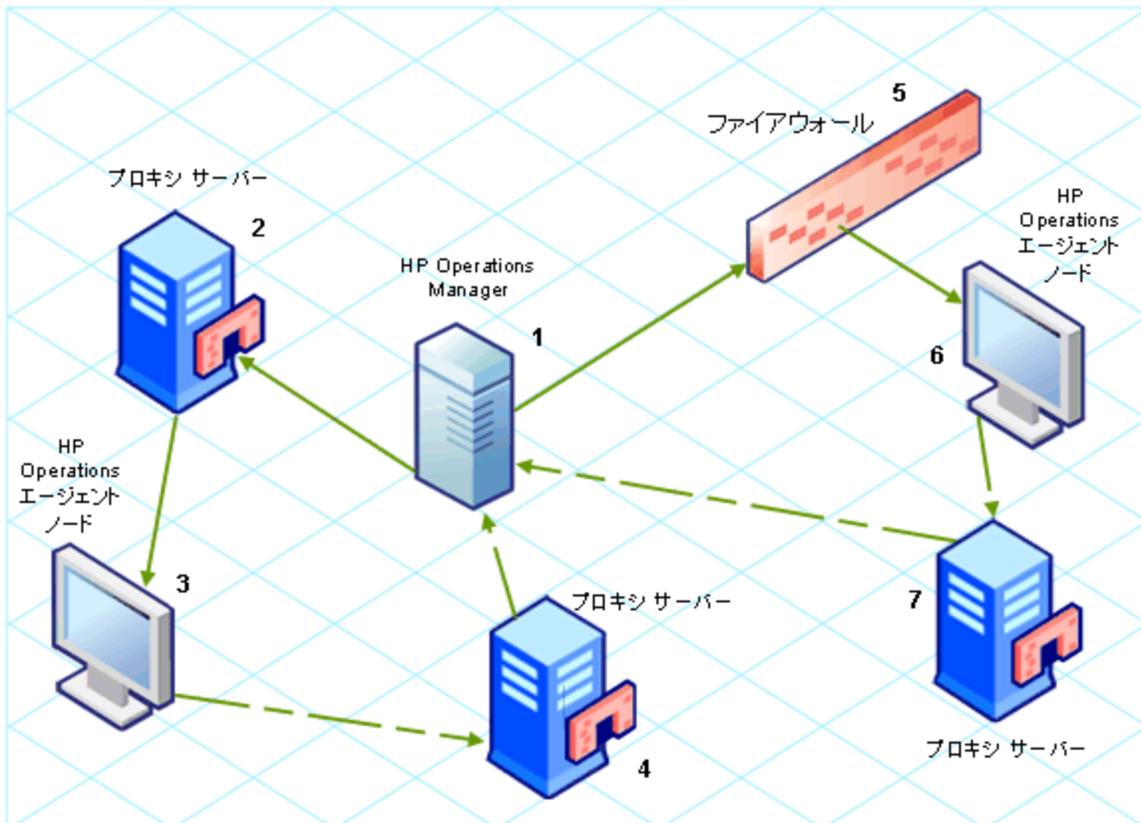
管理サーバー (1) は、プロキシ (2) への接続を開設します。プロキシは、管理サーバーに代わってノード (3) への接続を開設します。

ノード (3) は、別のプロキシ (4) への接続を開設します。プロキシは、ノードに代わって管理サーバー (1) への接続を開設します。

このネットワークにより、管理サーバー (1) はファイアウォール (5) を介して別のノード (6) と直接、アウトバウンド HTTP 接続を行うことができます (ノード (3)、(6) は異なったネットワーク上に存在します)。

ファイアウォール (5) は、インバウンド HTTP 通信を許可しません。したがって、ノード (6) はプロキシ (7) を介して管理サーバーへの接続を開設します。

プロキシを使用した通信



### プロキシパラメータの構文

管理サーバーとノードの `bbc.http` 名前空間のプロキシパラメータを設定することにより、プロキシを介してアウトバウンド HTTPS 通信をリダイレクトします。このパラメータを設定する手順は次のとおりです。

- HP Operations エージェントのインストール時にデフォルトの値を設定します。この方法は、多数のノードに対してプロキシを設定する必要がある場合にお勧めします。ノードを作成および移行する前に、インストールのデフォルトを計画して設定する必要があります。
- コマンド プロンプトで `ovconfchg` を使用します。

プロキシパラメータの値には、1 つ以上のプロキシ定義を含めることができます。各プロキシは、次の形式で指定します。

`<プロキシ ホスト名>:<プロキシ ポート>+(<対象ホスト>)-(<除外ホスト>)`

`<対象ホスト>` には、プロキシが通信可能なホスト名または IP アドレスのリストをカンマで区切って指定します。`<除外ホスト>` には、プロキシが接続不能なホスト名または IP アドレスのリストをカンマで区切って指定します。アスタリスク(\*)は、ホスト名とIP アドレスの中でワイルドカードとして使用します。`<対象ホスト>` と `<除外ホスト>` は、両方ともオプションです。

複数のプロキシを指定するには、各プロキシをセミコロン (;) で区切ります。リスト内の最初の適切なプロキシが優先されます。

### プロキシパラメータ値の例

すべてのアウトバウンド接続で proxy1.example.com のポート 8080 を使用するノードを設定するには、以下の値を使用します。

```
proxy1.example.com:8080
```

proxy2.example.com:8080 を使用し、\*.example.com または \*.example.org に一致するホスト名のホスト (ただし、192.168.0.0 ~ 192.168.255.255 の範囲の IP アドレスを持つホストを除く) に接続する管理サーバーを設定するには、以下の値を使用します。

```
proxy2.example.com:8080+(*.example.com,*.example.org)-(192.168.*.*)
```

上記の例を proxy3.example.com を使用して backup.example.com にのみ接続するように拡張するには、以下の値を使用します。

```
proxy3.example.com:8080+(backup.example.com);  
proxy2.example.com:8080+(*.example.com,*.example.org)-(192.168.*.*)
```

上記の例では、proxy2.example.com の対象リストに \*.example.com が含まれているので、proxy3.example.com:8080+(backup.example.com) を最初に指定する必要があります。

プロキシを介した HTTPS 通信をリダイレクトするには

1. 管理者または root として管理サーバーまたはノードにログインし、コマンドプロンプトまたはシェルを開きます。
2. ノードが使用するプロキシを指定します。エージェントが接続するホストに応じて、異なるプロキシを使用するように指定できます。次のコマンドを実行します。

```
ovconfchg -ns bbc.http -set PROXY <proxy>
```

注: クラスタ内で稼働する管理サーバーで ovconfchg コマンドを使用するときは、パラメータ -ovrg <サーバー> を追加します。

#### PROXY\_CFG\_ファイルパラメータ構文

PROXY 設定変数でプロキシサーバーの詳細を指定するのではなく、外部の設定ファイルを使用してプロキシサーバーのリストを指定し、設定ファイルからプロキシサーバーのデータを読み込むように HP Operations エージェントを設定できます。

PROXY\_CFG\_ファイル変数を設定する前に、外部設定ファイルを作成する必要があります。プロキシ設定ファイルは XML ファイルです。このファイルを使用して、プロキシサーバーの詳細を XML 要素内で指定できます。テキストエディタを使用して、ファイルを次のディレクトリに保存します。

Windows の場合

```
%ovdatadir%\conf\bbc
```

UNIX/Linux の場合

```
/var/opt/OV/conf/bbc
```

## プロキシ設定ファイルの構成

XML のプロキシ設定ファイルには、プロキシサーバー、エージェントノード、管理サーバーの詳細を指定する異なる XML 要素が含まれています。複数のプロキシサーバーの設定データを設定ファイルに指定できます。

#### XML のプロキシ設定ファイルの構造

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<proxies>
  <proxy>
    <server>proxy_server.domain.example.com:8080</server>
    <for>
      <target> *.domain.example.com </target>
      <target> *.domain2.example.com </target>
      <target> *.domain3.example.com </target>
    </for>
  </proxy>
</proxies>
```

- proxies:proxies 要素では、HPOM 管理対象環境で使用するプロキシ サーバーの詳細を追加できます。このXML ファイルのすべてのコンテンツは、proxies 要素内に含まれています。
- proxy: この要素では、プロキシ サーバーを経由してローカルノード内で通信するプロキシ サーバーとシステムの詳細を指定します。このXML ファイルに複数の proxy 要素を設定できます。
- server: この要素を使用して、監視環境で使用するプロキシ サーバーのFQDN (またはIP アドレス)を指定します。
- for:for 要素には、server 要素内で指定したプロキシ サーバーを経由してのみローカルノードと通信する必要がある他のすべてのエージェント ノード または管理サーバーのFQDN またはIP アドレスを含めます。target 要素には、それぞれのFQDN またはIP アドレスを追加する必要があります。

たとえば、次のようになります。

```
<for>
  <target> system3.domain.example.com </target>
  <target> system3.domain.example.com </target>
</for>
```

ワイルドカード文字 (\*)を使用して、1つのターゲット要素内に複数のシステムを設定できます。IP アドレスの範囲を指定することもできます。

たとえば、次のようになります。

```
<for>
  <target> *.domain2.example.com </target>
  <target> 172.16.5.* </target>
  <target> 192.168.3.50-85 </target>
</for>
```

- except:この要素を使用して、設定したプロキシ サーバー (server 要素で指定) を経由してローカルノードと通信しないシステムの除外リストを作成します。除外するすべてのシステムのFQDN またはIP アドレスをtarget 要素に含めます。

たとえば、次のようになります。

```
<except>
    <target> *.domain3.example.com </target>
    <target> 172.16.10.* </target>
    <target> 192.168.9.5-25 </target>
</except>
```

### プロキシ設定ファイルの例

構文	説明
<pre>&lt;proxies&gt; &lt;proxy&gt; &lt;server&gt; server1.domain.example.com:8080 &lt;/server&gt; &lt;for&gt; &lt;target&gt;*.domain2.example.com&lt;/target&gt; &lt;/for&gt; &lt;/proxy&gt; &lt;/proxies&gt;</pre>	<p>サーバー server1.domain.example.com は、プロキシサーバーとして設定され、ドメイン domain2.example.com に属するすべてのシステムは、server1.domain.example.com を介してのみノードと通信する必要があります。</p>
<pre>&lt;proxies&gt; &lt;proxy&gt; &lt;server&gt; server2.domain.example.com:8080 &lt;/server&gt; &lt;for&gt; &lt;target&gt;*.domain2.example.com&lt;/target&gt; &lt;target&gt;192.168.2.*&lt;/target&gt; &lt;/for&gt; &lt;/proxy&gt; &lt;proxy&gt; &lt;server&gt; server3.domain.example.com:8080</pre>	<p>サーバー server2.domain.example.com は、プロキシサーバーとして設定され、ドメイン domain2.example.com に属するシステムまたは 192.168.2 で始まる IP アドレスを持つシステムはすべて、server2.domain.example.com を介してのみノードと通信する必要があります。</p> <p>サーバー server3.domain.example.com は、2つ目のプロキシサーバーとして設定され、192.168.3 で始まる IP アドレスを持つシステムはすべて、server3.domain.example.com を介してのみノードと通信する必要があります。さらに、IP アドレスが 192.168.3.10-20 の範囲にあるシステムは、プロキシサーバー server3.domain.example を使用できません。</p>

構文	説明
<pre> &lt;/server&gt;  &lt;for&gt;  &lt;target&gt;192.168.3.*&lt;/target&gt;  &lt;/for&gt;  &lt;except&gt;  &lt;target&gt;192.168.3.10-20&lt;/target&gt;  &lt;/except&gt;  &lt;/proxy&gt;  &lt;/proxies&gt; </pre>	

### PROXY\_CFG\_FILE 変数の設定

1. 管理者または root としてノードにログオンします。
2. テキスト エディタで新しい XML ファイルを作成します。
3. 次の行をファイルの先頭に追加します。

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
```

4. コンテンツをファイルに追加します。
5. ファイルを以下のディレクトリに保存します。

*Windows の場合*

```
%ovdatadir%conf\bbs
```

*UNIX/Linux の場合*

```
/var/opt/OV/conf/bbs
```

6. 次のコマンドを実行します。

*Windows の場合*

```
%ovinstalldir%bin\ovconfchg -ns bbc.http -set PROXY_CFG_FILE <filename>.xml
```

*HP-UX、Linux、Solaris の場合*

```
/opt/OV/bin/ovconfchg -ns bbc.http -set PROXY_CFG_FILE <filename>.xml
```

*AIX の場合*

```
/usr/lpp/OV/bin/ovconfchg -ns bbc.http -set PROXY_CFG_FILE <filename>.xml
```

## 通信ブローカポートの設定

デフォルトでは、HP Operations エージェント ノードはインバウンド通信用にポート 383 を使用します。通信ブローカはすべての HP Operations エージェント サーバーまたはノードで、ポート 383 を通じてインバウンド通信を円滑に実施します。

通信ブローカは、383 以外のポートで待ち受けるように設定することもできます。この場合は、環境内の他の管理サーバーとノードでも設定を行い、アウトバウンド接続が正しいポートに向かうようにする必要があります。たとえば、ノードの通信ブローカをポート 5000 で待ち受けるように設定した場合、管理サーバーもこのノードと通信するときにポート 5000 に接続するように設定する必要があります。

#### PORTS パラメータの構文

互いに通信するすべての管理サーバーとノードの `bbc.cb.ports` 名前空間の PORTS パラメータを設定することにより、通信ブローカのポートを設定します。

このパラメータを設定する手順は次のとおりです。

- HP Operations エージェントのインストール時に、プロファイルファイルでデフォルトの値を設定します。多数のノードの通信ブローカポートを設定する必要がある場合は、この方法を推奨します。ノードを作成および移行する前に、インストールのデフォルトを計画して設定する必要があります。
- コマンド プロンプトで `ovconfchg` を使用します。

値には 1 つ以上のホスト名または IP アドレスが含まれ、以下の形式に従う必要があります。

<ホスト>:<ポート>[, <ホスト>:<ポート>] ...

