HP Operations Smart Plug-in for Systems Infrastructure

ソフトウェア バージョン: 12.00
HP Operations Manager (Windows®、HP-UX、Linux、および Solaris オペレーティング システム向け)

ユーザー ガイド

ドキュメント リリース日 : 2015 年 9 月 (英語版)
ソフトウェア リリース日 : 2015 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。ここでの記載は、追加保証を提供するものではありません。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文書類、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

商標について

Adobe™ は、Adobe Systems Incorporated (アドビシステムズ社) の登録商標です。

Microsoft ® および Windows ® 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。

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 バージョンの番号は、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変更されます。
- 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。

更新状況、およびご使用のドキュメントが最新版かどうかは、次のサイトで確認できます。
https://softwaresupport.hp.com

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 の登録は、次の Web サイトから行うことができます。**https://hpp12.passport.hp.com/hppcf/createuser.do**

または、HP ソフトウェアサポートページ上部の**登録**リンクをクリックしてください。

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。**https://softwaresupport.hp.com**

このサイトでは、HP のお客様窓口のほか、HP ソフトウェアが提供する製品、サービス、およびサポートに関する詳細情報をご覧いただけます。

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。お客様のビジネスを管理するのに必要な対話型の技術サポートツールに、素早く効率的にアクセスできます。HP ソフトウェアサポートの Web サイトでは、次のようなことができます。

- 関心のあるナレッジドキュメントの検索
- サポートケースの登録とエンハンスメント要求のトラッキング
- 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

一部のサポートを除き、サポートのご利用には、HP Passport ユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HP Passport ID を登録するには、次の Web サイトにアクセスしてください。

https://hpp12.passport.hp.com/hppcf/createuser.do

アクセスレベルの詳細については、次の Web サイトをご覧ください。

https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now は、HPSW のソリューションと統合に関するポータル Web サイトです。このサイトでは、お客様のビジネスニーズを満たす HP 製品ソリューションを検索したり、HP 製品間の統合に関する詳細なリストや ITIL プロセスのリストを閲覧することができます。このサイトの URL は **http://h20230.www2.hp.com/sc/solutions/index.jsp** です。

目次

第1章: このドキュメントで使用する名称 7
第2章: はじめに 9
第3章: Systems Infrastructure SPI のコンポーネント 10
HPOM for Windows のマップ ビュー 10
HPOM for UNIX のマップ ビュー 11
ツール 13
ポリシー 13
グラフ 14
レポート 15
第4章: 作業の開始 16
HPOM for Windows の場合 16
SI SPI の起動 16
Quick Start ポリシーの HPOM for Windows からの配布 17
HPOM for UNIX の場合 18
SI SPI の起動 19
Quick Start ポリシーの HPOM for UNIX からの配布 19
レポートとグラフの表示 20
HP Performance Manager と HPOM for UNIX との統合 20
SPI のアップグレード後のレポートの更新 21
レポート用のデータ収集 21
第5章: Systems Infrastructure SPI のポリシー 22
トレース 22
検出ポリシー 23
検出の制限 23
プロセスとサービスを監視するポリシー 27
可用性ポリシー 33
SI-ProcessMonitor 33
SI-ZombieProcessCountMonitor 37
設定変更ポリシー 38
SI-ChangeConfigurationMonitor 38
ハードウェア監視ポリシー 43
ポート番号の変更 43
Server Health Traps Monitor ポリシー 44
RAID Controller Traps Monitor ポリシー 47
NIC Traps Monitor ポリシー 48
CMC Traps Monitor ポリシー 49
System Information Traps Monitor ポリシー 51

Virtual Connect Domain Traps Monitor ポリシー 51
Cluster Traps Monitor ポリシー 52
Rack Power Manager Traps Monitor ポリシー 53
Intelligent Drive Array Traps Monitor ポリシー 58
Rack Information Traps Monitor ポリシー 72
UPS Traps Monitor ポリシー 77
Blade Type 2 Traps Monitor ポリシー 78
Storage Systems Traps Monitor ポリシー 79
Virtual Connect Module Traps Monitor ポリシー 86
SIM Agent Process Monitoring ポリシー 87
容量ポリシー 87
Disk Capacity Monitor ポリシー 87
Remote Drive Space Utilization Monitor ポリシー 94
NFS ファイル システム用の Remote Drive Space Utilization Monitor ポリシー 95
CIFS ファイル システム用の Remote Drive Space Utilization Monitor ポリシー 96
Paged and Nonpaged Pool Utilization ポリシー 97
ログ監視ポリシー 98
Linux システム サービス ログ ファイル ポリシー 98
Boot Log ポリシー 99
Secure Log ポリシー 99
Kernel Log ポリシー 99
Windows システム サービス ログ ファイル ポリシー 100
NFS Log ポリシー 100
DNS Log ポリシー 100
Windows Logon ポリシー 101
Terminal Service Log ポリシー 101
Windows Server DHCP 101
AIX システム ログ ファイル監視ポリシー 102
ERRPT Log Monitoring ポリシー 102
パフォーマンス ポリシー 102
Network Usage and Performance ポリシー 103
Memory Bottleneck Diagnosis ポリシー 107
CPU Spike Check ポリシー 111
CPU Bottleneck Diagnosis ポリシー 114
Sample Performance ポリシー 115
Disk Peak Utilization Monitor ポリシー 116
RealTimeAlerts ポリシー 117
SI-CPUStealtimeUtilMonitor 121
Adaptive Thresholding ポリシー 121
SI-ConfigureBaselining ポリシーの設定と配布 122
SI-AdaptiveThresholdingMonitor ポリシーの設定と配布 123
偏差の設定 123

SI-ConfigureBaselining ポリシーでの偏差の設定 124
SI-AdaptiveThresholdingMonitor ポリシーでの偏差の設定 126
アラート メッセージの生成 127
使用例: 適応監視に対するベースライン データの使用 128
CPU 使用率の監視 129
セキュリティ ポリシー 130
Windows 用の Failed Login Collector ポリシー 131
Windows 用の Last Logon Collector ポリシー 131
Linux 用の Failed Login Collector ポリシー 131
Linux 用の Last Logon Collector ポリシー 132
Linux 用の Bad Login ポリシー 133
AIX 用の Bad Login ポリシー 133
AIX 用の Logins ポリシー 134
AIX 用の Switch User ポリシー 134
AIX 用の Sys Log ポリシー 135
HP-UX 用の Bad Logins ポリシー 135
HP-UX 用の Logins ポリシー 136
HP-UX 用の Switch User ポリシー 136
HP-UX 用の Syslog ポリシー 137
Sun Solaris Bad Logins 137
Sun Solaris Logins 138
Sun Solaris snmp Log ポリシー 138
Sun Solaris Syslog ポリシー 139
HPOM for Windows 管理サーバーからの SI SPI ポリシーの配布 139
HPOM for UNIX 管理サーバーからの SI SPI ポリシーの配布 140
タスク 1: ポリシーまたはポリシー グループの割り当て 141
タスク 2: ポリシーの配布 141
Systems Infrastructure SPI ツール 141
ユーザーの前回のログイン ツール 141
Energy Data Collector 142
第6章: Systems Infrastructure SPI のレポートとグラフ 147
Systems Infrastructure SPI のレポート 147
Systems Infrastructure SPI のグラフ 149
第7章: トラブルシューティング 152
ドキュメントのフィードバックを送信 157

第1章: このドキュメントで使用する名称

このドキュメントでは、以下の名称を使用します。

名称	説明
HPOM for UNIX	HPOM for UNIX は、HPOM on HP-UX、HPOM on Linux、および HPOM on Solaris の総称としてドキュメントで使用されます。 オペレーティング システムを区別する必要がある場合は次の名称を使用します。 • HPOM on HP-UX • HPOM on Linux • HPOM on Solaris
Infrastructure SPIs	HP Operations Smart Plug-ins for Infrastructure を示します。このソフトウェア スイートには、以下の 3 つの Smart Plug-in が含まれています。 • HP Operations Smart Plug-in for Systems Infrastructure • HP Operations Smart Plug-in for Virtualization Infrastructure • HP Operations Smart Plug-in for Cluster Infrastructure
SI SPI	HP Operations Smart Plug-in for Systems Infrastructure
VI SPI	HP Operations Smart Plug-in for Virtualization Infrastructure
CI SPI	HP Operations Smart Plug-in for Cluster Infrastructure
%OvDataDir%	Windows 管理サーバーおよび管理ノード上のデータ ディレクトリ変数です。この変数は、インストーラによって設定されます。ユーザー要件に合わせてパスをリセットできます。デフォルト値は `C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software` です。
$OvDataDir	HPOM for UNIX 管理サーバーおよび UNIX 管理ノードでのデータ ディレクトリ変数です。すべての UNIX ノードおよびサーバーでは、データ ディレクトリは次のとおりです。 • HP-UX (ノードおよびサーバー): `/var/opt/OV` • Linux (ノードおよびサーバー): `/var/opt/OV` • Solaris (ノードおよびサーバー): `/var/opt/OV` • AIX (ノード): `/var/opt/OV` この変数は変更できません。

名称	説明
%OvInstallDir%	Windows 管理サーバーおよび管理ノード上でのインストール ディレクトリ変数です。この変数は、インストーラによって設定されます。ユーザー要件に合わせてパスをリセットできます。デフォルト値は C:\Program Files\HP\HP BTO Software です。
$OvInstallDir	HPOM for UNIX 管理サーバーおよび UNIX 管理ノードでのインストール ディレクトリ変数です。すべての UNIX ノードおよびサーバーでは、インストール ディレクトリは次のとおりです。 • HP-UX (ノードおよびサーバー):/opt/OV • Linux (ノードおよびサーバー):/opt/OV • Solaris (ノードおよびサーバー):/opt/OV • AIX (ノード):/usr/lpp/OV 上記の変数は変更できません。

第2章: はじめに

システム インフラストラクチャは、企業にとって欠かせない基盤またはベース インフラストラクチャです。システム インフラストラクチャは、CPU、オペレーティング システム、ディスク、メモリ、ネットワーク リソースなどで構成されていますが、これを継続的に監視することによって、基盤となる物理システムの可用性、パフォーマンス、セキュリティ、スムーズな動作を確保する必要があります。監視システム インフラストラクチャは、効率化や生産性向上を実現します。また、インフラストラクチャの障害やパフォーマンス低下を引き起こす根本原因の関連性の特定、切り分け、修正などの作業でも役立ちます。