<ホスト> は、ドメイン名または IP アドレスのいずれかです。たとえば、ホスト名が `manager1.emea.example.com` の管理サーバーで通信ブローカのポートを 5000 に設定するには、その管理サーバー自体と、それに対して接続を開設する他のすべての管理サーバーとノードで以下のコマンドを使用します。

```
ovconfchg -ns bbc.cb.ports -set PORTS manager1.domain.example.com:5000
```

複数のシステムに対して通信ブローカのポートを設定する必要がある場合は、次のようにワイルドカードと範囲を使用することができます。

ドメイン名の最初に、ワイルドカードとしてアスタリスク (\*) を付加します。たとえば、次のようになります。

```
*.test.example.com:5000
```

```
*.test.com:5001
```

```
*:5002
```

IP アドレスの最後にワイルドカードとして最大 3 つのアスタリスク (\*) を付加することができます。たとえば、次のようになります。

```
192.168.1.*:5003
```

```
192.168.**:5004
```

```
10.**:5005
```

IP アドレスの 1 つのオクテットを範囲に置き換えることができます。範囲は、ワイルドカードより前に指定する必要があります。たとえば、次のようになります。

```
192.168.1.0-127:5006
```

```
172.16-31.**:5007
```

PORTS パラメータに複数の値を指定する場合は、それぞれをカンマ (,) で区切ります。たとえば、次のようになります。

```
ovconfchg -ns bbc.cb.ports -set PORTS
*.test.example.com:5000,10.*.*.*:5005
```

ワイルドカードと範囲を使用して重複する複数の値を指定したときは、管理サーバーまたはノードは以下の順番でポートを選択します。

完全修飾ドメイン名

ワイルドカードを使用したドメイン名

完全な IP アドレス

範囲を使用した IP アドレス

ワイルドカードを使用した IP アドレス

#### 例

以下の仕様に対して、HPOM 監視環境を設定する必要があります。

ドメイン \*.test2.example.com 内のすべてのシステムを、通信ブローカがポート 6000 を使用するように設定します。

IP アドレスの最初のオクテットが 10 である (10.\*.\*.\*) すべてのシステムを、通信ブローカがポート 6001 を使用するように設定します。ただし、以下の例外があります。

IP アドレスの 2 番目のオクテットが 0~127 である (10.0-127.\*.\*) すべてのシステムを、通信ブローカがポート 6003 を使用するように設定します。

システム manager1.test2.example.com を、通信ブローカがポート 6002 を使用するように設定します。

上記仕様の HPOM 監視環境を設定するには、以下のコマンドを実行します。

```
ovconfchg -ns bbc.cb.ports -set PORTS
*.test2.example.com:6000,10.*.*.*:6001,manager1.test2.example.com:6002,10.0-127.*.*:6003
```

この変更は、監視環境のすべてのエージェント ノードとすべての HPOM 管理サーバーでこのコマンドを実行した場合のみ反映されます。

どのポートが現在設定されているかを確認するには、以下のコマンドを実行します。

```
bbcutil -getcbport <ホスト>
```

通信ブローカをデフォルト以外のポートを使用するように設定するには

**注:** 環境内のすべての HPOM サーバーと HP Operations エージェント ノードの通信ブローカは、必ず同じポートを使用するように設定してください。

1. HP Operations エージェント ノードにログオンします。
2. コマンド プロンプトまたはシェルを開きます。
3. 以下のコマンドを実行し、通信ブローカのポートにデフォルト以外の値をセットします。

```
ovconfchg -ns bbc.cb.ports -set PORTS <ホスト>:<ポート>[,<ホスト>:<ポート>] ...
```

クラスタ内で稼働する HP Operations エージェント ノードで `ovconfchg` コマンドを使用するときには、パラメータ `-ovrg <server>` (`<server>` はリソースグループ) を追加します。

4. 上記コマンドを、すべてのエージェント ノードとすべての管理サーバーで実行します。

## ローカル通信ポートの設定

デフォルトでは、管理サーバーとノードはアウトバウンド接続でローカルポート 0 を使用します。このことは、オペレーティングシステムは各接続に対してローカルポートを割り当てておくことを意味します。通常、オペレーティングシステムはローカルポートを順番に割り当てます。たとえば、オペレーティングシステムがローカルポート 5055 をインターネット ブラウザに割り当て、次に HTTPS エージェントが接続を開示した場合、HTTPS エージェントはポート 5056 で受信します。

しかし、ファイアウォールが使用可能なポートを制約する場合は、管理サーバーとノードを設定し、代わりに特定範囲のローカルポートを使用することができます。

### CLIENT\_PORT パラメータの構文

管理サーバーとノードの `bbc.http` 名前空間の `CLIENT_PORT` パラメータを設定することにより、ローカル通信ポートを設定します。このパラメータを設定する手順は次のとおりです。

- HP Operations エージェントのインストール時にデフォルトの値を設定します。この方法は、多数のノードでローカル通信ポートを設定する必要がある場合にお勧めします。ノードを作成および移行する前に、インストールのデフォルトを計画して設定する必要があります。
- コマンド プロンプトで `ovconfchg` を使用します。

この値は、以下の形式でポートの範囲を指定します。

```
<小さい方のポート番号>-<大きい方のポート番号>
```

たとえば、ファイアウォールがポート 5000～6000 から発信されるアウトバウンド接続のみを許可する場合は、以下の値を使用します。

```
5000-6000
```

ローカル通信ポート設定するには

1. HP Operations エージェント ノードにログオンします。
2. コマンド プロンプトまたはシェルを開きます。
3. 以下のコマンドを入力し、管理サーバーまたはノードがアウトバウンド接続に使用できるローカルポートの範囲を指定します。

```
ovconfchg -ns bbc.http -set CLIENT_PORT <小さい方のポート番号>-<大きい方のポート番号>
```

クラスタ内で稼働する管理サーバーで `ovconfchg` コマンドを使用するときは、パラメータ `-ovrg <サーバー>` を追加します。

## 複数の IP アドレスがあるノードの設定

ノードに複数の IP アドレスがある場合、エージェントは通信に以下のアドレスを使用します。

通信ブローカは、すべての IP アドレスで受信接続を受け入れます。

エージェントは、最初に検出したネットワークインターフェイスを使用して管理サーバーへの接続を開設します。

HP Reporter または HP Performance Manager と通信を行うために、通信デーモン (CODA) はすべての IP アドレスで受信接続を受け入れます。

特定の IP アドレスを使用するように HP Operations エージェント を設定するには

1. HP Operations エージェント ノードにログオンします。
2. コマンド プロンプトまたはシェルを開きます。
3. 以下のコマンドを実行し、通信ブローカ用の IP アドレスを設定します。

```
ovconfchg -ns bbc.cb SERVER_BIND_ADDR <ip_address>
```

4. 以下のコマンドを実行し、管理サーバーへのアウトバウンド接続の開設時にエージェントに使用させたい IP アドレスを設定します。

```
ovconfchg -ns bbc.http CLIENT_BIND_ADDR <ip_address>
```

5. 以下のコマンドを実行し、HP Performance Manager または HP Reporter からの受信接続で使いたい IP アドレスを設定します。

```
ovconfchg -ns coda.comm SERVER_BIND_ADDR <ip_address>
```

## プロキシを介した HTTPS 通信の設定

ネットワークにおいて、ファイアウォールを介した接続の開設が特定のプロキシシステムにのみ許可されている場合、これらのプロキシを介して HPOM 通信をリダイレクトさせることができます。以下のリストは、この設定を使用した管理サーバーとエージェントの通信に関するワークフローを示しています。

1. 管理サーバーは、プロキシへの接続を開設します。
2. プロキシは、管理サーバーに代わってノードへの接続を開設し、両者間の通信を転送します。
3. ノードは、プロキシへの接続を開設します。
4. プロキシは、ノードに代わって管理サーバーへの接続を開設します。

プロキシを介した通信をリダイレクトするには

1. root 権限または管理者権限を使用して、管理サーバーまたはノードにログオンします。
2. コマンド プロンプトで、以下のコマンドを実行します。

```
ovconfchg -ns bbc.http -set PROXY <proxy>:<port>
```

この場合、<プロキシ> はプロキシサーバーの IP アドレスまたは FQDN であり、<ポート> はプロキシサーバーの通信ポートです。

## 安全性の高い環境における通信

ファイアウォールに制御された安全な環境では、安全地帯に存在するシステムは自由に通信し、互いに情報を交換できます。しかし、特定のファイアウォール設定により、安全地帯の外側に属するシステムとの通信が制限される可能性があります。非武装地帯 (DMZ) と呼ばれる信頼性のないネットワークは、ファイアウォール設定の制約により安全地帯にデータを送信できない場合があります。

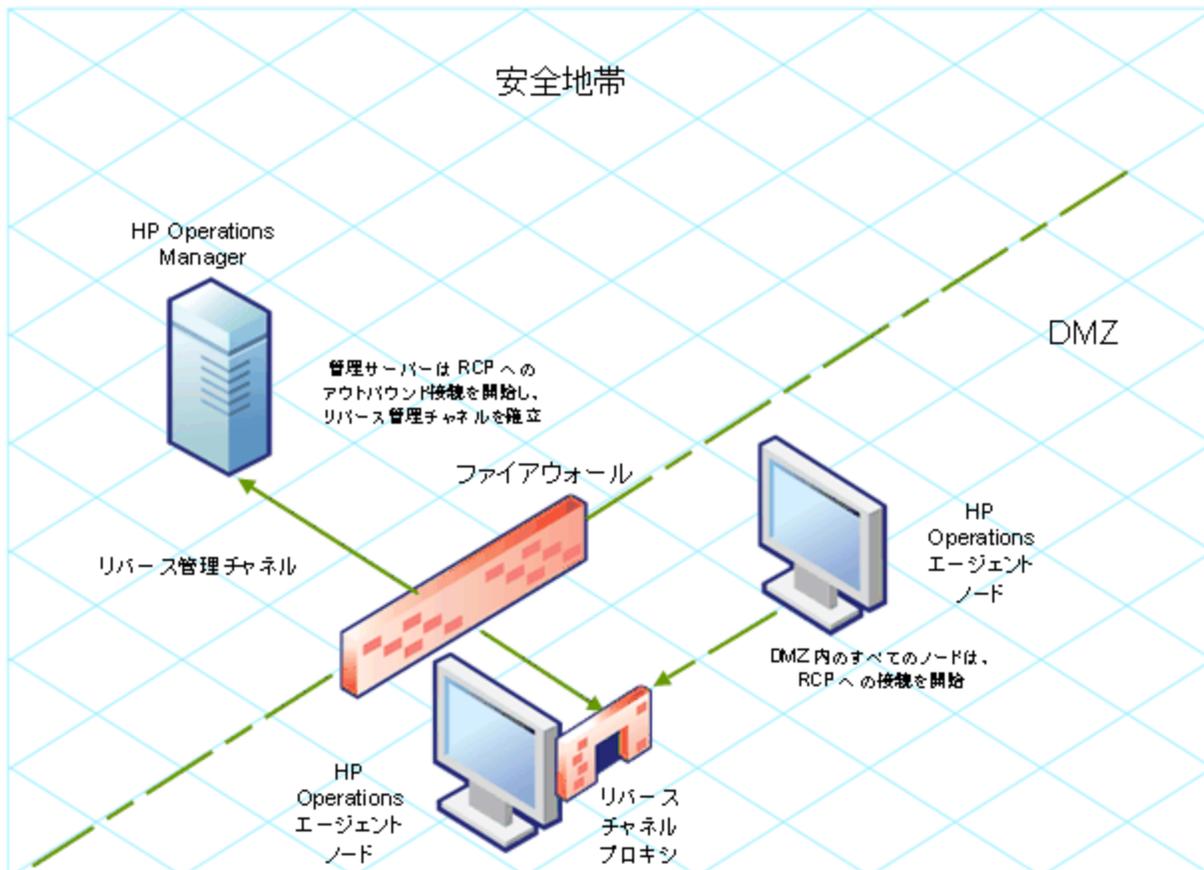
## インストールおよび設定ガイド

### 第9章: 安全な環境へのHP Operations エージェントの配布

多くの配備シナリオでは、HPOM 管理サーバーは安全地帯に存在し、管理対象ノードはDMZに存在します。DMZ内のシステムが安全地帯のシステムと通信できないようにファイアウォールが設定されていた場合、サーバーとエージェント間の通信は不可能となります。

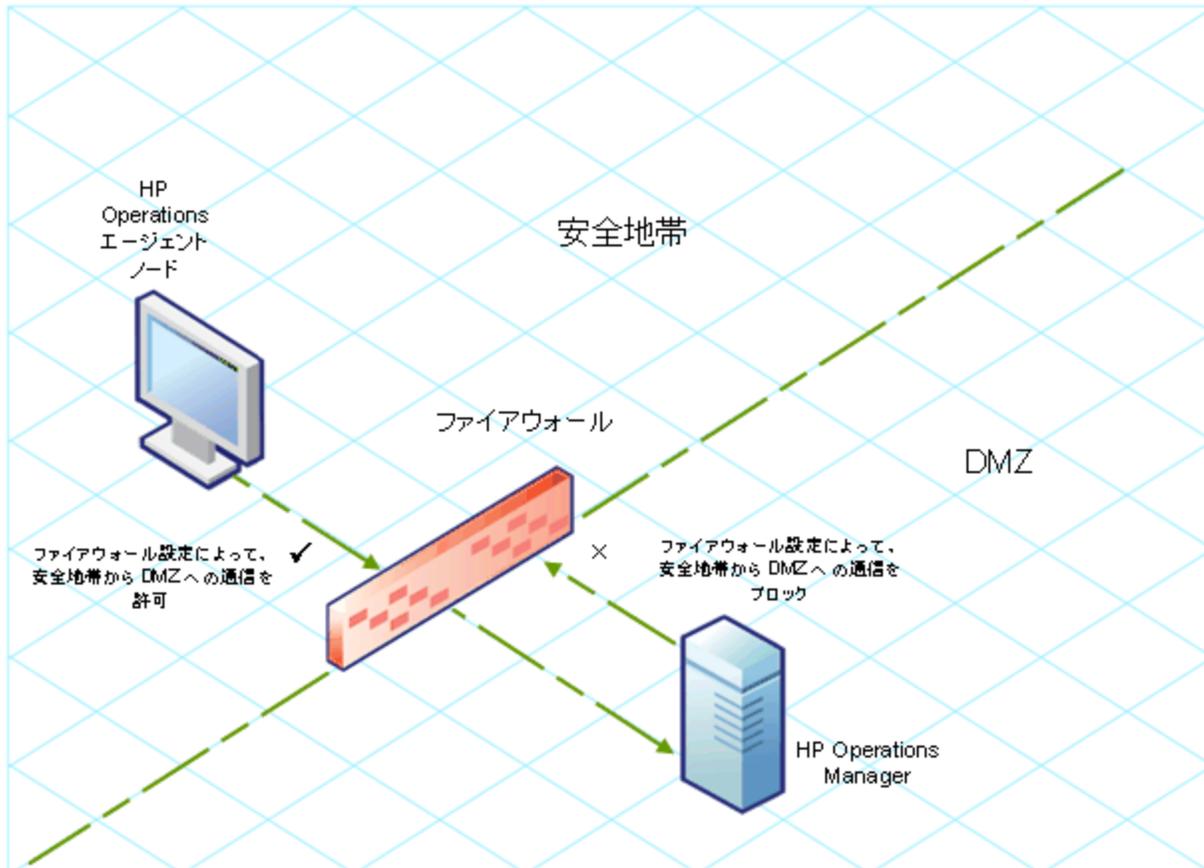
以下のシナリオでは、管理対象ノードはDMZに配置されていますが、一方、管理サーバーは安全地帯に属しています。この例では、ファイアウォール設定はアウトバウンド通信のみを許可しています。したがって、管理サーバーへのインバウンド通信はファイアウォールによりブロックされます。

#### DMZ内の管理対象ノード



以下のシナリオでは、管理対象ノードは安全地帯に配置されていますが、一方、管理サーバーはDMZに属しています。この例では、ファイアウォール設定はノードからHPOM管理サーバーへのアウトバウンド通信のみを許可していますが、ノードへのインバウンド通信はブロックしています。

#### DMZ内のHPOM管理サーバー



## リバース チャネル プロキシの概要

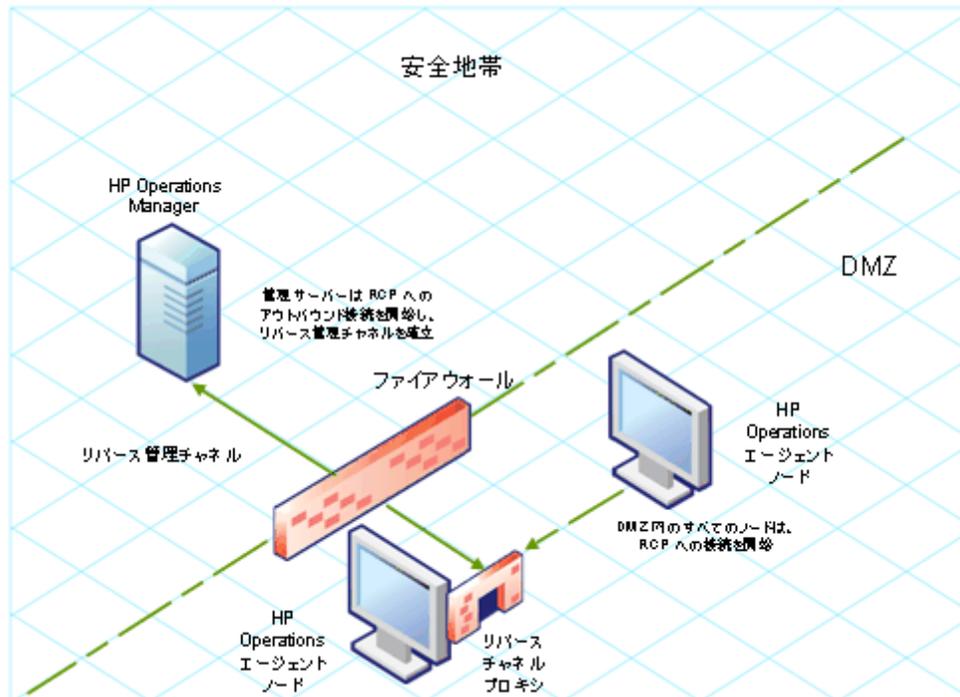
双方向通信を可能とする1つの簡単なソリューションは、ポート 383 (通信ブローカのポート) へのインバウンドトラフィックを許可するようにファイアウォールを設定することです。しかし、これによりシステムは外部からの攻撃に対して脆弱になります。通信ブローカのポートへのインバウンドトラフィックを許可せずに安全な通信を実現するには、リバースチャネルプロキシ (RCP) を設定する必要があります。

DMZ に属するシステムは、安全地帯内のシステムとは異なり、RCP と接続を開通させます。安全地帯内のシステムは、アウトバウンド通信チャネル (リバース管理チャネル) を RCP と接続するように設定できます。安全地帯内のシステムはアウトバウンドチャネルを維持しているため、DMZ 内のシステムはリバース管理チャネルを使用し、RCP を介して詳細を安全地帯に送信することができます。

ノードが DMZ に、管理サーバーが安全地帯に配置されている場合、HPOM は以下のワークフローを使用して設定されます。

1. RCP は、DMZ 内のノードに設定されます。
2. DMZ 内のすべてのノードは、RCP への接続を開通させます。
3. 管理サーバーは RCP へのアウトバウンド接続を開通させ、リバース管理チャネルを確立します。リバース管理チャネルにより、管理サーバーは一切ポートを追加することなく、RCP から発生するインバウンドデータを受け入れることができます。
4. DMZ のすべてのノードはリバース管理チャネルを通じて、HPOM 管理サーバーと通信します。

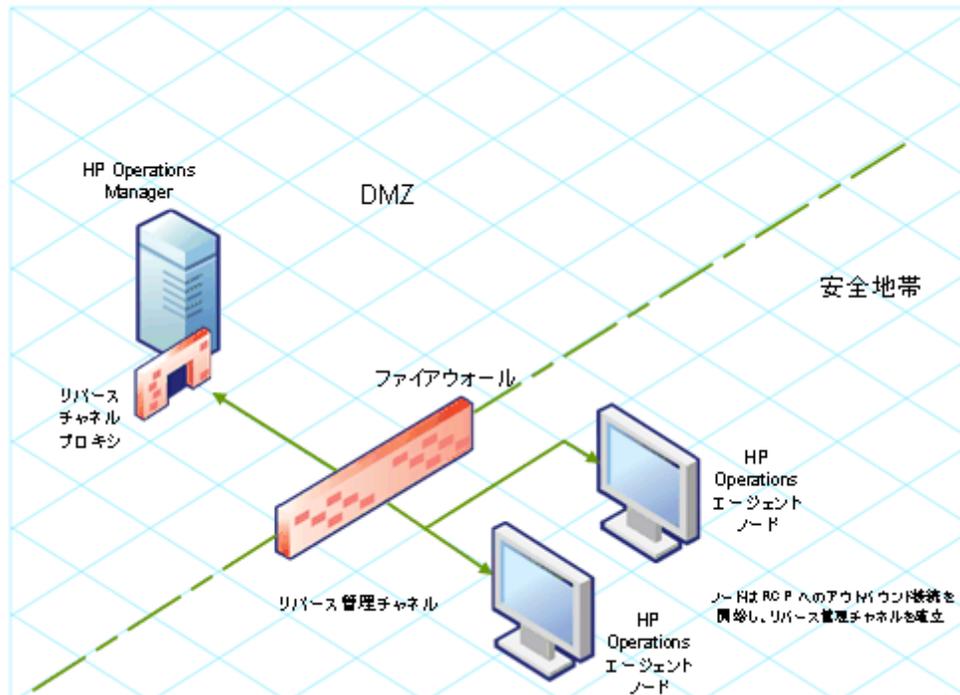
RCP を通じた DMZ 内のノードとの安全な通信



ノードが安全地帯に、管理サーバーがDMZに配置されている場合、HPOMは以下のワークフローを使用して設定されます。

1. RCPは、DMZ内の管理サーバーに設定されます。
2. ノードはRCPへのアウトバウンド接続を開通し、リバース管理チャネルを確立します。リバース管理チャネルにより、ノードは一切ポートを追加することなく、RCPから発生するインバウンドデータを受け入れることができます。
3. DMZ内の管理サーバーはリバース管理チャネルを通じて、ノードと通信を行います。

*RCPを通じたDMZ内の管理サーバーとの安全な通信*



## アウトバウンドのみの環境における安全な通信の設定

アウトバウンドのみの環境において、RCP とリバース管理チャンネルを使用して安全な通信を設定するには、以下のタスクを実行します。

### RCP の設定

RCP を設定する前に、ノードの証明書を設定する必要があります。

RCP を設定するには

1. 管理者権限または root 権限を持つユーザーとして、(ネットワーク上の配置に応じて) ノードまたは管理サーバーにログオンします。
2. コマンドプロンプトまたはシェルを開きます。
3. 次のコマンドを実行します。

```
ovconfchg -ns bbc.rcp -set SERVER_PORT <port_number>.
```

この場合、<ポート番号> は RCP が使用するポートです。指定したポートが、他のアプリケーションに使用されていないことを確認します。

4. UNIX/Linux のみ。通信ブローカ (ovbbcbb) の実行時のルートディレクトリは /var/opt/OV です。Transmission Control Protocol (TCP) 接続を開くために必要な設定ファイルは、/etc ディレクトリにあります。そのため、ovbbcbb は、RCP への接続を確立できません。この問題を解決するには、以下の手順を実行します。
  - a. /var/opt/OV の下に etc という名前のディレクトリを作成します。
  - b. 関連の設定ファイル (resolv.conf、hosts、nsswitch.conf などのファイル) を /etc to /var/opt/OV/etc からコピーします。

- c. この方法の代わりに、以下のコマンドを実行して ovbbccb chroot 機能を無効にする方法もあります。この方法で、ovbbccb が RCP への接続を確立できないという問題が解決します。

```
ovconfchg -ns bbc.cb -set CHROOT_PATH /
```