HP Operations Smart Plug-in for Systems Infrastructure (SI SPI) は、Microsoft Windows、Linux、Oracle Solaris、IBM AIX、HP-UX 用のシステム インフラストラクチャを監視します。容量、可用性、使用率などの監視要素に基づいてシステム パフォーマンスを分析できます。

SI SPI は、HP Operations Smart Plug-ins for Infrastructure スイート (Infrastructure SPIs) の一部として提供されています。このスイートには他にも、Virtualization Infrastructure Smart Plug-ins (VI SPI)、Cluster Infrastructure Smart Plug-ins (CI SPI)、レポート パック、グラフ パックなどが含まれています。Infrastructure SPIs メディアに収録されている他のコンポーネントをインストールする場合は、SI SPI をインストールする必要があります。

注: HP Reporter 4.0 は、64 ビット版の Windows オペレーティング システムでサポートされます。

SI SPI は、HP Operations Manager (HPOM)、HP Performance Manager、HP Performance Agent、HP Operations Agent の組み込みパフォーマンス コンポーネント (EPC) などの HP ソフトウェア製品と統合します。この統合により、ポリシー、ツール、各種サービス ビューが提供されます。

SI SPI でサポートしているオペレーティング システムのバージョンの詳細は、『HP Operations Smart Plug-in for Systems Infrastructure リリース ノート』を参照してください。

第3章: Systems Infrastructure SPI のコンポーネント

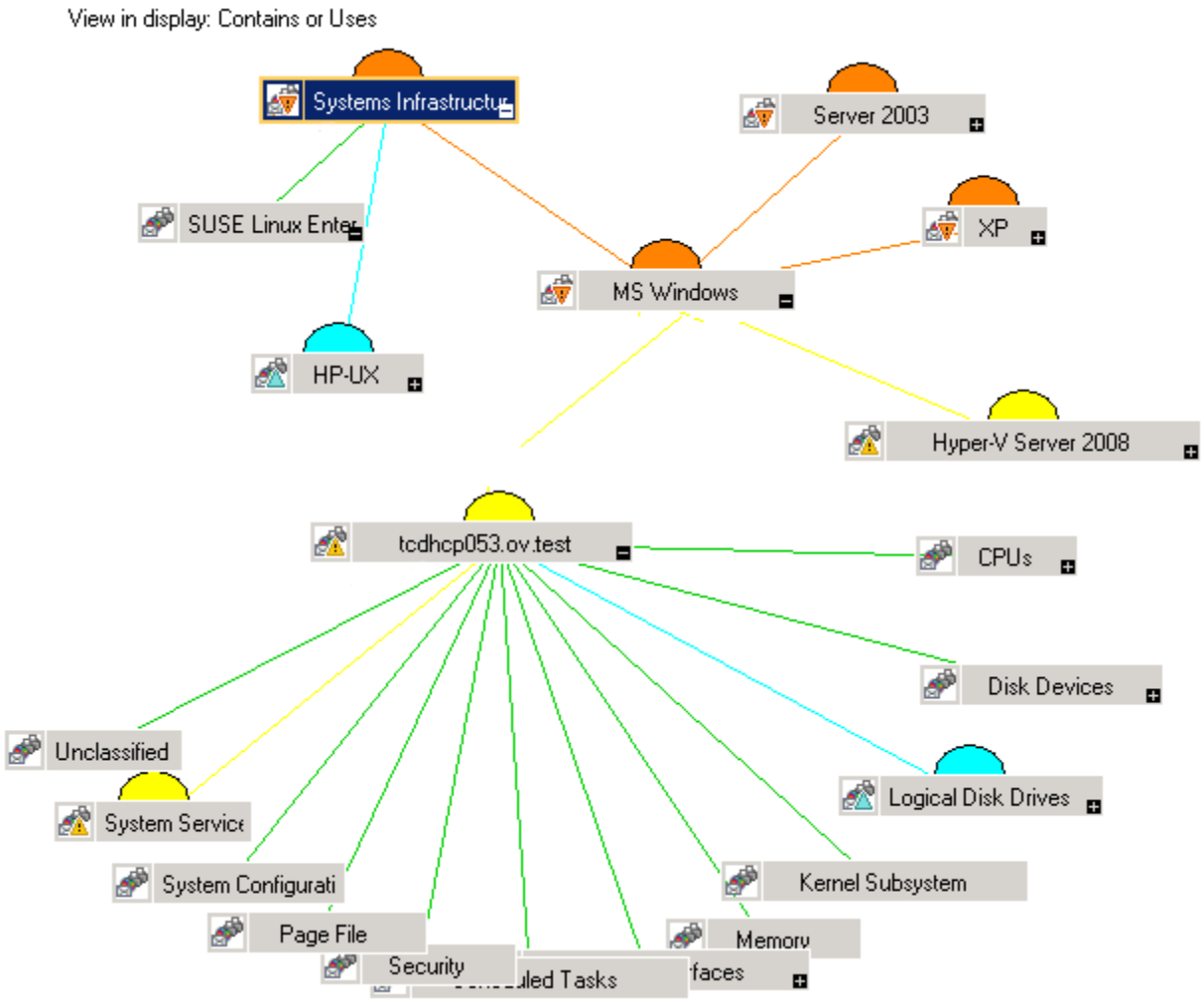
SI SPI は、管理ノードの動作、可用性、パフォーマンスを監視するための設定済みポリシーとツールを提供します。これらのポリシーおよびツールと検出機能を組み合わせて使用することにより、IT インフラストラクチャの重要な要素をすばやくコントロールできます。

HPOM for Windows のマップ ビュー

検出ポリシーによってノードが特定される前に、『HP Operations Infrastructure Smart Plug-ins インストール ガイド』の「SI SPI の起動」を読んでください。この項では、SI SPI ポリシーを配布するための前提条件について説明しています。

HPOM コンソールにノードを追加すると、そのノードに SI SPI service discovery ポリシーが自動的に配布されます。この情報は、ノードとサービスを示す SI SPI のマップ ビューに反映されます。

マップ ビューには、インフラストラクチャ環境のリアルタイムな状態が表示されます。マップ ビューを表示するには、HPOM コンソールで **[サービス]** を選択し、**[Systems Infrastructure]** をクリックします。マップ ビューには、インフラストラクチャ環境のサービスまたはノードの階層構造全体が、サブシステムやサブサービスを含め、グラフィカルに表示されます。次の図に、HPOM for Windows のマップ ビューを示します。



マップのアイコンや線は色分けされており、マップの項目の重要度レベルやステータス伝達が示されます。マップ ビューでは、ノードまたはサービス階層の問題が発生しているレベルにドリル ダウンできます。

サービス ビューに、検出された要素がグラフィカルに表示されることで、問題を迅速に診断できます。

- メッセージ ブラウザに表示された問題の根本原因を表示するには、**[表示]** → **[障害原因]** をクリックします。
- 問題の影響を受けているサービスとシステム コンポーネントを表示するには、**[表示]** → **[影響範囲]** をクリックします。

HPOM for UNIX のマップ ビュー

検出ポリシーによってノードが特定される前に、『HP Operations Infrastructure Smart Plug-ins インストール ガイド』の「SI SPI の起動」を読んでください。この項では、SI SPI ポリシーを配布するた

めの前提条件について説明しています。

マップ ビューには、インフラストラクチャ環境のリアルタイムな状態が表示されます。管理サーバーで以下のコマンドを実行すると、HPOM for HP-UX、Solaris、Linux の操作インターフェイスでオペレータがサービス ビューを表示できるようになります。

```
opcservice -assign <オペレータ名 > SystemServices
```

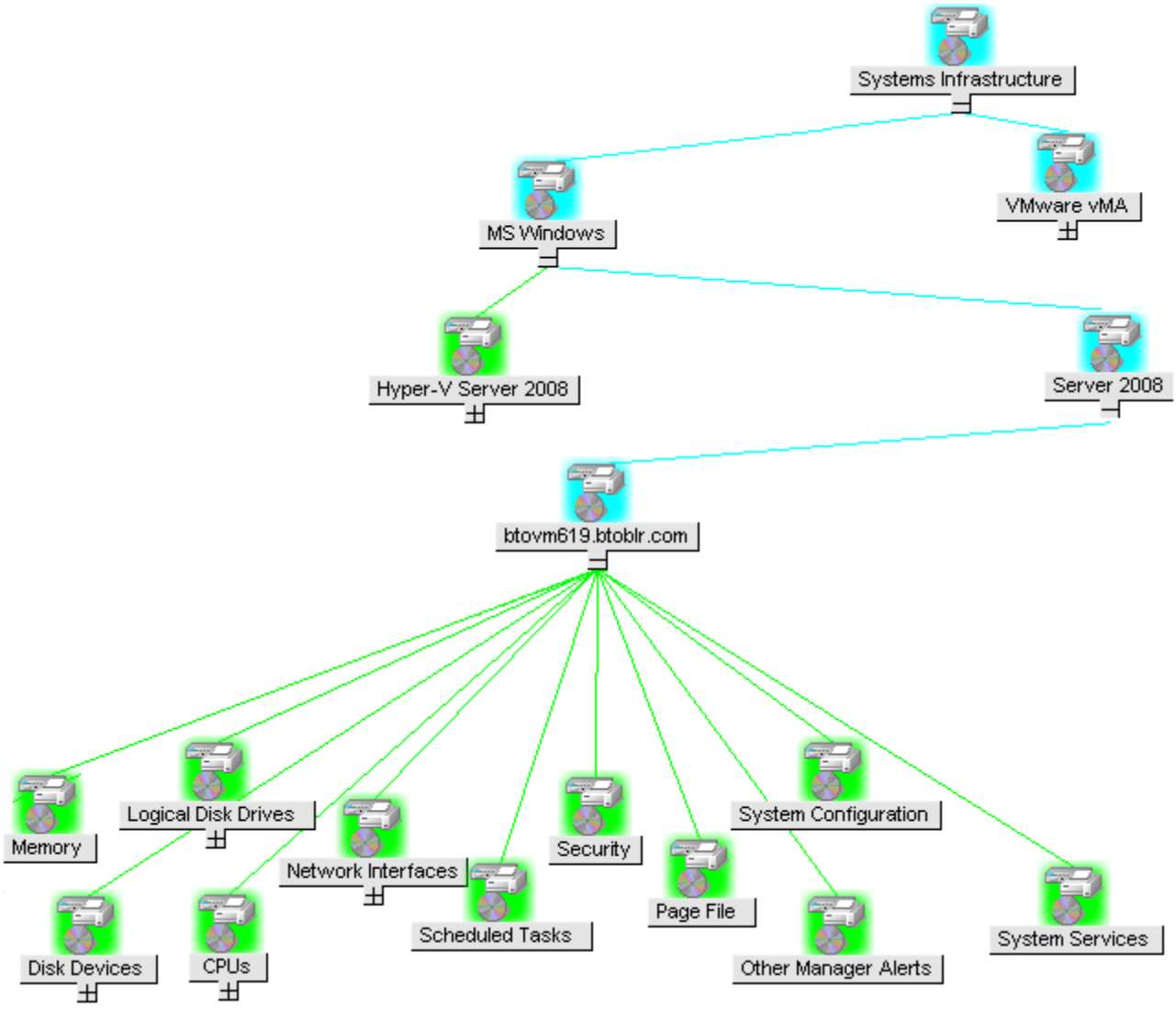
このインスタンスで、<オペレータ名 >は、サービスを割り当てるオペレータを指定します (例: opc_adm、opc_op)。