5. RCP コンポーネントを登録し、ovc により RCP コンポーネントを起動、停止、および監視できるようにします。次のコマンドを入力します。

```
ovcreg -add <install_dir>/newconfig/DataDir/conf/bbc/ovbbccrcp.xml
```

```
ovc -kill
```

```
ovc -start
```

#### リバース管理チャネルの設定

作成した RCP を使用してリバース管理チャネルを設定し、アウトバウンドのみのファイアウォール環境においてインバウンド通信を円滑に実施できるようにする必要があります。リバース管理チャネルを設定するには、以下の手順に従います。

1. 管理者権限または root 権限を持つユーザーとして、(ネットワーク上の配置に応じて) ノードまたは管理サーバーにログオンします。
2. コマンドプロンプトまたはシェルを開きます。
3. 以下のコマンドを実行し、リバース管理チャネルを作成します。

```
ovconfchg [-ovrg <server>] -ns bbc.cb -set ENABLE_REVERSE_ADMIN_CHANNELS true
```

4. 以下のコマンドを実行し、RCP の詳細を指定します。

```
ovconfchg [-ovrg <server>] -ns bbc.cb -set RC_CHANNELS <rcp>:<port>[,<OvCoreId>][; <rcp2>...]
```

```
ovconfchg [-ovrg <server>] -ns bbc.cb -set PROXY <rcp>:<port>[,<OvCoreId>][; <rcp2>...]
```

上記形式の説明

<rcp>:RCP を設定するシステムの FQDN、または IP アドレス。

<ポート>:RCP 用に設定するポート番号 (SERVER\_PORT 変数に指定したポート)

<OvCoreId>:RCP を設定するシステムのコア ID。

また、設定ファイルを使用して RCP の詳細を指定することも可能です。

5. オプション: 失敗したリバース管理チャネル接続をサーバーが自動的に復元するように設定します。デフォルトでは、サーバーは失敗した接続を復元しません。デフォルトを変更するには、以下のコマンドを実行します。

```
ovconfchg [-ovrg <server>] -ns bbc.cb -set RETRY_RC_FAILED_CONNECTION TRUE
```

6. オプション: サーバーが RCP への接続を行う最大試行回数を設定します。デフォルトでは -1 (無限) に設定されています。デフォルトを変更するには、以下のコマンドを実行します。

```
ovconfchg [-ovrg <server>] -ns bbc.cb -set MAX_RECONNECT_TRIES <number of tries>
```

7. オプション: リバース管理チャネル接続の失敗時に警告メッセージを生成するように、管理サー

バーを設定します。デフォルトでは、管理サーバーはこの失敗メッセージを生成しません。デフォルトを変更するには、以下のコマンドを実行します。

```
ovconfchg [-ovrg <サーバー>] -ns bbc.cb -set RC_ENABLE_FAILED_OVEVENT TRUE
```

RETRY\_RC\_FAILED\_CONNECTION に TRUE をセットすると、管理サーバーはメッセージを生成しません。

8. オプション: リバース管理チャンネルが開設していることをチェックするには、次のコマンドを実行します。

```
ovbbccb -status
```

開設しているすべてのリバース管理チャンネルのリストが出力されます。

9. オプション: 失敗したリバース管理チャンネルを復元するには、次のコマンドを実行します。

```
ovbbccb -retryfailedrcp [-ovrg <server>]
```

### パフォーマンスリバース管理チャンネルのパフォーマンスに関する考慮事項

リバース管理チャンネルのパフォーマンスは、チャンネルに接続するノード数に依存する場合があります。RC\_MAX\_WORKER\_THREADS 変数により、リバース管理チャンネルのパフォーマンスを調整できるようになります。

RC\_MAX\_WORKER\_THREADS 変数を使用するには

1. リバース管理チャンネルを確立するノードにログオンします。
2. エージェントがチャンネルを確立するのにかかった時間をメモします。この時間は、**ovbbccb -status** コマンドを実行することで決定できます。**ovbbccb -status** コマンドの出力は、システムで発生したリバース管理チャンネルのステータスを示します。**ovbbccb -status** コマンドを繰り返し実行することにより、エージェントがチャンネルを確立するのにかかったおおよその時間を決定することができます。
3. チャンネルを確立するための目標時間と、エージェントがチャンネルを確立するのに実際にかかったおおよその時間の比率を計算します。
4. RC\_MAX\_WORKER\_THREADS 変数に、その比率より大きい次の整数をセットします。以下のコマンドを使用して、この変数を設定します。

```
ovconfchg -ns bbc.cb -set RC_MAX_WORKER_THREADS <Maximum_Threads>
```

## 設定ファイルによる RCP 詳細の指定

設定ファイルを使用して、RCP の詳細を指定することができます。設定ファイルを使用するには、以下の手順に従います。

1. テキストファイルを作成します。
2. 新しい行に以下の形式で、各 RCP の詳細を指定します。

```
<rcp>:<ポート>[,<OvCoreId>]
```

上記形式の説明

<rcp>:RCP を設定するシステムの FQDN、または IP アドレス。

<ポート>:RCP 用に設定するポート番号 (SERVER\_PORT 変数に指定したポート)。

<OvCoreID>:RCP を設定するシステムのコア ID。

3. ファイルを以下の場所に保存します。

```
<data_dir>/conf/bbc
```

高可用クラスタやサーバー プール設定にある管理サーバーでこの手順を実行する場合、次の場所にファイルを保存します。

```
<data_dir>/shared/<server>/conf/bbc
```

4. 次のコマンドを実行します。

```
ovconfchg [-ovrg <server>] -ns bbc.cb -set RC_CHANNELS_CFG_FILES <file_name>
```

上記形式の説明

<ファイル名>:作成したファイルの名前。

<server>:クラスタまたはサーバー プール設定のリソースグループの名前。

## 複数のシステムに対する RCP の設定

DMZには1つのRCPのみを設定できますが、次にDMZの他のシステムにRCPを使用するための設定を行います。そのためには、DMZ内の全システムのPROXY変数に、RCPをホストするシステムのIPアドレス(またはFQDN)とポートをセットする必要があります。1つのRCPを使用するように複数のシステムを設定するには、以下の手順に従います。

1. root 権限または管理権限でノードにログオンします。
2. コマンド プロンプト (シェル) を開きます。
3. 次のコマンドを実行します。

```
ovconfchg -ns bbc.http -set PROXY "<rcp>:<ポート>+<対象ホスト>-<除外ホスト>"
```

上記形式の説明

<rcp>:RCPを設定するシステムのFQDN、またはIPアドレス。

<ポート>:RCP用に設定するポート番号 (SERVER\_PORT 変数に指定したポート)

<対象ホスト>:RCPへのリバース管理チャネルを開設するシステムのFQDNまたはIPアドレスを指定します。このシナリオでは、安全地帯に属する管理サーバーのFQDNまたはIPアドレスを指定する必要があります。複数の管理サーバーを使用したい場合は、カンマで区切って複数のFQDNを指定することができます。

<除外ホスト>:RCPを通じてアクセスする必要がないシステムのFQDNまたはIPアドレスを指定します。複数のFQDNをカンマで区切って指定できます。ただし、ローカルシステムのFQDNとホスト名(カンマ区切り)を指定する必要があります。例: `ovconfchg -ns bbc.http -set PROXY "<rcp>:<ポート>-<ローカルホスト>,<ローカルホスト>.domain.com"`

4. システムがHP Operations エージェント ノードの場合は、以下のコマンドを実行してメッセージ エージェントを再起動します。

```
ovc -restart opcmsga
```

DMZ内のすべてのシステムに対して、手順3と手順4を繰り返します。

### RCPのパフォーマンスに関する考慮事項

1つのシステムに対してのみRCPを設定する場合は、エージェントシステムに対する最小限の要求を満たせば十分です。

複数のエージェント ノードに使用される RCP を設定する場合は、大幅な遅延が発生することなく、RCP システムがすべての着信要求にサービスできるようにする必要があります。

## RCP を介した通信の検証

RCP を設定してリバース管理チャネルを確立した後、以下のタスクを実行してサーバーとノード間の通信が正常に確立されたかどうかを検証することができます。

### RCP に対する通信の検証

DMZ 内のシステムが RCP と通信できることを検証するには、以下の手順に従います。

1. root 権限または管理者権限を使用して、DMZ 内のシステムにログオンします。
2. コマンド プロンプト (シェル) を開きます。
3. 次のコマンドを実行します。

```
bbcutil -gettarget <FQDN>
```

この場合、<FQDN> は RCP へのリバース管理チャネルを確立するシステムの FQDN です。管理サーバーが安全地帯に配置されている場合は、管理サーバーの FQDN を指定します。

RCP が正常に作成された場合、出力として以下のメッセージが表示されます。

```
HTTP Proxy: <rcp>: <port>
```

上記形式の説明

<rcp>:RCP を設定するシステムの FQDN、または IP アドレス。

<ポート>:RCP 用に設定するポート番号 (SERVER\_PORT 変数に指定したポート)

### リバース管理チャネルのチェック

リバース管理チャネルが正しく確立されていることを検証するには、以下の手順に従います。

1. root 権限または管理者権限を使用して、安全地帯内のシステムにログオンします。
2. コマンド プロンプト (シェル) を開きます。
3. 次のコマンドを実行します。

```
ovbbccb -status
```

チャネルが正しく確立されている場合、出力として以下のメッセージが表示されます。

```
HTTP Communication Reverse Channel Connections
```

```
Opened:
```

```
system1.mydomain.com:1025 BBC 11.00.000; ovbbccrcp 11.00.000
```

```
system2.mydomain.com:1025 BBC 11.00.000; ovbbccrcp 11.00.000
```

```
system3.mydomain.com:1025 BBC 11.00.000; ovbbccrcp 11.00.000
```

```
system4.mydomain.com:1025 BBC 11.00.000; ovbbccrcp 11.00.000
```

この場合、システムは次の RCP システムに対してリバース管理チャネルを確立しました。system1, system2, system3, and system4.

RCP へのリバース管理チャンネルが失敗した場合、`ovbcbcb -status` コマンドは以下の形式でステータスを表示します。

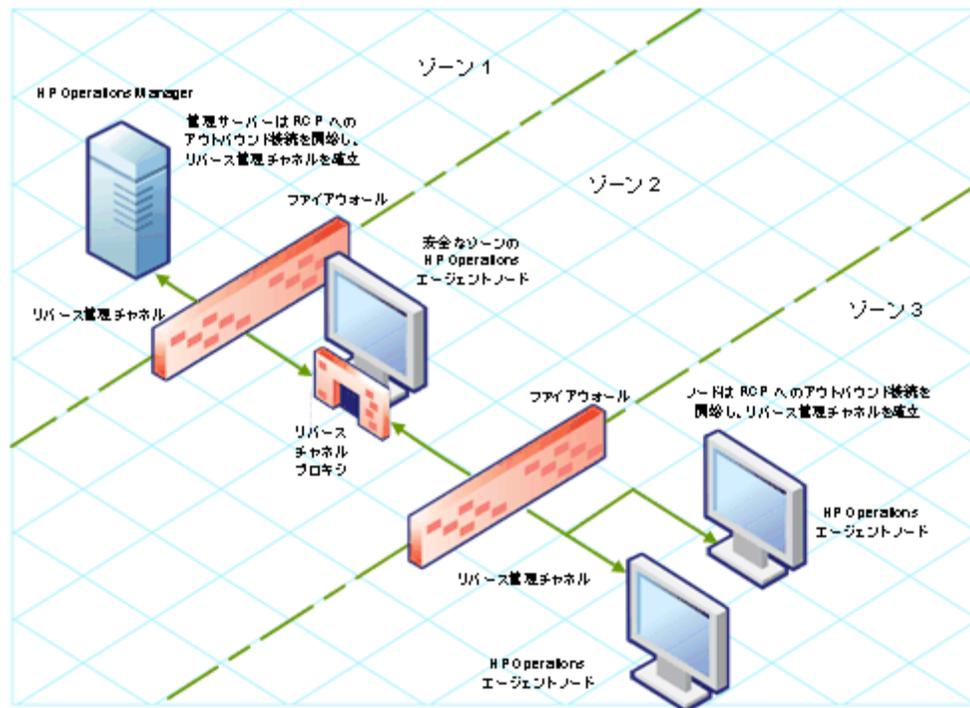
Pending:

```
system5.mydomain.com:1025 Connection To Host Failed
```

## 2つのファイアウォールを介した通信

あるケースでは、管理環境が2つの異なるファイアウォールを使用して設定され、管理サーバーが一方のファイアウォールの背後に存在し、ノードグループがもう一方のファイアウォールの背後に存在する場合があります。

### 2つのファイアウォールによる安全な通信



このシナリオでは、エージェントを中間地帯 (ゾーン2) のシステムにインストールし、RCP をシステムに設定する必要があります。ゾーン3のノードとゾーン1の管理サーバーを設定してRCPへのリバース管理チャンネルを確立すると、サーバーとノードの双方向通信がRCPを介して行われます。

このシナリオで安全な双方向通信を設定するには、以下の手順に従います。

1. エージェントをゾーン2のノードにインストールします。
2. RCP をゾーン2のノードに設定します。
3. 管理サーバーからRCPに対して、リバース管理チャンネルを設定します。
4. ゾーン3のノードからRCPに対して、リバース管理チャンネルを設定します。

## 第10章

# Performance Collection Component のリモートからの設定

管理サーバーからリモートで、管理対象ノードの特定の設定タスクを実行することができます。Performance Collection Component の設定タスクをすべてのノードでローカルに実行する代わりに、ポリシーとツールの特設なセットを使用し、HPOM コンソールから複数のノードの Performance Collection Component を設定、操作することができます。

この機能は、HP Operations エージェント配布パッケージを HPOM for Windows、または UNIX/Linux 上の HPOM 管理サーバーにインストールした場合のみ使用可能です。この機能は、HPOM for UNIX 8.x 管理サーバーでは使用できません。

## 事前準備

Performance Collection Component を HPOM コンソールからリモートで設定、制御する前に、エージェントが稼働するノードの HP Operations エージェント インストールメンテーション グループにインストールメンテーション ファイルを配布する必要があります。

インストールメンテーションを HPOM for Windows コンソールから配布するには、以下の手順に従います。

1. クラスタノードを監視する場合、クラスタを構成するすべてのノードにインストールメンテーションを配布し、仮想ノードには配布しないでください。
2. コンソールツリーで、(エージェントが稼働している) ノードまたはノード グループを右クリックし、次に **[すべてのタスク] > [プログラムの配布]** をクリックします。[プログラムの配布] ダイアログボックスが開きます。
3. [プログラムの配布] ダイアログボックスで、**[HP Operations エージェント]** をクリックし、次に **[OK]** をクリックします。必要なインストールメンテーション ファイルが、ノードに配布されます。

インストールメンテーションを UNIX/Linux の HPOM コンソールから配布するには、以下の手順に従います。

**注:** クラスタノードを監視する場合、クラスタを構成するすべてのノードにインストールメンテーションを配布し、仮想ノードには配布しないでください。

1. 管理 UI にログオンします。
2. **[配布] > [設定の配布]** をクリックします。
3. [パラメータの配布] セクションで、[インストールメンテーション] を選択し、**[ノードの選択]** をクリックします。[セレクト] ポップアップボックスが開きます。
4. [セレクト] ポップアップボックスで、エージェント プログラムが稼働しているノードを選択します。
5. [強制更新] オプションを選択し、古いインストールメンテーション ファイルを上書きします。  
このオプションは、エージェントの古いバージョンからアップグレードしたノードで選択します。
6. **[配布]** をクリックします。

## OA-PerfCollComp-opcmsg ポリシーの配布

Performance Collection Component がアラームを生成すると、OA-PerfCollComp-opcmsg ポリシーはアラートメッセージを HPOM メッセージ ブラウザに送信します。このポリシーは、[HP Operations エージェント] > [Performance Collection Component] > [メッセージ インターセプタ] ポリシー グループに配置されています。Performance Collection Component の他のポリシーを配布する前に、このポリシーをノードに配布します。

注: クラスタノードを監視する場合、クラスタを構成するすべてのノードにポリシーを配布し、仮想ノードには配布しないでください。

## Performance Collection Component の設定

HP Operations エージェントの Performance Collection Component の動作は、以下のファイルで指定された設定により決定されます。

- 収集パラメータファイル (**parm**)
- アラーム定義ファイル (**alarmdef**)

収集パラメータファイルとアラーム定義ファイルに関する詳細は、『HP Operations エージェント コンセプトガイド』の Performance Collection Component を参照してください。

## parm ファイルの設定

**parm** ファイルは、scope コレクタのデータ収集メカニズムを定義します。HP Operations エージェントは **parm** ファイルを、すべてのノードの以下のパスに配置します。

HP-UX、Solaris、AIX、Linux の場合 :`/var/opt/perf/`

Windows の場合 :`%ovdatadir%`

**parm** ファイルに指定された設定を変更し、データ収集メカニズムをカスタマイズすることができます。しかし、HP Operations エージェントを備えた多数のノードを管理している場合は、すべてのノード上にある **parm** ファイルの単一コピーをすべて変更することは困難です。

HPOM コンソールを使用すると、変更した **parm** ファイルを一元的に管理サーバーから複数のノードに配布することができます。

## HPOM for Windows の場合

HPOM for Windows コンソールは ConfigFile ポリシーを提供し、**parm** ファイルに対するあらゆる変更を、中央の管理サーバーから複数のノードに配布することができます。ノードのさまざまなオペレーティングシステム用に、異なった ConfigFile ポリシーを利用できます。

**parm** ファイルを編集して収集メカニズムを変更するには、以下の手順に従います。

1. 変更した収集メカニズムを反映させたいノードを特定します。
2. コンソールツリーで、[ポリシー管理] > [ポリシーグループ] > [HP Operations エージェント] > [パフォーマンス収集コンポーネント] > [収集設定] をクリックします。parm ファイルを設定するための ConfigFile ポリシーが、詳細ペインに表示されます。

3. 変更した収集メカニズムを反映させたいプラットフォームの ConfigFile ポリシーをダブルクリックします (HP-UX の場合は **parm** など)。<プラットフォーム> 用 **parm** ファイルのダイアログボックスが開きます。
4. [データ] タブで、設定を変更します。parm ファイルの設定パラメータに関する詳細は、『HP Operations エージェント ユーザーガイド』の parm ファイルパラメータ セクションを参照してください。
5. [ポリシーを保存して閉じる] をクリックします。詳細ペインでポリシーのバージョンが .1 だけ増加します。
6. 更新したポリシーを、選択したノードに配布します。クラスタノードを監視する場合、クラスタを構成するすべてのノードにポリシーを配布し、仮想ノードには配布しないでください。

## UNIX/Linux 9.10 の HPOM の場合

UNIX/Linux 9.10 の HPOM コンソールは ConfigFile ポリシーを提供し、parm ファイルに対するあらゆる変更を、中央の管理サーバーから複数のノードに配布することができます。ノードのさまざまなオペレーティングシステム用に、異なる ConfigFile ポリシーを利用できます。

HPOM for UNIX 9.10 コンソールから parm ファイルを編集して収集メカニズムを変更するには、以下の手順に従います。

1. 変更した収集メカニズムを反映させたいノードを特定します。
2. コンソールで、[参照] > [すべてのポリシー グループ] をクリックします。利用可能なすべてのポリシー グループのリストが、ページに表示されます。
3. [H] をクリックします。HP Operations エージェント ポリシー グループが表示されます。
4. [HP Operations エージェント] をクリックし、[パフォーマンス収集コンポーネント] をクリックして、次に [収集設定] をクリックします。parm ファイルに対して使用可能な ConfigFile ポリシーのリストが表示されます。
5. 変更した収集メカニズムを反映させるプラットフォームの ConfigFile ポリシーをクリックします。[OA\_ <プラットフォーム> ParmPolicy] ポリシー ページが表示されます。
6.  をクリックし、次に [編集 (Raw モード)] をクリックします。[設定ファイルポリシーの編集] ページが表示されます。
7. [内容] タブで、設定を変更します。

parm ファイルの設定パラメータに関する詳細は、『HP Operations エージェント ユーザーガイド』の parm ファイルパラメータ セクションを参照してください。
8. [保存] をクリックします。
9. 更新したポリシーを、選択したノードに配布します。

クラスタノードを監視する場合、クラスタを構成するすべてのノードにポリシーを配布し、仮想ノードには配布しないでください。

## alarmdef ファイルの設定

アラーム定義ファイル (alarmdef) は、パフォーマンス サブエージェントにアラーム生成プロセス用のデフォルト仕様を提供します。HP Operations エージェントは alarmdef ファイルを、すべてのノードの以下のパスに配置します。

HP-UX、Solaris、AIX、Linux の場合 :/var/opt/perf/

Windows の場合 :%ovdatadir%

**alarmdef** ファイルのデフォルト設定を変更し、アラーム生成メカニズムをカスタマイズすることができます。HPOM コンソールを使用して一元的に、変更した **alarmdef** ファイルを複数のノードに配布することができます。

## HPOM for Windows の場合

HPOM for Windows コンソールは ConfigFile ポリシーを提供し、**alarmdef** ファイルに対するあらゆる変更を、中央の管理サーバーから複数のノードに配布することができます。ノードのさまざまなオペレーティングシステム用に、異なった ConfigFile ポリシーを利用できます。

**alarmdef** ファイルを編集して収集メカニズムを変更するには、以下の手順に従います。

変更した収集メカニズムを反映させたいノードを特定します。

1. コンソールツリーで、[ポリシー管理] > [ポリシーグループ] > [HP Operations エージェント] > [パフォーマンス収集コンポーネント] > [アラーム定義] をクリックします。**alarmdef** ファイルを設定するための ConfigFile ポリシーが、詳細ペインに表示されます。
2. 変更した収集メカニズムを反映させたいプラットフォームの ConfigFile ポリシーをダブルクリックします (HP-UX の場合は Alarmdef ファイルなど)。<プラットフォーム> 用 Alarmdef ファイルのダイアログボックスが開きます。
3. [データ] タブで、設定を変更します。**alarmdef** ファイルの設定パラメータに関する詳細は、『HP Operations エージェント ユーザーガイド』の **alarmdef** ファイルパラメータセクションを参照してください。
4. [ポリシーを保存して閉じる] をクリックします。詳細ペインでポリシーのバージョンが .1 だけ増加します。
5. 更新したポリシーを、選択したノードに配布します。

クラスタノードを監視する場合、クラスタを構成するすべてのノードにポリシーを配布し、仮想ノードには配布しないでください。

## UNIX/Linux 9.10 の HPOM の場合

UNIX/Linux 9.10 の HPOM コンソールは ConfigFile ポリシーを提供し、**alarmdef** ファイルに対するあらゆる変更を、中央の管理サーバーから複数のノードに配布することができます。ノードのさまざまなオペレーティングシステム用に、異なった ConfigFile ポリシーを利用できます。

HPOM for UNIX 9.10 コンソールから **alarmdef** ファイルを編集して収集メカニズムを変更するには、以下の手順に従います。

1. 変更したアラートメカニズムを反映させるノードを特定します。
2. コンソールで、[参照] > [すべてのポリシーグループ] をクリックします。利用可能なすべてのポリシーグループのリストが、ページに表示されます。
3. [H] をクリックします。HP Operations エージェントポリシーグループが表示されます。
4. [HP Operations エージェント] をクリックし、[パフォーマンス収集コンポーネント] をクリックして、次に [アラーム定義] をクリックします。**alarmdef** ファイルに使用できる ConfigFile ポリシーのリストが表示されます。

- 変更した収集メカニズムを反映させるプラットフォームの ConfigFile ポリシーをクリックします。[OA\_<platform>AlarmdefPolicy] ポリシー ページが表示されます。



- をクリックし、次に **[編集 (Raw モード)]** をクリックします。[設定ファイルポリシーの編集] ページが表示されます。
- [内容] タブで、設定を変更します。alarmdef ファイルの設定パラメータに関する詳細は、『HP Operations エージェント ユーザー ガイド』の alarmdef ファイル パラメータ セクションを参照してください。
- [保存]** をクリックします。
- 更新したポリシーを、選択したノードに配布します。

クラスタノードを監視する場合、クラスタを構成するすべてのノードにポリシーを配布し、仮想ノードには配布しないでください。

## HP Operations エージェントのリモートからの操作

HPOM コンソールを使用し、HP Operations エージェントの起動、停止、監視、および詳細の表示を行うことができます。HPOM コンソールからさまざまなツールを使用し、HP Operations エージェントの運用を管理することができます。これらのツールは、エージェントが配備されたノードで起動する必要があります。実行したツールの結果は、以下のセクションに表示されます。

### HPOM for Windows

[ツールのステータス] ウィンドウの [ツールの出力] セクション

### UNIX/Linux の HPOM

Java GUI (HPOM for UNIX の操作 UI) の [アプリケーション出力] ウィンドウ

HPOM コンソールから以下のツールを使用できます。

エージェントの起動	管理対象ノードで HP Operations エージェントを起動します。
エージェントの停止	管理対象ノードで HP Operations エージェントを停止します。
エージェントの再起動	管理対象ノードで HP Operations エージェントを再起動します。
ステータス表示	管理対象ノードの HP Operations エージェントのプロセス、サービス、デーモンに関するステータスを表示します。
バージョン情報の表示	管理対象ノードの HP Operations エージェントのバージョンを表示します。
アラーム サービスの更新	Performance Collection Component のアラーム サービスを更新します。
パフォーマンスコンポーネントのログファイルの検索	ノード上で scope コレクタが使用するログファイルを検索します。
パフォーマンスコンポーネントのパラメータファイル構文のチェック	管理対象ノードのパラメータファイルの構文をチェックします。