SI SPI service discovery ポリシーによってポリシーがノードに自動的に配布されることはありません。手動でポリシーを配布できます。

マップを表示するには、次のステップに従います。

1. HPOM の操作インターフェイスを起動します。
2. ユーザー名とパスワードを使用してログオンします。
3. **[サービス]** → **[Systems Infrastructure]** → **[グラフの表示]** を選択すると、マップ ビューが表示されます。

図 2: HPOM for UNIX/Linux/Solaris のマップ ビュー



マップ ビューには、インフラストラクチャ環境のサービスまたはノードの階層構造全体が、サブシステムやサブサービスを含め、グラフィカルに表示されます。

ツール

SI SPI ツールでは、特定の管理ノードに関して収集したデータが表示されます。SI SPI のツールの詳細は、「Systems Infrastructure SPI ツール」(141ページ)を参照してください。

ポリシー

HPOM for Windows では、インストール時に複数のデフォルト ポリシーが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。これらのポリシーをそのまま使用して、システム インフラストラ

クチャに関するデータや環境からのメッセージの受信を開始できます。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保存し、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。

管理サーバーからのポリシーの配布の詳細 は、「HPOM for Windows 管理サーバーからの SI SPI ポリシーの配布」(139ページ)を参照してください。

HPOM for HP-UX、Linux、または Solaris では、SI SPI service discovery ポリシーによってポリシーがノードに自動的に配布されることはありません。手動でポリシーを配布できます。

管理サーバーからのポリシーの配布の詳細 は、「HPOM for UNIX 管理サーバーからの SI SPI ポリシーの配布」(140ページ)を参照してください。

SI SPI のポリシーの名前は、わかりやすく、簡単に変更できるように、SI で始まっています。ポリシー タイプは以下のとおりです。

- **Service/Process Monitoring ポリシー**は、システム サービスおよびプロセスを監視する手段を提供します。
- **Logfile Entry ポリシー**は、システム ノードによって生成されたステータス メッセージおよびエラー メッセージをキャプチャします。
- **Measurement Threshold ポリシー**は、収集されたメトリック値を解釈し、警告またはメッセージをメッセージ ブラウザに表示できるように、各メトリックの条件を定義します。各 Measurement Threshold ポリシーは、実際のメトリック値と指定したしきい値または自動しきい値を比較して、実際のメトリック値がしきい値に反する場合、問題を解決するためのメッセージや指示文が表示されます。
- **Scheduled Task ポリシー**は、収集の対象となるメトリック値と、収集を開始する時間を定義します。収集間隔も定義します。収集間隔は、特定のグループに対するデータの収集頻度を示します。Scheduled Task ポリシーには 2 つの機能があります。ノードの収集間隔ごとにコレクタ/アナライザを実行する機能と、ポリシーの **[コマンド]** テキスト ボックス内に表示されているすべてのメトリックのデータを収集する機能です。
- **Service Discovery ポリシー**は、個々のシステム ノード インスタンスを検出し、SI SPI で検出されたすべてのインスタンスを含むマップ ビューを生成します。

SI SPI のポリシーの詳細は、「Systems Infrastructure SPI のポリシー」(22ページ)を参照してください。

グラフ

SI SPI では、監視対象の要素の正常域の動作に矛盾が生じた場合に原因を表示してトレースできます。HPOM は、HP Performance Manager と統合されています。これは、システム パフォーマンスの評価、使用率の傾向の把握、システム間でのパフォーマンス比較を行う Web ベース ツールです。HP Performance Manager では、以下の表示が可能です。

- グラフ (折れ線グラフ、棒グラフ、面グラフなど)
- データ表 (プロセス詳細など)
- ベースライン グラフ

- Java 形式の動的グラフ。個々のメトリックの表示をオフにしたり、グラフ上の点の値を表示したりすることができます

データをグラフィカルに表示することで、レポートされた重大または危険域のエラー メッセージをすばやく簡単に分析できます。SI SPI のグラフの詳細は、「Systems Infrastructure SPI のグラフ」(149ページ)を参照してください。

レポート

HP Reporter をインストールして SI SPI と統合することにより、メトリック データに基づいて Web ベースのレポートを生成できます。

HP Reporter を Windows 向けの HPOM 管理サーバーにインストールした場合、コンソールからレポートを表示できます。レポートを表示するには、コンソール ツリーで **[レポート]** を展開し、個別のレポートをダブルクリックします。

HP Reporter を HPOM 管理サーバー (Windows、UNIX、Linux、または Solaris オペレーティング システム向け) に接続されている別のシステムにインストールした場合、HP Reporter システムでレポートを表示できます。HP Reporter と HPOM を統合する方法の詳細は、『HP Reporter Installation and Special Configuration Guide』を参照してください。

SI SPI のレポートの詳細は、「Systems Infrastructure SPI のレポート」(147ページ)を参照してください。

第4章: 作業の開始

HPOM for Windows 管理サーバーまたは HPOM for UNIX 管理サーバーに Infrastructure SPIs をインストールした後で、インフラストラクチャの管理に必要な作業を実行する必要があります。

ポリシーの配布を開始する前に必要な作業の一覧は、配布チェックリストに記載されています。

配布チェックリスト

完了 (はい/いいえ)	タスク
	管理サーバーに HPOM 9.10 がインストールされていることを確認します。 Windows の場合: これに加えて、HP Operations Agent バージョン 11.00 以上がインストールされていることを確認します。 UNIX の場合 : これに加えて、HP Operations Agent バージョン 12.00 以上がインストールされていることを確認します。 HPOM および HP Operations Agent に対する入手可能なすべてのパッチとホットフィックスがインストールされていることを確認します。
	グラフとレポートを作成するために、Performance Manager と HP Reporter がインストールされていることを確認します。
	監視ポリシーの配布を開始する前に、HP Operations Agent がメトリックを収集できるように十分な時間を取ります。

HPOM for Windows の場合

HPOM for Windows を初めて使用するには、次の手順を実行します。

SI SPI の起動

HPOM for Windows 管理サーバーに SI SPI をインストールしたら、次の手順を実行します。

1. 監視するノードを追加します。ノードの追加時には、**[ポリシーとパッケージの自動配布]** オプションがデフォルトでオンになっています。

   このオプションは、管理ノード上の以下のポリシーの自動配布を有効にします。

- SI-SystemDiscovery
- InfraSPI-Messages
- OPC_OPCMON_OVERRIDE_THRESHOLD
- OPC_PERL_INCLUDE_INSTR_DIR
- AUTO_ADDITION_SETTINGS

既存のノード (Infrastructure SPIs のインストール前に追加された) の場合、または管理ノードの追加中に **[ポリシーとパッケージの自動配布]** チェック ボックスがオフにされた場合は、これらのポリシーを手動で配布します。

2. 管理ノード上でポリシーのアクセスと配布 (順序は任意) を行うには、以下のオプションを任意の順序で実行します。

- **[ポリシー管理]** → **[ポリシー グループ]** → **[Infrastructure Management]** → **[v12.0]** → **[<言語>]** → **[メッセージ]** を選択し、InfraSPI-Messages ポリシーを配布します。
- **[ポリシー管理]** → **[ポリシー グループ]** → **[Infrastructure Management]** → **[v12.0]** → **[<言語>]** → **[Systems Infrastructure]** → **[AutoDiscovery]** を選択し、SI-SystemDiscovery ポリシーを選択します。
- **[ポリシー管理]** → **[ポリシー グループ]** → **[Infrastructure Management]** → **[v12.0]** → **[Settings and Thresholds]** → **[Agent Settings]** を選択し、次のポリシーを配布します。
  - AUTO_ADDITION_SETTINGS
  - OPC_OPCMON_OVERRIDE_THRESHOLD
  - OPC_PERL_INCLUDE_INSTR_DIR

注:

- ゲスト仮想マシンを自動的に追加するには、AUTO_ADDITION_SETTINGS ポリシーの AutoAdd_Guests パラメータを True に設定します。このパラメータはデフォルトでは False に設定されています。
- ノードを Windows 管理サーバー間で移動する場合、必ず `infraspi.nodegrp` 名前空間の変数をクリーンアップしてください。これらの変数をクリーンアップしない場合、新しい Windows 管理サーバーで自動追加メッセージがトリガーされません。

Quick Start ポリシーの HPOM for Windows からの配布

SI SPI 検出が正常に完了すると、検出されたノードは各 Infrastructure SPI ノード グループに自動的に追加されます。

このノード グループには、デフォルトで QuickStart ポリシーが割り当てられます。ノードがノード グループに追加されると、この QuickStart ポリシーは自動的に管理ノードに配布されます (ポリシーの自動配布が有効になっている場合)。