ツク	
パフォーマンスコンポーネントの Alarmdef ファイル構文のチェック	管理対象ノードの alarmdef ファイルの構文をチェックします。
ポリシー配布アクション投入のステータス表示	<p>parm または alarmdef ポリシーのノードへの配布に関するステータスをチェックします。このツールを起動する際、必ず parm または alarmdef のいずれか適切な方を、ツールパラメータとして指定してください。</p> <p>ツールパラメータは HPOM for Windows を使用するとき、[パラメータの編集] ウィンドウの [パラメータ] ボックスに設定できます。</p> <p>UNIX/Linux で HPOM を使用するとき、そのツールの [ツールステータスの編集] ページを開いて [OVO Tool (OVO ツール)] タブへ移動し、[パラメータ] ボックスにツールパラメータを指定します。</p>
リアルタイム恒久ライセンスの設定	HP Ops OS Inst の恒久ライセンスを Realtime Inst LTU に設定します。
Glance 恒久ライセンスの設定	Glance Software LTU の恒久ライセンスを設定します。
ライセンスステータスの取得	ノードの LTU のステータスを表示します。

## 第11章

### HP Operations エージェントの監視

HP Operations エージェント配布パッケージは、HP Operations エージェントのヘルスを監視するための一連のポリシーを提供します。これらのポリシーを使用すると、必要なエージェント プロセスが停止していないことを確認できます。

HP Operations エージェント配布パッケージを HPOM 監視サーバーにインストールすると、Self Monitoring (自己監視) ポリシーグループが作成されます。Self Monitoring (自己監視) ポリシーグループには、HP Operations エージェントを円滑に機能させるために必要なポリシーが含まれています。

**注:** Self Monitoring (自己監視) ポリシーグループと HP Operations エージェント プロセスのヘルスを監視するためのポリシーは、HP Operations エージェント配布パッケージを HPOM for Windows、または UNIX/Linux 上の HPOM 管理サーバーにインストールした場合のみ使用可能です。これらのポリシーは、HPOM for UNIX 8.x 管理サーバーでは使用できません。

#### 事前準備

Self Monitoring ポリシーを使用して HP Operations エージェントの監視を始める前に、エージェントが稼働するノードの HP Operations エージェント インストールメンテーショングループにインストールメンテーションファイルを配布する必要があります。

インストールメンテーションを HPOM for Windows コンソールから配布するには、以下の手順に従います。

**注:** クラスタノードを監視する場合、クラスタを構成するすべてのノードにインストールメンテーションを配布し、仮想ノードには配布しないでください。

1. コンソールツリーで、(エージェントが稼働している) ノードまたはノードグループを右クリックし、次に **[すべてのタスク] > [プログラムの配布]** をクリックします。[プログラムの配布] ダイアログボックスが開きます。
2. [プログラムの配布] ダイアログボックスで、**[HP Operations エージェント]** をクリックし、次に **[OK]** をクリックします。必要なインストールメンテーションファイルが、ノードに配布されます。

UNIX/Linux 上の HPOM にインストールメンテーションを配布するには

**注:** クラスタノードを監視する場合、クラスタを構成するすべてのノードにインストールメンテーションを配布し、仮想ノードには配布しないでください。

1. 管理 UI にログオンします。
2. **[配布] > [設定の配布]** をクリックします。
3. [パラメータの配布] セクションで、**[インストールメンテーション]** を選択し、**[ノードの選択]** をクリックします。[セレクト] ポップアップボックスが開きます。
4. [セレクト] ポップアップボックスで、エージェントプログラムが稼働しているノードを選択します。

5. [強制更新] オプションを選択し、古いインストールメンテーション ファイルを上書きします (このオプションは、エージェントの古いバージョンからアップグレードしたノードで選択します)。
6. [配布] をクリックします。

## 自己監視ポリシー

Self Monitoring ポリシーを使用することにより、HP Operations エージェントの以下のコンポーネントに関するヘルスを監視することができます。

- **opcmona** (監視エージェント)
- **opcmsga** (メッセージ エージェント)
- **opcmsgi** (メッセージ インターセプタ)
- **opcacta** (アクション エージェント)
- **scope** (データコレクタ)
- **opcle** (ログファイル エンキャプスレータ)
- **opctrapi** (トラップ インターセプタ)
- **coda** (通信 デーモン)
- **perfd**

Self Monitoring ポリシー グループには以下のポリシーが含まれます。

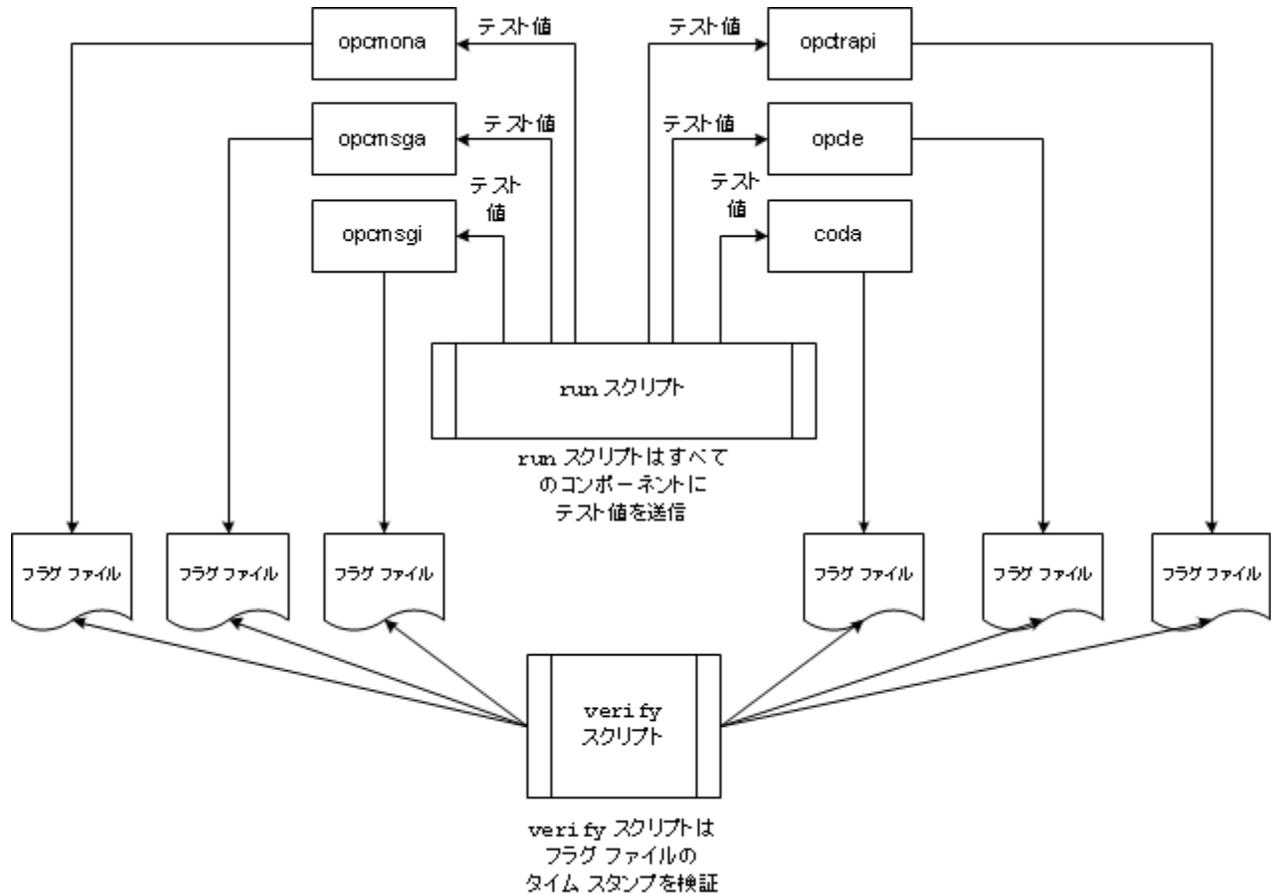
- **OA-SelfMonTstMonaExt**: 監視エージェントのテスト
- **OA-SelfMonVerifyMon**: 監視エージェントによるフラグ ファイルの検証
- **OA-SelfMonTstLe**: ログファイル エンキャプスレータのテスト
- **OA-SelfMonVerifyLe**: ログファイル エンキャプスレータによるフラグ ファイルの検証
- **OA-SelfMonTstTrapi**: SNMP トラップ インターセプタのテスト
- **OA-SelfMonTstMsgi**: メッセージ インターセプタのテスト
- **OA-SelfMonTstActa**: アクション エージェントのテスト
- **OA-SelfMonTstAll**: opcle、opcmona、opcmsgi、および opctrapi を除くすべてのプロセスのテスト

opctrapi コンポーネントのヘルスと可用性を監視するには、SNMP トラップのデーモン/サービスがノードで稼働している必要があります。

HP Operations エージェント インストールメンテーション グループに配布されたスクリプトとプログラムは、HP Operations エージェントのさまざまなコンポーネントにテスト値を送信します (毎分 1 回)。また、すべての監視コンポーネントに対して、**フラグ ファイル**が作成されます。監視コンポーネントが HP Operations エージェント インストールメンテーション スクリプトから発生したテスト値を正常に受信すると、対応するフラグ ファイルのタイムスタンプが更新されます。

HP Operations エージェント インストールメンテーションの検証スクリプトは、定期的に (**3 分**に 1 回) フラグ ファイルの状態を監視します。フラグ ファイルのタイムスタンプが現在時刻より古いことをスクリプトが検出すると、監視コンポーネントがテスト値の受信に失敗したことを意味するので、HPOM メッセージ ブラウザにアラート メッセージが送信されます。

自己監視スクリプトのワークフロー



## 自己監視ポリシーの配布

Self Monitoring ポリシーグループで利用可能なポリシーを、選択的に配布することはできません。これらのポリシーは互いに依存関係にあるので、すべてのポリシーを同時にノードに配布する必要があります。

Self Monitoring ポリシーを HPOM for Windows コンソールから配布するには、以下の手順に従います。

1. HPOM コンソールのコンソールツリーで [ポリシー管理] > [ポリシーグループ] > [HP Operations エージェント] の順に展開します。
2. [自己監視] を右クリックし、[すべてのタスク] > [配布先ノード] をクリックします。[ポリシーの配布先] ダイアログボックスが開きます。
3. [ポリシーの配布先] ダイアログボックスでノードを選択し、次に [OK] をクリックします。HPOM は選択したノードに、Self Monitoring (自己監視) ポリシーの配布を開始します。

**注:** クラスタノードを監視する場合、クラスタを構成するすべてのノードにポリシーを配布し、仮想ノードには配布しないでください。

Self Monitoring (自己監視) ポリシーを UNIX/Linux の HPOM コンソールから配布するには、以下の手順に従います。

1. 管理 UI にログオンします。
2. [OMU] をクリックし、次に [参照] > [すべてのポリシー グループ (All Policy Groups)] をクリックします。[すべてのポリシー グループ (All Policy Groups)] ページが開きます。
3. [すべてのポリシー グループ (All Policy Groups)] ページで、[HP Operations エージェント] ポリシー グループを選択し、[Choose an Action (アクションの選択)] ドロップダウン リストから [Assign to Node/Node Group (ノード/ノード グループへの割り当て)] を選択して  をクリックします。[セレクト] ポップアップ ボックスが開きます。
4. [セレクト] ポップアップ ボックスで、エージェント プログラムが稼働しているノードを選択し、[OK] をクリックします。

クラスタノードを監視する場合、クラスタを構成するすべてのノードにポリシーを配布し、仮想ノードには配布しないでください。

## コンポーネントのステータス表示

Self Monitoring ポリシーはいずれかのコンポーネントの障害を検出すると、エージェントをトリガして適切なアラートメッセージを HPOM コンソールに送信させます。Self Monitoring ポリシーから発生したメッセージには、常に Self Monitor という接頭辞が付いています。Self Monitor という接頭辞が付いたメッセージを開くと、障害の詳細が表示されます。

また、ノード上のフラグ ファイルをチェックして、エージェント コンポーネントが稼働しているかどうかを確認することも可能です。フラグ ファイルは、以下の場所に存在します。

Windows の場合: %ovdatadir%\tmp\OpC\selfmon

UNIX/Linux の場合: /var/opt/OV/tmp/selfmon

フラグ ファイルをテキスト エディタ プログラムで開けば、最新のタイム スタンプをチェックすることができます。最新のタイム スタンプが3分以上古い場合は、監視コンポーネントが機能していないと判断することができます。

## 第12章

### Infrastructure SPI のみのインストール

#### ハードウェアとソフトウェアの要件

サポート対象ハードウェア、オペレーティングシステム、HPOM バージョン、エージェント バージョンの一覧については、サポート マトリックスを参照してください。

#### ディスク領域の要件

HPOM 管理サーバーのオペレーティングシステム	一時ディレクトリ <sup>a</sup>	合計ディスク領域
Windows	%tmp% - 15 MB	90 MB
Linux	/tmp - 35 MB	90 MB
HP-UX	/tmp - 17 MB	240 MB
Solaris	/tmp - 35 MB	80 MB

<sup>a</sup>一時ディレクトリドライブ用のディスク領域は、インストール中にのみ必要になります。これらは概算値です。

#### Infrastructure SPI のインストール

- 管理サーバーにログオンします。
- 次のいずれかの作業を実行します。
  - 物理メディアから Infrastructure SPI をインストールする場合、*HP Operations エージェントおよび Infrastructure SPI 11.10 DVD* を DVD-ROM ドライブに挿入します。
  - いずれかの HP Web サイトからインストールメディア (.iso ファイル) をダウンロードします。  
すべてのプラットフォーム用の配布パッケージが含まれる物理 DVD または .iso ファイルを使用します。プラットフォーム固有の .iso ファイルには、Infrastructure SPI が含まれていません。
- 構成ファイルを作成して、インストール詳細を指定します。  
`oainstall` プログラムにより、配布パッケージの登録中に Infrastructure SPI が管理サーバーにインストールされます。このインストールには、Infrastructure SPI の (HP Reporter に必要な) レポートと (Performance Manager に必要な) グラフのパッケージが含まれています。HP Operations エージェント パッケージの登録を省略するには、次の手順に従います。
  - テキスト エディタで新しいファイルを作成します。
  - 次の内容を追加します。

```
[agent.parameter]  
REGISTER_AGENT=NO
```

```
[hpinfraspi.parameter]  
InfraSPI=  
InfraSPI_With_Graphs=
```

- c. Windows のみ。次の行を追加します。

```
InfraSPI_With_Reports=
```

HP Reporter は Windows でのみサポートされているため、UNIX/Linux システムの設定ファイルで前述の行を追加しても影響はありません。

- d. [hpinfraspi.parameter] セクションでは、次のようにしてください。
- Infrastructure SPI でレポート (Windows のみ) とグラフもインストールするには、ファイルを変更しないでください ([hpinfraspi.parameter] セクションのプロパティの値を設定しないでください)。
  - Infrastructure SPI だけをインストールして、レポート (Windows のみ) とグラフをインストールしない場合は、InfraSPI を YES に設定して、他のプロパティは NO に設定します。
  - Infrastructure SPI とグラフだけをインストールする場合は、InfraSPI\_With\_Graphs を YES に設定して、他のプロパティは NO に設定します。
  - Infrastructure SPI とグラフだけをインストールする (レポートはインストールしない) 場合は、InfraSPI\_With\_Graphs を YES に設定して、他のプロパティは NO に設定します。
  - Infrastructure SPI とレポートだけをインストールする (グラフはインストールしない) 場合は、InfraSPI\_With\_Reports を YES に設定して、他のプロパティは NO に設定します。

**注:** HP Performance Manager が管理サーバーにインストールされていない場合は、グラフパッケージをインストールしないでください。HP Performance Manager がリモートサーバーにインストールされている場合、グラフパッケージを個別にサーバーにインストールする必要があります。HP Reporter は UNIX/Linux ではサポートされていないため、HP Reporter はリモートサーバー上で利用できるようにする必要があります。Infrastructure SPI のレポートパッケージをリモート HP Reporter サーバーにインストールするには、[この手順](#)に従います。

UNIX/Linux 上で HPOM を使用し、HP Performance Manager でグラフを表示する場合、HP Performance Manager を UNIX/Linux 上の HPOM に統合する必要があります ([UNIX/Linux 上での HP Performance Manager の HPOM への統合](#)を参照してください)。

- e. ローカルディレクトリにファイルを保存します。

4. 次のコマンドを実行します。

Windows の場合

```
cscript oainstall.vbs -i -m -spiconfig <config_file>
```

UNIX/Linux の場合

```
./oainstall.sh -i -m -spiconfig <config_file>
```

ここで、<config\_file> は (ファイルへの完全なパスが指定された) 設定ファイルの名前です。

HA クラスタ内に HPOM がある場合、クラスタ内のアクティブ ノードで前述のステップを実行し、HA クラスタ内のすべてのノードで [ステップ 1](#) ~ [ステップ 4](#) を実行します。

### 例

- i. 設定ファイルを作成して、次の内容を指定します。

```
[agent.parameter]
REGISTER_AGENT=NO

[hpinfraspi.parameter]
InfraSPI=YES
InfraSPI_With_Graphs=NO
InfraSPI_With_Reports=NO
```

- ii. 次のディレクトリに config\_file としてファイルを保存します。

C:\temp

- iii. 以下のコマンドを実行して、Infrastructure SPI をインストールします。

```
cscript oainstall.vbs -i -m -spiconfig C:\temp\config_file
```

このコマンドにより、エージェント、レポート パッケージ、グラフ パッケージはインストールせず  
に、Infrastructure SPI がインストールされます。

### レポート パッケージとグラフ パッケージのリモート サーバーへのインストール

HP Reporter と HP Performance Manager が HPOM 管理サーバー以外のサーバーにインストールされている場合、次の手順に従って、Infrastructure SPI のレポート パッケージとグラフ パッケージをインストールする必要があります。

レポート パッケージをインストールするには

1. 管理者として、HP Reporter サーバーにログオンします。
2. システムに *HP Operations エージェントおよび Infrastructure SPI 11.10 メディア* を配置するか、マウントします。
3. 以下のディレクトリに移動します。

Windows X64 システムの場合:

```
<media_root>\integration\infraspi\WIN\Windows_X64
```

Windows X86 システムの場合:

```
<media_root>\integration\infraspi\WIN\Windows_X86
```

4. 次のファイルをインストールします。

```
HPSpiInfR.msi
```

グラフ パッケージをインストールするには

1. 管理者または root として HP Performance Manager サーバーにログオンします。
2. システムに HP Operations エージェントおよび Infrastructure SPI 11.10 メディアを配置するか、マウントします。
3. 以下のディレクトリに移動します。

Linux システムの場合:

```
<media_root>\integration\infraspi\LIN\Linux2.6_X64
```

HP-UX システムの場合:

```
<media_root>\integration\infraspi\HP-UX\HP-UX_IA32
```

Solaris システムの場合:

```
<media_root>\integration\infraspi\SOL\Solaris_SPARC32
```

Windows X64 システムの場合:

```
<media_root>\integration\infraspi\WIN\Windows_X64
```

Windows X86 システムの場合:

```
<media_root>\integration\infraspi\WIN\Windows_X86
```

#### 4. Linux の場合

HPSpiInfG.rpm.gz ファイルのコンテンツを抽出して、HPSpiInfG.rpm ファイルをインストールします。

HP-UX の場合

HPSpiInfG.depot.gz ファイルのコンテンツを抽出して、HPSpiInfG.depot ファイルをインストールします。

Solaris の場合

HPSpiInfG.sparc.gz ファイルのコンテンツを抽出して、HPSpiInfG.sparc ファイルをインストールします。

Windows の場合

HPSpiInfG.msi ファイルをインストールします。

#### 5. UNIX/Linux 上での HP Performance Manager の HPOM への統合 ([UNIX/Linux 上での HP Performance Manager の HPOM への統合](#))

##### ログファイル

登録ログファイル (oainstall.log) は、次のディレクトリにあります。

```
/var/opt/OV/shared/server/log
```

```
%OvDataDir%shared\server\log
```

##### インストールの確認

Infrastructure SPI をインストールしたら、インストールログファイル (oainstall.log) の内容を確認します。インストールが成功している場合は、ファイルにはエラーがなく、ファイルの最後の方に次のメッセージが表示されています。

```
HPSpiSysI installation completed successfully
```

```
HPSpiVmI installation completed successfully
```

```
HPSpiClI installation completed successfully
```

#### UNIX/Linux 上での HP Performance Manager と HPOM の統合

1. HPOM 管理サーバーで、/opt/OV/contrib/OpC/OVPM ディレクトリに移動します。
2. 次のコマンドを実行します。

```
./install_OVPM.sh <hostname>:<port>
```

この場合、<hostname> は HP Performance Manager サーバーの FQDN であり、<port> は HP Performance Manager によって使用されるポートです。HP Performance Manager が HPOM 管理サーバーにインストールされていても、同じコマンドと同じオプションを使用します。

#### Infrastructure SPI ライセンス

System Infrastructure SPI または Virtualization Infrastructure SPI に個別のライセンスは必要ありません。これらの SPI は、HP Software Operations Instance Advanced LTU (使用権) の購入に含まれています。Cluster Infrastructure SPI の LTU と CI SPI の LTU は、HP Software Operations Instance Advanced LTU を 1 つ購入するたびに含まれています。

Virtualization Infrastructure SPI のライセンス要件は、Virtualization Infrastructure SPI を使用して HPOM サーバーによって管理される仮想化された環境内の仮想インスタンスの数に従って定義されます。

- **Microsoft Hyper-V:** Hyper-V の場合、ライセンスは Virtualization Infrastructure SPI が配布される Hyper-V ホストの数によって決まります。Virtualization Infrastructure SPI によって監視される Hyper-V ホスト システムには、それぞれ個別の VI SPI LTU が必要になります。
- **VMware:** Virtualization Infrastructure SPI による監視対象として vMA に追加された ESX および ESXi ホストには、それぞれ個別の VI SPI LTU が必要になります。Virtualization Infrastructure SPI による監視対象として vMA に追加された vCenter には、それぞれ個別の VI SPI LTU が必要になります。
- **HPVM:** HPVM サーバーの場合、ライセンスは Virtualization Infrastructure SPI を配布する HPVM サーバーの数によって決まります。Virtualization Infrastructure SPI で監視する HPVM サーバーには、それぞれ個別の VI SPI LTU が必要になります。
- **AIX LPAR:** AIX LPAR の場合、ライセンスは Virtualization Infrastructure SPI を配布する LPAR サーバーの数によって決まります。Virtualization Infrastructure SPI インストールごとにそれぞれ個別の VI SPI LTU が必要になります。
- **Oracle Solaris ゾーン:** Oracle Solaris ゾーンの場合、ライセンスは Virtualization Infrastructure SPI を配布するグローバルゾーンの数によって決まります。Virtualization Infrastructure SPI で監視するグローバルゾーンには、それぞれ個別の VI SPI LTU が必要になります。

Virtualization Infrastructure SPI には、インストール後 60 日間当該製品を使用できる、試用ライセンスが付いています。

ライセンスの取得方法、永久ライセンスキー パスワード の適用方法、または HPOM でのライセンス レポートの表示方法の詳細は、『*HP Operations Manager for Windows インストールガイド*』または『*HP Operations Manager for UNIX インストールガイド*』を参照してください。

## HPOM for Windows での Infrastructure SPIs のコンポーネント

以下に、HPOM for Windows コンソールでの Infrastructure SPIs のコンポーネントを示します。

#### サービス

ノードを HPOM for Windows ノード グループに追加すると、SI SPI サービス検出ポリシーが自動的に配布されます。

このサービス検出ポリシーは、ノード上のシステムインフラストラクチャとサービスを検出し、この情報を HPOM サービス領域に追加します。

SI SPI サービスマップを表示するには、**[サービス]→[Systems Infrastructure]** を選択します。The SI SPI service map 検出されたシステムとインスタンスをグラフィカルに表示します。

**注:** SI SPI 検出ポリシーと QuickStart ポリシーは新しいノードに自動配布され (自動配布が有効になっている場合)、HPOM for Windows サーバーに追加されます。既存のノードでは、SI SPI 検出ポリシーを手動で配布する必要があります。

#### Virtual Infrastructure の検出

SI SPI 検出ポリシーによってノードが仮想化ノードとして特定されると、VI SPI 検出が自動配布されます。これらのノードで実行されている仮想マシンがそれぞれの Virtualization Infrastructure ノードグループの下に追加され、ベンダー固有の QuickStart ポリシーがこれらのノードに自動配布されます。

VI SPI 検出ポリシーによって、検出された要素が HPOM サービスマップに追加されます。VI SPI サービスマップを表示するには、**[サービス]→[Virtualization Infrastructure.]** を選択します。VI SPI サービスマップは、検出された仮想システムをグラフィカルに表示します。