インフラストラクチャが検出され、サービス マップが HPOM for Windows 管理サーバーに設定されると、QuickStart ポリシーが自動的に管理ノードに配布されます (ポリシーの自動配布が有効になっている場合)。QuickStart ポリシーは、3 つの Infrastructure SPIs すべてで使用可能で、設定のカスタマイズに時間をかけずにすぐに使用できます。ポリシーの自動配布は、デフォルトで有効になっています。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保存し、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。

高度なポリシーは、特定のシナリオで使用されます。これらのポリシーは、必要に応じて手動で配布できます。

ポリシーの自動配布をオフにした場合、Infrastructure SPIs によって提供される 2 つのポリシー グループのいずれかにアクセスすることで、QuickStart ポリシーを手動で配布できます。グループ化は、監視対象要素、およびベンダーとオペレーティング システムに基づいています。監視を目的としたグループでは、複数のオペレーティング システムを対象に、パフォーマンス、可用性、キャパシティ、ログ、セキュリティを監視するポリシーにアクセスおよび配布できます。たとえば、インフラストラクチャでスケジュールされたジョブ サービスの可用性を監視するには、以下の順に展開します。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Availability] → [Scheduled Job Service]

ベンダー別にグループ化されたポリシーでは、1 つの場所からご使用のオペレーティング システムに関連するポリシーにすぐにアクセスできます。たとえば、管理ノードに配布する SI-RHELCronProcessMonitor ポリシーにアクセスするには、以下の順に展開します。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Policies grouped by Vendor] → [RHEL - Advanced Policies] → SI-RHELCronProcessMonitor

HPOM for UNIX の場合

HPOM for UNIX (HP-UX、Linux、および Solaris) で Infrastructure SPIs を初めて使用するには、以下の手順を実行します。

開始する前に、最新のパッチとホットフィックスがインストールされていることを確認します。

パッチのリスト

HPOM for HP-UX	HPOM for Linux	HPOM for Solaris
PHSS_43465	OML_000057	ITOSOL_00789

SI SPI の起動

管理ノードを追加して SI SPI 検出ポリシーを配布するには、以下の手順を実行します。

1. 監視するノードを管理サーバーに追加します。これらのノードは登録ノードに表示されます。

   SI SPI は、SI-Deployment ノード グループを作成し、このノード グループに次のポリシーを自動的に割り当てます。
   - SI-SystemDiscovery
   - SI-ConfigureDiscovery
   - InfraSPI-Messages
   - OPC_OPCMON_OVERRIDE_THRESHOLD
   - OPC_PERL_INCLUDE_INSTR_DIR
   - AUTO_ADDITION_SETTINGS
2. 管理ノードを SI-Deployment ノード グループに追加します。
3. 割り当てられたポリシーと Infrastructure SPI インストルメンテーションを管理ノードに配布 (分配) します。

注: ゲスト仮想マシンを自動的に追加するには、AUTO_ADDITION_SETTINGS ポリシーの AutoAdd_Guests パラメータを True に設定します。このパラメータはデフォルトでは False に設定されています。

Quick Start ポリシーの HPOM for UNIX からの配布

SI SPI 検出が正常に完了すると、検出されたノードは各 Infrastructure SPI ノード グループに自動的に追加されます。

このノード グループには、デフォルトで QuickStart ポリシーが割り当てられます。ノードがノード グループに追加されると、この QuickStart ポリシーは自動的にノードに配布されます。次に、管理 GUI の **[アクション]** メニューから **[設定の配布]** を選択して、ポリシーをノードに手動で配布します。

QuickStart ポリシーは、3 つの Infrastructure SPIs すべてで使用可能で、設定のカスタマイズに時間をかけずにすぐに使用できます。ポリシーの自動割り当ては、デフォルトで有効になっています。

グループ化は、監視対象要素、およびオペレーティング システムまたはベンダーに基づいています。監視を目的としたグループでは、複数のオペレーティング システムを対象に、パフォーマンス、可用性、キャパシティ、ログ、セキュリティを監視するポリシーにアクセスおよび配布できます。たとえば、インフラストラクチャでスケジュールされたジョブ サービスの可用性を監視するには、以下の順に選択します。

[登録ポリシー] → [Infrastructure Management] → [v12.0] → [ja] → [Systems Infrastructure] → [Availability] → [Scheduled Job Service]

オペレーティング システムとベンダー別にグループ化されたポリシーでは、1 つの場所からご使用のオペレーティング システムに関連するポリシーにすぐにアクセスできます。たとえば、管理ノードに配布する SI-CPUSpikeCheck ポリシーにアクセスするには、以下の順に選択します。

[登録ポリシー] → [Infrastructure Management] → [v12.0] → [ja] → [Systems Infrastructure] → [Policies grouped by Vendor] → [RHEL - QuickStart Policies]

オペレーティング システム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の 2 つのサブグループがあります。QuickStart グループには、最もよく使用されるポリシーが含まれています。ディスク使用率ポリシーやディスク容量監視ポリシーなどの高度なポリシーは、特定のシナリオで使用されます。

レポートとグラフの表示

Infrastructure SPIs によって収集されたデータからレポートとグラフを作成して表示するには、HP Reporter と HP Performance Manager をそれぞれ HPOM と連動して使用する必要があります。Infrastructure SPIs は、レポート用とグラフ用のデータを収集してデータ ストア内に格納します。データ ストアとしては、CODA (HP Operations Agent のデータ ストアで、組み込みパフォーマンス コンポーネントとも呼ばれる) または HP Performance Agent を指定できます。

HPOM for HP-UX、HPOM for Linux、または HPOM for Solaris でグラフを表示するには、最初に HP Performance Manager を HPOM 管理サーバーに統合する必要があります。

HP Performance Manager と HPOM for UNIX との統合

HPOM for UNIX (HP-UX、Linux、または Solaris) サーバーを HP Performance Manager と統合するには、以下の手順を実行します。

- HP Performance Manager が HPOM サーバーにインストールされている場合、以下のコマンドを実行します。

  # /opt/OV/contrib/OpC/OVPM/install_OVPM.sh

  install_OVPM.sh <ノード名>:<ポート>

  例: install_OVPM.sh test.ovtest.com:8081

- HP Performance Manager が HPOM サーバーに接続しているリモート システムにインストールされている場合は、以下の手順を実行します。

  1. グラフ テンプレートを HP Performance Manager がインストールされているリモート システムから HPOM サーバーにコピーします。グラフのタイプとシステム上の場所を確認するには、『HP Performance Manager 管理者ガイド』を参照してください。
  2. HPOM サーバーで次のコマンドを実行してください。

     # /opt/OV/contrib/OpC/OVPM/install_OVPM.sh

install_OVPM.sh <ノード名>:<ポート>

例: install_OVPM.sh test.ovtest.com:8081

これらの手順によって、HPOM オペレータ GUI 内のイベントからグラフを起動する際に使用される HP Performance Manager のホスト システム設定が設定されます。

SPI のアップグレード後のレポートの更新

アップグレードの後、既存のレポート ファイルは新しいレポート ファイルと置き換えられます。レポートを更新するには、以下のコマンドを実行します。

1. **[スタート]** メニューに移動します。
2. **[ファイル名を指定して実行]** を選択します。
3. プロンプトで、コマンドとして「**repcrys**」と入力し、**[OK]** をクリックします。

管理サーバー上のすべてのレポートが HP Reporter GUI 上のレポートと同期していることを確認します。Reporter GUI の **[Reporter Status]** タブをクリックして、レポートがコンソールに送信した番号、およびエラー メッセージがあればそれもチェックします。

レポート用のデータ収集

SI SPI 用に提供されるレポートは、ポリシーに依存します。以下の表に、レポート、および対応するレポートのデータを収集するために管理ノードに配布する必要があるポリシーを示します。

レポート	ポリシー	管理ノードのプラットフォーム	SPI
Last Logins/ Unused Logins	SI-MSWindowsLastLogonsCollector	Windows	Systems Infrastructure
Last Logins/ Unused Logins	SI-LinuxLastLogonsCollector	Linux	Systems Infrastructure
Failed Login	SI-MSWindowsFailedLoginsCollector	Windows	Systems Infrastructure
Failed Login	SI-UNIXFailedLoginsCollector	Linux、HP-UX、AIX、Solaris	Systems Infrastructure

HPOM for Windows から Infrastructure SPI のレポートを表示するには、コンソール ツリーで **[レポート]** → **[Infrastructure Management]** → **[Systems Infrastructure]** を選択して展開します。レポートを表示するには、HPOM コンソールで必要なレポートを選択して右クリックし、続いて **[レポートの表示]** を選択します。

第5章: Systems Infrastructure SPI のポリシー

ポリシーは、監視を自動化するための 1 つまたは複数のルールです。SI SPI のポリシーを使用して、Windows、Linux、Solaris、AIX、HP-UX の各環境を監視できます。ほとんどのポリシーはすべての環境に共通ですが、特定の環境でのみ使用できたり、該当するプラットフォームでのみ配布する必要があるポリシーもあります。サポートされていないプラットフォームにポリシーを配布すると、予期しない動作が発生したり、ポリシーにエラーが発生したりすることがあります。

[Infrastructure Management group] フォルダには、言語で分類されたサブグループがあります。たとえば、英語のポリシーのサブグループは **[en]**、日本語のポリシーのサブグループは **[ja]**、簡体中国語のポリシーのグループは **[zh]** です。これらのポリシー サブグループに加えて、HPOM for UNIX 管理サーバー上には、韓国語 (**ko**) とスペイン語 (**es**) の 2 つのポリシー サブグループが追加されています。

HPOM for UNIX (HP-UX、Linux、または Solaris) では、ポリシー グループはコンソールまたは管理者用インターフェイスの以下の場所にあります。

[登録ポリシー] → [Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure]

管理サーバーからのポリシーの配布の詳細 は、「HPOM for UNIX 管理サーバーからの SI SPI ポリシーの配布」(140ページ)を参照してください。

HPOM for Windows でポリシーにアクセスするには、次を選択します。

[ポリシー管理] → ポリシー グループ] → [Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure]

管理サーバーからのポリシーの配布の詳細 は、「HPOM for Windows 管理サーバーからの SI SPI ポリシーの配布」(139ページ)を参照してください。