#### クラスタ インフラストラクチャの検出

HPOM for Windows では、SI SPI 検出ポリシーがノードをクラスタノードとして識別した場合、そのノード上で CI SPI 検出ポリシーが起動されます。CI SPI 検出は、クラスタ、クラスタノード、およびリソースグループを検出します。Cluster Infrastructure SPI サービスマップを表示するには、**[サービス]→[Cluster Infrastructure]** の順に選択します。

#### サービスタイプモデル

サービスタイプモデルでは、登録ノードのノードの論理的な割り当て先となるサービスタイプカテゴリが表示されます。HPOM for Windows では、サービスタイプモデルを表示できます。

#### ノードグループ

Systems Infrastructure SPI 2.01 をインストールすると、コンソールツリーの **[ノード]** フォルダの下にノードグループが追加されます。

**注:** 英語以外のロケールでも、ノードグループ名は英語で表示されます。

#### ポリシー管理

ポリシーは、[Infrastructure Management] の下で言語に従ってグループ化されます。たとえば、英語のポリシーは **[en]** の下で、日本語のポリシーは **[ja]** の下で、簡体中国語のポリシーは **[zh]** の下でグループ化されます。言語のグループは、インストール時に選択した言語に従って表示されます。

**注:** ConfigFile ポリシーの SI-ConfigureDiscovery および VI-VMwareEventTypes には、ローカライズされた名前はありません。英語以外のロケールであっても、ポリシー名は英語版と同じです。

それ以降のグループ化は、インストール時に選択した SI SPI、CI SPI、および VI SPI に基づきます。各 SPI の下では、パフォーマンス、可用性、容量、ログ、およびイベントによってポリシーがグループ化されます。

ベンダーに基づいたポリシーグループもあります。このグループの下では、さまざまなオペレーティングシステムやベンダーに基づいてポリシーが再度グループ化されます。ベンダー別にグループ化されたポリシーには、QuickStart ポリシーと高度なポリシーがあります。QuickStart ポリシーがノードそれぞれのノードグループに追加されると、サポートされている管理ノードに自動的に配布されます。サービス検出時にポリシーを自動配布する設定をオフにすることができます。また、設定済みのポリシーを変更して新しい名前で作成し、目的に応じたカスタムポリシーを作成することもできます。

Systems Infrastructure SPI ポリシーを表示しアクセスするには、**[ポリシー管理]**→**[ポリシーグループ]**→**[Infrastructure Management]**→**[<言語>]**→**[Systems Infrastructure]**の順に選択します。

VI SPI ポリシーを表示してアクセスするには、**[ポリシー管理]**→**[ポリシーグループ]**→**[Infrastructure Management]**→**[<言語>]**→**[Virtualization Infrastructure]**の順に選択します。

Cluster Infrastructure SPI ポリシーを表示しアクセスするには、**[ポリシー管理]**→**[ポリシーグループ]**→**[Infrastructure Management]**→**[<言語>]**→**[Cluster Infrastructure]**の順に選択します。

#### ツール

ツールは SI SPI および VI SPI 用に提供されます。Systems Infrastructure SPI ツールグループにアクセスするには、**[ツール]**→**[システム インフラストラクチャ]**の順に選択し、VI SPI ツールグループにアクセスするには、**[ツール]**→**[仮想化 インフラストラクチャ]**の順に選択します。

#### レポート

HP Reporter が HPOM for Windows 管理サーバーにインストールされている場合、HPOM for Windows コンソールからレポートグループを表示できます。

#### グラフ

SI SPI と VI SPI には、一連の設定済みのグラフが備わっています。HPOM コンソールからグラフにアクセスするには、Infrastructure SPI グラフパッケージをインストールする前に、HP Performance Manager を HPOM 管理サーバーにインストールする必要があります。

I SPI グラフにアクセスするには、以下の図に示すように **[Graphs]**→**[インフラストラクチャのパフォーマンス]**の順に選択し、VI SPI グラフにアクセスするには、**[Graphs]**→**[インフラストラクチャのパフォーマンス]**→**[仮想化]**の順に選択します。

または HP Performance Manager が HPOM 管理サーバーに接続している別の (スタンドアロン) システムにインストールされている場合、HP Performance Manager スタンドアロンシステム上でグラフを表示できます。

## HPOM for UNIX での Infrastructure SPIs のコンポーネント

以下に、HPOM for UNIX (HP-UX、Linux、および Solaris) 管理 UI での Infrastructure SPIs のコンポーネントを示します。

#### サービス

SI-service 検出ポリシーは、ノード上のシステム インフラストラクチャとサービスを検出し、この情報を HPOM サービス領域に追加します。サービス マップとオペレータ コンソールの表示には Java GUI を使用します。Java GUI は別のシステムにインストールする必要があります。

#### Virtual Infrastructure の検出

システム検出によってノードが仮想化ノードとして特定されると、VI SPI 検出が自動配布されます。これらのノードで実行されている仮想マシンがそれぞれの Virtualization Infrastructure ノード グループの下に追加され、ベンダー固有の QuickStart ポリシーがこれらのノードに自動で割り当てられます。

VI SPI 検出ポリシーは、管理ノード (ホスト マシン) 上でホストされている仮想マシン (ゲスト マシン) を検出し、この情報を HPOM サービス領域に追加します。VI SPI サービス マップを表示するには、[サービス]> [Virtualization Infrastructure]> [グラフの表示] の順に選択します。サービス マップは、検出された仮想システムをグラフィカルに表示します。

#### クラスタ インフラストラクチャの検出

クラスタノードを HPOM for HP-UX、Linux、または Solaris 登録ノードに追加した場合は、CI SPI サービス検出を手動で配布します。CI SPI 検出は、クラスタ、クラスタ ノード、およびリソースグループを検出します。CI SPI サービス マップを表示するには、[サービス]→ [Cluster Infrastructure ]→ [グラフの表示] の順に選択します。

#### ポリシー管理

ポリシーは、[Infrastructure Management] の下で言語に従ってグループ化されます。たとえば、英語のポリシーは [en] の下で、日本語のポリシーは [ja] の下で、簡体中国語のポリシーは [zh] の下でグループ化されます。言語のグループは、インストール時に選択した言語に従って表示されます。

ベンダーに基づいたポリシー グループもあります。このグループの下では、さまざまなオペレーティングシステムやベンダーに基づいてポリシーが再度グループ化されます。ベンダー別にグループ化されたポリシーには、QuickStart ポリシーと高度なポリシーがあります。QuickStart ポリシーが各ノード グループに追加されると、管理ノードに自動的に割り当てられます。このポリシーは、ノードに手動で配布できません。

また、設定済みのポリシーを変更して新しい名前で作成し、目的に応じたカスタムポリシーを作成することもできます。

SI SPI ポリシーを表示してアクセスするには、[Policy Bank]→[Infrastructure Management]→ [<言語>]→ [Systems Infrastructure] の順に選択します。

VI SPI ポリシーを表示してアクセスするには、[Policy Bank]→[Infrastructure Management]→ [<言語>]→ [Virtualization Infrastructure] の順に選択します。

CI SPI ポリシーを表示してアクセスするには、[Policy Bank]→[Infrastructure Management]→ [<言語>]→ [Cluster Infrastructure] の順に選択します。

#### ツール

Infrastructure SPIs には、SI SPI および VI SPI 用のツールが用意されています。SI SPI ツールグループにアクセスするには、[Tool Bank]→ [Systems Infrastructure] の順に選択し、VI SPI ツールグループにアクセスするには、[Tool Bank]→ [Virtualization Infrastructure] の順に選択します。

#### レポート

HP-UX、Linux、および Solaris オペレーティングシステム用の HPOM を使用する場合は、HP Reporter を管理サーバーに接続されている別の (スタンドアロン) システムにインストールします。レポートは、HP Reporter スタンドアロンシステムで表示できます。

HP Reporter と HPOM を統合する方法の詳細は、『HP Reporter インストールおよび特別構成ガイド』を参照してください。

#### グラフ

Infrastructure SPIs には、SI SPI および VI SPI 用のグラフが用意されています。収集されたデータからグラフを生成および表示するには、HP Performance Manager を HPOM と連動して使用する必要があります。

グラフにアクセスするには、アクティブなメッセージを選択して [メッセージのプロパティ] ウィンドウを開き、[アクション] をクリックします。[オペレータ起動アクション] セクションで、**[起動]** をクリックします。または、アクティブなメッセージを右クリックして **[アクションの起動/停止]** を選択し、**[オペレータ起動アクションの起動]** をクリックします。

HP Performance Manager が管理サーバーにインストールされている場合、管理サーバー上でグラフを起動して表示できます。HP Performance Manager が HPOM 管理サーバーに接続している別の (スタンドアロン) システムにインストールされている場合は、HP Performance Manager スタンドアロンシステム上でグラフを表示できます。

## 第13章

---

### HP Operations エージェント のアンインストール

1. root または管理者でノードにログオンします。
2. 以下のコマンドを実行して、すべてのエージェント プロセスを停止します。

```
opcagt -stop
```

```
ttd -k
```

3. 以下のディレクトリに移動します。

Windows 64 ビット

```
%OvInstallDir%bin\win64\OpC\install\%OvInstallDir%bin\win64\OpC\install
```

その他の Windows

```
%OvInstallDir%bin\OpC\install\cscript oainstall.vbs -r -a
```

Linux、HP-UX、Solaris

```
/opt/OV/bin/OpC/install/oainstall.sh -r -a
```

AIX

```
/usr/lpp/OV/bin/OpC/install/oainstall.sh -r -a
```

4. 以下のディレクトリを手動で削除します。

*Windows の場合:*

```
%OvInstallDir%
```

```
%OvDataDir%
```

*HP-UX、Solaris、Linux の場合:*

```
/opt/OV
```

```
/var/opt/OV
```

```
/opt/perf
```

```
/var/opt/perf
```

*AIX の場合:*

```
/usr/lpp/OV
```

```
/var/opt/OV
```

```
/usr/lpp/perf
```

```
/var/opt/perf
```

または、Windows ノードで [プログラムの追加と削除] ウィンドウを使用し、HP Operations エージェント 11.10 を削除することも可能です。

## 第14章

### Infrastructure SPI のアンインストール

#### 管理ノードからの Infrastructure SPI ポリシーの削除

##### HPOM for Windows の場合

1. HPOM コンソールツリーで、[Operations Manager] > [ポリシー管理] > [ポリシーグループ] > [Infrastructure Management] の順にフォルダを展開します。
2. [Infrastructure Management] を右クリックし、[すべてのタスク] > [アンインストールする対象ノード...] の順に選択します。
3. [ポリシーをアンインストールする対象ノード...] ダイアログボックスで [すべてのノード] を選択し、次に [OK] をクリックします。

##### UNIX/Linux の HPOM の場合

1. 管理者として HPOM コンソールにログオンします。
2. [参照] メニューから [すべてのポリシー割り当て] を選択します。[すべてのポリシー割り当て] ウィンドウが開きます。
3. [すべてのポリシー割り当て] ウィンドウで、ポリシーに対する [割り当てモード] チェックボックスをオンにして、ノードまたはノードグループから削除するポリシーまたはポリシーグループを選択します。
4. [アクションを選択] ボックスから [割り当てを削除...] を選択して、[Submit] をクリックします。操作を元に戻すことができないことを示す、メッセージ ウィンドウが表示されます。
5. [OK] をクリックします。ノードから選択されたポリシー割り当てが削除されます。
6. HPOM 管理 UI から、登録オブジェクト カテゴリ下の [登録ノード] をクリックします。[登録ノード] ウィンドウが開きます。
7. [登録ノード] ウィンドウで、ポリシーを削除するノードまたはノードグループを選択します。
8. [アクションを選択] ボックスから [このグループから割り当て解除...] を選択して、[Submit] をクリックします。

選択したノードからポリシーが削除されます。

すべてのポリシーがすべてのノードからアンインストールされるまで待機する必要があります。ポリシーのアンインストールのステータスは、[配布ジョブ] ウィンドウで参照できます。

#### Infrastructure SPI のアンインストール

**注:** Infrastructure SPI を削除するには、管理サーバー上でほぼ 240 MB の合計ディスク領域および一時フォルダとして 35 MB の領域が使用可能なことを確認してください。

1. 管理サーバーにログオンします。
2. 以下のディレクトリに移動します。

##### Windows の場合

```
%ovinstalldir%bin\OpC\agtinstall
```

*UNIX/Linux の場合*

```
/opt/OV/bin/OpC/agtinstall
```

3. 次のコマンドを実行します。

*Windows の場合*

```
cscript oainstall.vbs -r -m -spiconfig
```

*UNIX/Linux の場合*

```
./oainstall.sh -i -m -spiconfig
```

上記のステップは、はじめに HA クラスタ内のアクティブ ノードで実行してから、クラスタ内のすべてのノードで実行します。