注: SI-LinuxSecureLog、**SI-LinuxBootLog**、**SI-LinuxKernelLog**、**SI-LinuxLastLogonsCollector** の各ポリシーは、非 root ユーザー モードで実行中の HP Operations Agent では機能しません。

トレース

キャパシティとパフォーマンスを監視するポリシーには、トレース用に Debug または DebugLevel スクリプト パラメータが含まれます。このパラメータを指定することで、トレースを有効にできます。次のいずれかの値を指定できます。

- Debug=0、トレース メッセージは送信されません。
- Debug=1、トレース メッセージがコンソールに送信されます。
- Debug=2、トレース メッセージが管理ノード上のトレース ファイルに記録されます。管理ノード上のトレース ファイルの場所は、`$OvDataDir/Log` です。

スクリプト パラメータを確認するには、以下の手順を実行します。

1. ルート ユーザーとしてログオンします。
2. 目的のポリシーをダブルクリックします。ポリシー ウィンドウが開きます。
3. [スクリプト パラメータ] タブを選択します。そのポリシーのスクリプト パラメータが一覧表示されます。

また、パラメータ値はユーザー要件に応じて変更できます。スクリプト パラメータの値を編集する方法の詳細は、『HP Operations Smart Plug-ins for Infrastructure コンセプト ガイド』を参照してください。

検出ポリシー

SI-SystemDiscovery ポリシーは、ハードウェア リソース、オペレーティング システム属性、アプリケーションなどのサービス情報を管理ノードから収集します。

HPOM コンソールのノード グループにノードを追加すると、SI-SystemDiscovery ポリシーと共に配布された検出モジュールがノード上でサービスの検出を実行します。このサービス検出モジュールは、収集した情報を XML スニペットの形式で HPOM に返します。このスニペットは、SI SPI 検出プロセスを実行する時点で、管理ノード上のサービスのスナップショットを取得し、これを示すサービス ツリーを作成します。Autodiscovery ポリシーは、配布後、定期的に実行されるように設定されます。検出エージェントは、収集したサービス情報と前回実行時の結果を比較します。前回実行時から、管理ノード上で実行中のサービスに変更や追加が見つかった場合、HPOM 管理サーバーにメッセージを送信し、管理サーバーがサービス ビューに変更内容を反映します。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [AutoDiscovery]

検出の制限

SI-ConfigureDiscovery ポリシーは、仮想マシン上の指定されたリソースの検出を対象にするか除外できる ConfigFile ポリシーです。

デフォルトでは、SI-SystemDiscovery ポリシーは、ノードで実行されているすべてのサービスとリソースを検出します。ただし、サービス マップ内のすべてのリソースを表示する必要がない場合があります。

検出を制限するには、検出ポリシーを実行する前に、SI-ConfigureDiscovery ポリシーを配布する必要があります。

SI-ConfigureDiscovery ポリシーには、Infrastructure SPI がサポートしているすべての仮想化テクノロジで、すべての仮想マシン上のリソースを対象にするか除外する構成スイッチがあります。

このポリシーをノードに配布すると、`SI-Discovery.cfg` 構成ファイルが次のフォルダに保存されます。

UNIX:`/var/opt/OV/conf/sispi/configuration`

Windows: `%Ovdatadir%\Data\conf\sispi\configuration`

注: SIDiscovery.cfg ファイルが /var/opt/OV/conf/sispi/configuration/ フォルダに存在しない場合、SI 検出はデフォルトですべてのリソースを検出します。

SIDiscovery.cfg ファイルには、次の情報が含まれています。

```
#To include or exclude a particular resource in SI discovery, add the particular
value under the respective Resource.

#The resources which can be restricted or expanded for being discovered are
mentioned below:

#

#File System

#Disk

#Network

#CPU

#

#The values which can be part of the INCLUDE and EXCLUDE parameters with respect to
each of the resources can be as follows:

#

#FS include or exclude parameters should contain File system path(In general FS_
DIRNAME value)

# Example:

# FS_INCLUDE: /etc* Or

# FS_EXCLUDE: /zones*

#

#DSK include or exclude parameters should contain name of the Disk device(In
general BYDSK_DEVNAME value)

# Example:

# DSK_INCLUDE: vdc0 Or

# DSK_EXCLUDE: vdc1

#

#NET include or exclude parameters should contain Network Interface name(In general
BYNETIF_NAME value)

# Example:

# NET_INCLUDE: lo0 Or

# NET_EXCLUDE: vnet0

#

#CPU include or exclude parameters should contain ID number of the CPU (In general
BYCPU_ID value)
```

```
# Example:

# CPU_INCLUDE: 0,1 Or

# CPU_EXCLUDE: 2,3

#

#Multiple entries should be separate with comma -

#For example if one wants to exclude 2 of the File Systems, then the following
entry should configured:

#FS_INCLUDE: /zones*,/etc*

#

#Resource Name and value should be separated with ":"-

#For example if one wants to add FS_EXCLUDE, then the following entry should be
configured separated with ":"

#FS_EXCLUDE: /zones*

##Different resources(_INCLUDE and _EXCLUDE) should be separated with "===".As in
the below case, FS, DSK, NET and CPU are

#separated with "==="
################################################################################
##############################################===

FS_INCLUDE:

FS_EXCLUDE: /zones*

===

DSK_INCLUDE:

DSK_EXCLUDE:

===

NET_INCLUDE:

NET_EXCLUDE:

===

CPU_INCLUDE:

CPU_EXCLUDE:
```

リソースを検出の対象にするか除外するには、ファイルに記載されている指示に従って SIDiscovery.cfg ファイルを編集します。

INCLUDE パラメータに特定のリソース名を入力した場合、SI 検出では、それらのリソースのみ検出されてサービス マップに表示されます。EXCLUDE パラメータに特定のリソース名を入力した場合、SI 検出では、それらのリソースは検出されず、サービス マップに表示されません。

リソース名全体を指定するか、ワイルドカード (*) を使用できます。

設定できるパラメータは 1 つのみで、EXCLUDE または INCLUDE のいずれかです。両方のパラメータに値を設定した場合や、いずれのパラメータにも値を設定しない場合は、SI 検出ポリシーでは、デフォルトですべてのリソースが検出されます。

注: INCLUDE パラメータに誤ったインスタンス値を設定すると、SI 検出では、その特定のリソース インスタンスが検出されず、重要度が注意域の次のアラート メッセージが HPOM コンソールに送信されます。
`Improper usage as _INLUCDE parameter is not having the correct value.`

ただし、EXCLUDE パラメータに誤ったインスタンス値を設定した場合は、SI 検出によってそのリソース インスタンスが検出されます。

SI-SystemDiscovery ポリシーは、`SIDiscovery.cfg` ファイルを開くか読み取れない場合、重要度が注意域の次のアラート メッセージを HPOM コンソールに送信します。
`Improper usage as both _INCLUDE and _EXCLUDE are configured.`

例

email server、webserver1、webserver2 という名前の 3 つの非グローバル ゾーンを持つ Oracle Solaris コンテナー上には、次のような複数のファイル システムがある可能性があります。

```
/etc/svc/volatile
/tmp
/var/run
/zones/emailserver/root/etc/svc/volatile
/zones/emailserver/root/tmp
/zones/emailserver/root/var/run
/zones/webserver1/root/etc/svc/volatile
/zones/webserver1/root/tmp
/zones/webserver1/root/var/run
/zones/webserver2/root/etc/svc/volatile
/zones/webserver2/root/tmp
/zones/webserver2/root/var/run
```

- 特定のファイル システムのみ検出する場合、INCLUDE パラメータに次のいずれかの値を入力して、`SIDiscovery.cfg` ファイルを変更します。
  - `FS_INCLUDE:/zones/webserver2*`
  - `FS_INCLUDE:/zones/webserver2/root/etc/svc/volatile`
- 特定のファイル システムを検出しない場合、EXCLUDE パラメータに次のいずれかの値を入力して、`SIDiscovery.cfg` ファイルを変更します。
  - `FS_EXCLUDE:/zones/emailserver*`
  - `FS_EXCLUDE:/zones/emailserverroot/tmp`

プロセスとサービスを監視するポリシー

これらのポリシーのデフォルトのポリシー グループは以下のとおりです。

- **[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Availability] → [<プロセス/サービス>] → <os>**
- **[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Policies grouped by vendor] → [<os> - Advanced]**

このインスタンスでは、**<os>** は管理ノードのオペレーティング システムです。サポートされているオペレーティング システムは、AIX、Debian、HP-UX、RHEL、SLES、Solaris、Ubuntu、および Windows です。次の表では、プロセスとサービス、各プラットフォームでサポートされる監視ポリシーをまとめます。

Infrastructure SPIs では、Solaris ゾーンでプロセスを監視する可用性ポリシーが用意されています。Solaris マシンには、グローバル ゾーンとローカル ゾーン (コンテナー) があります。可用性ポリシーは、Solaris プロセスの可用性を監視し、使用不能状態を検出すると、HPOM に警告メッセージを送信します。

表 1: AIX 用の監視ポリシー

プロセス/サービス名	監視ポリシー
DHCP Server	SI-AIXDHCPProcessMonitor
DNS Server	SI-AIXNamedProcessMonitor
Email Service	SI-AIXSendmailProcessMonitor
Fax Service	-
File Services	SI-AIXNfsServerProcessMonitor
Firewall Service	-
Internet Service	SI-AIXInetdProcessMonitor
Network Services	-
Print Service	• SI-AIXQdaemonProcessMonitor • SI-AIXLpdProcessMonitor
RPC Service	SI-AIXPortmapProcessMonitor
Scheduled Job Service	SI-AIXCronProcessMonitor
Secure Login Service	SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-UnixSnmpdProcessMonitor

プロセス/サービス名	監視ポリシー
System Logger	SI-AIXSyslogProcessMonitor
Terminal Services	-
Web Server	SI-AIXWebserverProcessMonitor

表 2: Debian 用の監視ポリシー

プロセス/サービス名	監視ポリシー
Apache	SI-DebianApacheProcessMonitor
Cron	SI-DebianCronProcessMonitor
Exim (メール転送エージェント)	SI-DebianEximProcessMonitor
Inetd	SI-DebianInetdProcessMonitor
Named	SI-DebianNamedProcessMonitor
Nfs Server	SI-DebianNfsServerProcessMonitor
Nmbd	SI-DebianNmbdProcessMonitor
Samba	SI-DebianSambaProcessMonitor
Sshd	SI-DebianSshdProcessMonitor

表 3: HP-UX 用の監視ポリシー

プロセス/サービス名	監視ポリシー
DHCP Server	SI-HPUXBootpdProcessMonitor
DNS Server	SI-HPUXNamedProcessMonitor
Email Service	SI-HPUXSendmailProcessMonitor
Fax Service	-
File Services	SI-HPUXNfsServerProcessMonitor
Firewall Service	-
Internet Service	SI-HPUXInetdProcessMonitor
Network Services	-
Print Service	SI-HPUXLpschedProcessMonitor

プロセス/サービス名	監視ポリシー
RPC Service	-
Scheduled Job Service	SI-HPUXCronProcessMonitor
Secure Login Service	• SI-HPUXSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-UnixSnmpdProcessMonitor
System Logger	SI-HPUXSyslogProcessMonitor
Terminal Services	-
Web Server	SI-HPUXWebserverProcessMonitor

表 4: RHEL 用の監視ポリシー

プロセス/サービス名	監視ポリシー
DHCP Server	SI-LinuxDHCPProcessMonitor
DNS Server	SI-LinuxNamedProcessMonitor
Email Service	SI-LinuxSendmailProcessMonitor
Fax Service	-
File Services	• SI-LinuxNfsServerProcessMonitor • SI-LinuxSmbServerProcessMonitor
Firewall Service	-
Internet Service	SI-LinuxXinetdProcessMonitor
Network Services	-
Print Service	SI-LinuxCupsProcessMonitor
RPC Service	-
Scheduled Job Service	SI-RHELCronProcessMonitor
Secure Login Service	• SI-LinuxSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-UnixSnmpdProcessMonitor
System Logger	SI-RHELSyslogProcessMonitor

プロセス/サービス名	監視ポリシー
Terminal Services	-
Web Server	SI-LinuxWebserverProcessMonitor

表 5: SLES 用の監視ポリシー

プロセス/サービス名	監視ポリシー
DHCP Server	SI-LinuxDHCPProcessMonitor
DNS Server	SI-LinuxNamedProcessMonitor
Email Service	SI-LinuxSendmailProcessMonitor
Fax Service	-
File Services	• SI-LinuxNfsServerProcessMonitor • SI-LinuxSmbServerProcessMonitor
Firewall Service	-
Internet Service	SI-LinuxXinetdProcessMonitor
Network Services	-
Print Service	SI-LinuxCupsProcessMonitor
RPC Service	-
Scheduled Job Service	SI-SLESCronProcessMonitor
Secure Login Service	• SI-LinuxSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-UnixSnmpdProcessMonitor
System Logger	SI-SLESSyslogProcessMonitor
Terminal Services	-
Web Server	SI-LinuxWebserverProcessMonitor

表 6: Solaris 用の監視ポリシー

プロセス/サービス名	監視ポリシー
DHCP Server	SI-SunSolarisDHCPProcessMonitor
DNS Server	SI-SunSolarisNamedProcessMonitor

プロセス/サービス名	監視ポリシー
Email Service	SI-SunSolarisSendmailProcessMonitor
Fax Service	-
File Services	SI-SunSolarisNfsServerProcessMonitor
Firewall Service	-
Internet Service	SI-SunSolarisInetdProcessMonitor
Network Services	-
Print Service	SI-SunSolarisLpdProcessMonitor
RPC Service	-
Scheduled Job Service	SI-SunSolarisCronProcessMonitor
Secure Login Service	• SI-SunSolarisSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-UnixSnmpdProcessMonitor
System Logger	SI-SunSolarisSyslogProcessMonitor
Terminal Services	-
Web Server	SI-SunSolarisWebserverProcessMonitor

表 7: Ubuntu 用の監視ポリシー

プロセス/サービス名	監視ポリシー
Atd	SI-UbuntuAtdProcessMonitor
Cron	SI-UbuntuCronProcessMonitor
Inetd	SI-UbuntuInetdProcessMonitor
Nmb Server	SI-UbuntuNmbServerProcessMonitor
Smb Server	SI-UbuntuSmbServerProcessMonitor
Sshd	SI-UbuntuSshdProcessMonitor
Udev	SI-UbuntuUdevProcessMonitor

表 8: Windows 用の監視ポリシー

プロセス/サービス名	監視ポリシー
DHCP Server	SI-MSWindowsDHCPServerRoleMonitor
DNS Server	SI-MSWindowsDNSServerRoleMonitor
Email Service	-
Fax Service	SI-MSWindowsFaxServerRoleMonitor
File Services	• SI-MSWindowsWin2k3FileServicesRoleMonitor • SI-MSWindowsDFSRoleMonitor • SI-MSWindowsFileServerRoleMonitor • SI-MSWindowsNFSRoleMonitor
Firewall Service	SI-MSWindowsFirewallRoleMonitor
Internet Service	-
Network Services	• SI-MSWindowsRRAServicesRoleMonitor • SI-MSWindowsNetworkPolicyServerRoleMonitor
Print Service	SI-MSWindowsPrintServiceRoleMonitor
RPC Service	SI-MSWindowsRpcRoleMonitor
Scheduled Job Service	SI-MSWindowsTaskSchedulerRoleMonitor
Secure Login Service	SI-OpenSshdProcessMonitor[1]
SNMP Service	SI-MSWindowsSnmpProcessMonitor
System Logger	SI-MSWindowsEventLogRoleMonitor
Terminal Services	• SI-MSWindowsTSWebAccessRoleMonitor • SI-MSWindowsTSGatewayRoleMonitor • SI-MSWindowsTerminalServerRoleMonitor • SI-MSWindowsTSLicensingRoleMonitor
Web Server	SI-MSWindowsWebServerRoleMonitor

[1] このポリシーは、AIX、HP-UX、Linux、MS Windows、Solaris の各オペレーティング システムでサポートされます。いずれのプラットフォームでも、このポリシーを配布する場合は、事前に openssh パッケージをインストールしてください。

注: 最新の Solaris 用プロセス監視ポリシーをグローバル ゾーンに配布した場合、SI SPI では、プロセスが属しているゾーンを区別せずに、グローバル ゾーンと非グローバル ゾーンで実行中の

すべてのプロセスを監視します。したがって、グローバル ゾーンで実行されるプロセスを監視する場合、非グローバルのプロセスを含めるようにしきい値レベルを設定する必要があります。

例: グローバル ゾーンの一部となっている非グローバル ゾーンが「x」個ある場合、しきい値レベルは、グローバル ゾーンと非グローバル ゾーンのすべてのプロセスを含めるように、つまり、x+1 に設定する必要があります。

グローバル ゾーンとグローバル ゾーンの一部となっている非グローバル ゾーンに同じポリシーを配布すると、重複したアラートが送信されます。

非グローバル ゾーンでサポートされないポリシー

- SI-CPUSpikeCheck

可用性ポリシー

可用性監視は、リソースの可用性を適切に確保するのに役立ちます。リソースの可用性について、許容できないレベルを特定することが重要です。IT インフラストラクチャの現在の負荷を計算し、しきい値と比較することによって、リソースの可用性に不足部分がないかチェックします。

IT リソースの使用方法が変わり、機能が進化するにつれ、ディスク容量、処理能力、メモリ、その他のパラメータも変わります。現在のニーズと、時間の経過に伴ってニーズがどのように変化するかを把握することが重要です。一定の期間にわたってこれらの要素を監視することは、IT リソースの使用率に対する影響を理解する上で役に立ちます。

サーバーの役割では、Fax サーバーや電子メール サーバーなどの主要機能を記述します。1 つのシステムに、サーバーの役割を 1 つまたは複数インストールすることができます。各サーバーの役割には、その役割の子要素として、1 つまたは複数のサービスを指定できます。可用性ポリシーは、管理ノード上にある役割サービスの可用性を監視します。

これらのポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Availability]

可用性ポリシーは、Linux、Windows、Solaris、AIX、HP-UX の各管理ノード上で、プロセスやサービスの可用性を監視します。プロセスが使用不能状態に陥るか、サービスのステータスが変化すると (停止または無効になる)、ポリシーは HPOM にメッセージを送信します。ポリシーでは、監視対象となるステータスと、ステータスが変化した時点で実行するアクションを定義できます。

可用性ポリシーは、サーバー役割ごとにグループに分類し、さらにオペレーティング システムごとにサブ グループに分類することができます。また、管理ノード上で稼働するオペレーティング システムに基づいて、必要なポリシーを選択できます。

SI-ProcessMonitor

SI-ProcessMonitor ポリシーは、プロセス グループ内の一連のプロセスを監視します。SI-SPI で監視するすべてのプロセスとプロセス グループは、設定ファイル `procmon.cfg` で定義する必要がありま

す。設定ファイルで定義されたプロセスが実行を停止するか、期待どおりに動作しない場合、常にアラートが生成されます。

注: この設定ファイルは、procmon_local.cfg ファイルを使用して上書きまたは変更できます。TAB をprocmon_local.cfg ファイルの区切りとして使用します。

リソース グループに関連付けられているプロセス グループは、対応するリソース グループがオンラインの場合にのみ、監視対象になります。

SI-ProcessMonitor ポリシーは、30 秒間で 100 個のプロセスのみ監視できます。

ポリシー アラートに表示される山括弧 (><) は無視してください。

SI-ProcessMonitorConfig ファイル ポリシー:

SI-ProcessMonitorConfig ファイル ポリシーは、SI-ProcessMonitor 用に作成された設定ファイル ポリシーです。設定ファイル ポリシーでは、以下を指定する必要があります。

- 監視するプロセス ファイル。
- procmon.cfg ファイルの場所。ConfigFileLocation パラメータに、必ず procmon.cfg ファイルの場所を指定してください。

SI-ProcessMonitorConfig ポリシーの配布後に、以下の処理が行われます。

- procmon.cfg ファイルが存在しない場合、SI-ProcessMonitorConfig ファイル ポリシーで指定された場所に作成されます。
- procmon.cfg ファイルが存在する場合、SI-ProcessMonitorConfig ファイル ポリシーによって上書きされます。

SI-ProcessMonitor ポリシーは、以下を監視および表示します。

- 設定済みの制限を超えるプロセス。
- 機能を停止するプロセス。
- 指定された時間帯および曜日に制限を超えるプロセス。

サポートされているプラットフォーム	Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM-AIX Oracle Solaris Debian Ubuntu
スクリプト パラメータ	**説明**
ProcMonGroupName	設定ファイル内のプロセス グループを監視するには、ProcMonGroupName パラメータを使用します。

ConfigFilePath	procmon.cfg ファイルのパスを設定します。
LocalConfigFilePath	procmon_local.cfg ファイルのパスを設定します。
UseRepeatAlerts	ポーリング間隔ごとにアラートの繰り返しを受信するには、このパラメータを 1 に設定し、アラートの繰り返しを無効にするには、0 に設定します。
Debug	値を次のように設定します。 • 0: トレース メッセージを無効にします。 • 1: トレース メッセージを HPOM コンソールで受信します。 • 2: 管理ノード上のトレース ファイルにメッセージを記録します。 詳細については、「トレース」(22ページ)を参照してください。

設定ファイルの構文

プロセスは、次の図に示すようにプロセス グループにグループ化されます。

```
[OM_MGMT]
/opt/OV/bin/ovbbccb      -nodaemon        5-23    0,1,2,3,4,5,6    1-
/opt/OV/bin/ovcd         *        5-23    0,1,2,3,4,5,6    1-
/opt/OV/lbin/conf/ovconfd        *        5-23    0,1,2,3,4,5,6    1-
/opt/OV/lbin/sec/ovcs    *        5-23    0,1,2,3,4,5,6    1-
/opt/OV/bin/OpC/ovoareqsdr       -start   5-23    0,1,2,3,4,5,6    1-
/opt/OV/nonOV/jre/b/bin/java     -Dctlname=ovtomcatB -Dsun.lang.ClassLoader.allowAr
@severity=minor
```

スクリーンショットにマークされているインスタンスの場合、次のようになります。

プロセス グループ名	OM_MGMT
プロセス名	/opt/OV/bin/ovbbccb
引数	-nodaemon
時間帯	5-23
曜日	0,1,2,3,4,5,6
範囲	1-

注: プロセス グループの名前は、角括弧で囲む必要があります。

注:引数の一部を指定しても、プロセスは識別されます。

次の表に、設定ファイル内のプロセスおよびプロセス グループを定義するために使用される構文を示します。

カラム 1	カラム 2	カラム 3	カラム 4	カラム 5
名前	引数	範囲		
名前 @start=<cmd> @severity=<severity>	引数	範囲		
名前	引数	時間帯	曜日	範囲
名前 @start=<cmd> @severity=<severity>	引数	時間帯	曜日	範囲

このインスタンスの場合:

名前: 監視対象のプロセスの名前を指定します。

引数: 同時に実行している複数プロセスの区別に使用する、引数を指定します。引数が存在しない場合は、アスタリスク (*) を指定する必要があります。

時間帯: プロセスの失敗を報告する必要がある時間の長さ (24 時間形式) を指定します。

曜日: プロセスの失敗を報告する曜日を指定します。各曜日は、表にリストされている数値で識別されます。

数値	曜日
0	日曜日
1	月曜日
2	火曜日
3	水曜日
4	木曜日
5	金曜日
6	土曜日

注:数値はコンマで分けられていなければなりません。

範囲名前付きプロセスのインスタンス数を指定します。インスタンスの数は、次のように指定できます。

n	正確な数値

n-	最小 n
-n	最大 n
m-n	m ~ n の範囲

@Severity: 警戒域、重要警戒域、危険域などのアラート メッセージの重要度を指定します。デフォルトの重要度は注意域です。

@Start: プロセスの失敗時に実行する必要があるコマンド (<cmd>) を指定します。

SI-ZombieProcessCountMonitor

SI-ZombieProcessCountMonitor ポリシー (測定しきい値) は、ゾンビ プロセスの数を監視し、しきい値違反があった場合に、常にアラート メッセージを HPOM コンソールに送信します。

使用するメトリック	GBL_ZOMBIE_PROC
サポートされているプラットフォーム	Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM AIX Oracle Solaris Debian Ubuntu
スクリプト パラメータ	**説明**
ZombieProcessCountCriticalThreshold	ゾンビ プロセスの最小数でしきい値を設定します。この値に達すると、危険域のメッセージが受信されます。
ZombieProcessCountMajorThreshold	ゾンビ プロセスの最小数でしきい値を設定します。この値に達すると、重要警戒域のメッセージが受信されます。
ZombieProcessCountMinorThreshold	ゾンビ プロセスの最小数でしきい値を設定します。この値に達すると、警戒域のメッセージが受信されます。
ZombieProcessCountWarningThreshold	ゾンビ プロセスの最小数でしきい値を設定します。この値に達すると、注意域のメッセージが受信されます。

ShowDefunctProcessList	• デフォルトでは、この値は **False** に設定されています。 • 10 個のゾンビ プロセスおよびそのプロセス ID (PID) のリストを表示するには、値を **True** に設定します。
Debug	値を次のように設定します。 • 0: トレース メッセージを無効にします。 • 1: トレース メッセージを HPOM コンソールで受信します。 • 2: 管理ノード上のトレース ファイルにメッセージを記録します。 詳細については、「トレース」(22ページ)を参照してください。

設定変更ポリシー

設定変更ポリシーは、ファイル、Windows レジストリ設定、およびコマンド出力の変更状況を監視します。

SI-ChangeConfigurationMonitor

CCI Monitor (Change CI Monitoring または CCIMon) ポリシーは、設定ファイル `ccilist.cfg` にリストされている、ファイル、Windows レジストリ設定、およびコマンド出力の変更状況を監視します。これは、各実行ごとに `ccilist.cfg` ファイルを読み取り、ファイル、Windows レジストリ設定、およびコマンド出力に変更があれば、アラートを送信します。

監視の変更を開始するには、以下の手順を実行します。

1. 以下を配布します。

   SI-ChangeConfigurationMonitor - Windows および Linux の測定しきい値ポリシー

Windows の場合	SI-MSWindowsCCIConfig – Windows の設定ファイル ポリシー
Linux の場合	SI-LinuxCCIConfig – Linux および UNIX の設定ファイル ポリシー
AIX の場合	SI-AIXCCIConfig – AIX の設定ファイル ポリシー
Solaris の場合	SI-SunSolarisCCIConfig – Solaris の設定ファイル ポリシー
HP-UX の場合	SI-HPUXCCIConfig – HP-UX の設定ファイル ポリシー

2. `ccilist.cfg` ファイルが、`<OvDataDir>/ccimon/configuration` フォルダに作成されます。

> **注:** ccilist.cfg ファイルは、システム上の変更を監視するための設定ファイルです。このファイルは、任意のエディタで変更できます。詳細については、「監視用の ccilist.cfg ファイルの使用」(39ページ)を参照してください。
>
> 監視対象の変更を修正するには、ccilist.cfg ファイルまたは設定ファイル ポリシーに変更を追加し、ポリシーを再配布します。

3. CCI モニタ ポリシーは、各実行ごとに ccilist.cfg ファイルを読み取り、設定ファイル ccilist.cfg にリストされているファイル、Windows レジストリ設定、およびコマンド出力に変更があれば、アラートを送信します。

> **注: [メッセージのプロパティ]** ウィンドウの **[一般]** タブの **[アプリケーション]** ボックスに表示される、不明なアラートの重複したメッセージは無視してください。

監視用の ccilist.cfg ファイルの使用

<OvDataDir>/ccimon/configuration フォルダにある ccilist.cfg ファイルは、システム上の変更を監視するための設定ファイルです。CCI モニタ ポリシーは、各実行ごとにこのファイルを読み取ります。このポリシーは、システム上の以下の変更を監視します。

- インストール、削除、または変更されたソフトウェア
- インストールされたパッチ/サービス パック/更新プログラム
- カーネル パラメータに対する変更
- ブート設定
- レジストリ キー
- カーネル画像ファイル
- すべてのユーザー アカウント
- システム サービスの設定
- 追加、変更、または削除された共有ディレクトリ、NFS または CIFS (samba) のマウント
- システム環境変数

構文

次の構文を使用して、監視するすべての変更を追加します。

```
<change ci key,cci type,msg group,backup filename,alert severity[,unicode]>
```

このインスタンスの場合:

- <change ci key> - レジストリ キー、コマンド、または完全なパスを持つファイル名を指定します。
- <cci type> - これは次の値 - cmd、regkey、または change ci key に基づくファイルに設定します。

> **注:** レジストリ キー (regkey) のタイプは、Windows 管理ノードでのみ利用可能です。

- <msg group> - 変更アラートの HPOM メッセージ グループ設定を指定します。

  注: デフォルトのメッセージ グループは、Misc です。

- <backup filename> - これは、バックアップ フォルダでのバックアップ ファイルの作成に使用される名前です。作成されるバックアップ ファイルは、親ファイルとの比較に使用されます (CCI タイプ 'file' の監視には空の値を指定)。

  注: バックアップ フォルダは、<OvDataDir>/tmp ファイル内にあります。

- <alert severity> - HPOM 警告重要度設定を指定します。

  注: デフォルトの警告重要度は、注意域です。

- <[unicode]> - これはオプションの設定です。コマンド出力が Unicode 形式のコマンド出力を監視するために設定します (Windows にのみ必要)。

CCI モニタ ポリシーの使用例:

1. Windows 上の hosts ファイルを監視し、misc メッセージ グループ付きの注意域のアラートを送信するには、次のコマンドを実行します。

   ```
   c:\Windows\System32\drivers\etc\hosts,file,misc,,warning
   ```

   注: ファイル監視用のバックアップ ファイル名の指定は重要でないため、フィールドは空白のままにしています。

2. Windows 上の sys-temp フォルダの変更を監視するには、コマンド タイプとして変更の追跡を使用します。次のコマンドを実行します。

   ```
   dir "%temp%"| findstr /V bytes,cmd,OS,dirtmpbin,warning
   ```

   注:

   コマンドを実行すると、sys-temp フォルダで変更箇所が検索されます。dir コマンド出力の最後の数行を削除するには、findstr コマンドが使用されます。dir コマンド出力は頻繁に変更されるため、誤ったアラートが大量に生成されます。

   %TEMP% などの Windows 環境変数を使用できます。変数の値は、管理者ユーザーまたはドメイン ユーザーではない可能性がある、HP Operations Agent ユーザーによって計算されます。たとえば、HP Operations Agent がローカル システム管理者のユーザー資格情報で実行されている場合、%TEMP% は C:\Windows\Temp として評価される可能性があります。

3. Windows 上でレジストリ キーとその値を監視するには、次のコマンドを実行します。

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\CCIMon,regkey,misc,temp,warning
   ```

4. Windows 上で、opcmona.exe プロセスがノード上で実行中であるかどうか、およびそれが最後に実行したものと異なるかどうかを監視するには、次のコマンドを実行します。

   ```
   wmic process where name='opcmona.exe' get processid,cmd,OS,notepad-
   proc,major,unicode
   ```

注: また、このコマンドを使用して、システム上で実行されている権限がないソフトウェアをチェックすることもできます。

wmic コマンド出力は Unicode 形式であるため、最後のカラムに `unicode` 指定があります。

5. Linux 上の `/tmp` フォルダに新しいファイルまたはその他の変更があるかどうかを監視するには、次のコマンドを実行します。

   ```
   ls -1 /tmp | sort -u,cmd,Misc,ls1tmp.txt,warning
   ```

6. UNIX/Linux 上でユーザー変更があるかどうかを監視するには、次のコマンドを実行します。

   ```
   /etc/passwd,file,Security,,warning
   ```

7. UNIX/Linux 上にマウントされている新しいファイルシステムを確認するには、次のコマンドを実行します。

   ```
   /etc/mtab,file,OS,,minor
   ```

CCI モニタ ポリシーの削除

以下の手順を実行します。

1. すべてのノードからポリシーの配布を取り消します。
2. `<OvDataDir>/tmp/` フォルダから次の名前を持つすべてのファイルをクリーンアップします。`*.backup` および `*.current`。

警告および制限事項

- CCI モニタ ポリシーは、処理実行中の失敗を理解しやすくするために、ログ エントリを書き込みます。これらのログは、`<OvLogDir>` フォルダに `CCI Monitor-mm-dd-logfile.log` という名前で作成されます。これらのファイルは、デフォルトのロギングで約 2 MB の領域を占有し、新しいファイルが毎日作成されます。これらのファイルは、ロールオーバー スクリプトを使用すると削除できます。
- 1 つのノードには、CCI モニタ ポリシーの 1 つのコピーのみ配布するようにしてください。実運用用途の場合、CCI 設定ファイルと共にオリジナル ポリシーのみ使用するだけで十分です。バックアップ ルーチンはスレッドセーフではなく、ファイルの同時実行問題のため、監視が無期限にハングする可能性があります。
- 監視のデフォルトの頻度は、1 分です。20 を超える変更 CI を監視しようとすると、ソリューションのパフォーマンスが低下する可能性があります。このため、要素の数が 20 変更 CI を超える場合、少なくとも 5 分の間隔を設定することを推奨します。

必要な状態監視

必要な状態監視は、ファイル、Windows レジストリ設定、およびコマンド出力を監視します。

配布後に、必要な状態監視は、設定ファイル **ccilist.cfg** 内の == をチェックします。設定ファイルに追加されたファイル、Windows レジストリ設定、およびコマンド出力を、対応する gold ファイルと比較します。

注: gold ファイルとは、変更されることがないバックアップ ファイルまたは参照ファイルです。

設定ファイル **ccilist.cfg** に記載されている監視対象のファイル、Windows レジストリ設定、およびコマンド出力で変更があれば、必ずアラートが生成されます。

必要な状態監視の機能は、SI-ChangeConfigurationMonitor (CCIMon) ポリシーのものと同じです。唯一の相違は、CCIMon ポリシーの場合、毎回実行後にバックアップ ファイルが現在のファイル (**ccilist.cfg**) によって上書きされますが、必要な状態監視の場合、gold ファイル (バックアップ ファイルまたは参照ファイル) は不変のままということです。

注: gold ファイルの作成後にのみ、必要な状態監視を有効にするようにしてください。

例:

/etc ディレクトリにある **mtab** ファイルを監視するとします。このファイルをバックアップし、**mtab.gold** として **/etc** ディレクトリに保存します。これは、変更されない参照ファイルまたは gold ファイルです。**mtab** ファイルを監視するには、以下を設定ファイルに追加します。

```
/etc/mtab==/etc/mtab.gold,file,Os,,major
```

必要な状態監視が、設定ファイル **ccilist.cfg** を読み取り、**mtab** ファイルを **mtab.gold** ファイルと比較します。**mtab** ファイルを **mtab.gold** ファイルと比較して変更があれば、常にアラートが生成されます。

必要な状態監視の次の例で使用されている構文:

1. Windows 上の hosts ファイルを監視し、その他のメッセージ グループに注意域のアラートを送信するには、次のコマンドを実行します。

   構文: `filename==reference file name,ccitype,msg group,[backup filename],alert severity,charset`

   例: `/etc/mtab==/etc/mtab.gold,file,misc,,warning`

2. Windows 上のフォルダの変更を監視するには、変更の追跡用にコマンド タイプ cmd を使用します。次のコマンドを実行します。

   構文: `command==Path of the file containing command output,ccitype,msg group,[backup filename],severity`

   例: `ls /==/root/list.txt,cmd,Misc,,major`

   注:

   `ls /` コマンドを実行すると、結果の出力が `list.txt` ファイルの内容と比較されます。何らかの変更があれば、アラートがユーザーに送信されます。

3. Windows 上でレジストリ キーとその値を監視するには、次のコマンドを実行します。

   構文: `Registry key=='value of registry key',ccitype,msg group,[backup filename],severity`

   例: `HKEY_LOCAL_MACHINE\SOFTWARE\config==config,regkey,misc,,warning`

ハードウェア監視ポリシー

Systems Infrastructure SPI 12.00 には、HP ProLiant サーバーの正常性とステータスを監視できるポリシーが用意されています。これらのポリシーは、SIM エージェントによって生成される SNMP トラップを監視し、HPOM コンソールにアラート メッセージを送信します。これらのポリシーのタイプは、すべて SNMP Interceptor です。

これらのポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Hardware] → [HP ProLiant]

必要な設定:

- SNMP サービスが実行中であることを確認します。
- ハードウェア監視を有効にするには、ノードの **xpl config** ファイルを開き、**eaagt** ネームスペースの下に次の行を追加します。
  - HP Operations Agent 8.60 を使用している場合、次の行を追加します。
    ```
    [eaagt]
    SNMP_SESSION_MODE=NO_TRAPD
    ```
  - HP Operations Agent 12.00 を使用している場合、次の行を追加します。
    ```
    [eaagt]
    SNMP_SESSION_MODE=NETSNMP
    ```
- SIM Agent がインストールされている Linux ノードで、**/etc/snmp/snmpd.conf** に格納されている SNMP 設定ファイルを開き、末尾に次の行を追加します。
  `trapsink` <ノードのホスト名>
- Windows ノードで、次の SIM Agent がインストールされていることを確認します。
  - Foundation Agent
  - NIC Agent
  - Server Agent
  - Storage Agent

  インストールされていない場合は、HP Insight Management for the Windows Servers 2003/2008 x64 Edition をインストールします。

ポート番号の変更

デフォルトでは、`opctrapi` は、SNMP トラップと CMIP イベントを受信するようにポート番号 162 上に設定されます。ポート番号を変更するには、次のステップに従います。

1. SNMP サービスが実行中であることを確認します。
   Windows の場合、以下の手順を実行します。
   a. **[スタート]** → **[ファイル名を指定して実行]** をクリックし、「services.msc」と入力します。**[サービス]** ダイアログ ボックスが開きます。
   b. **[SNMP サービス]** を選択します。
   c. SNMP サービスが Status=Started であることを確認します。

   UNIX の場合、以下のコマンドを入力します。

   ```
   # service snmp status
   ```
2. opctrapi がデフォルトのポート番号 162 で設定されていることを確認します。
   Windows の場合、以下のコマンドを入力します。

   ```
   netstat -anb | findstr opctrapi
   ```

   UNIX の場合、以下のコマンドを入力します。

   ```
   # netstat -anp | grep 162
   ```
3. 管理ノード上の XPL 設定を変更するには、以下のコマンドを入力します。
   ```
   # ovconfchg -ns eaagt -set SNMP_TRAP_PORT <任意の許可されたポート>
   ```
4. eaagt 名前空間の下に SNMP_TRAP_PORT= <任意の許可されたポート> を追加します。
5. eaagt 名前空間内のすべての属性を返すには、以下のコマンドを入力します。
   ```
   # ovconfget eaagt
   ```
6. opctrapi を再起動するには、以下のコマンドを入力します。
   ```
   # ovc -restart opctrapi
   ```
7. ポート番号が変更されたことを確認します。
   Windows の場合、以下のコマンドを入力します。

   ```
   netstat -anb | findstr opctrapi
   ```

   UNIX の場合、以下のコマンドを入力します。

   ```
   # netstat -anp | grep <changed port>
   ```

Server Health Traps Monitor ポリシー

SI-HPProLiant_CPQHLTHTraps

SI-HPProLiant_CPQHLTHTraps ポリシーは、サーバーの正常性に関連する SNMP トラップをインターセプトし、トラップが生成されるたびに HPOM コンソールにアラートを送信します。このポリシーが監視する SNMP トラップは以下のとおりです。

MIB ID	SNMP トラップの説明。
1.3.6.1.2.1.11.6.0	coldStart。
1.3.6.1.2.1.11.6.1	warmStart。
1.3.6.1.2.1.11.6.2	linkDown。

1.3.6.1.2.1.11.6.3	linkUp。
MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.6003	システムは、この温度状態によりシャットダウンします。
1.3.6.1.4.1.232.0.6017	システムは、この温度状態によりシャットダウンします。
1.3.6.1.4.1.232.0.6004	温度が範囲外です。シャットダウンが行われる場合があります。
1.3.6.1.4.1.232.0.6018	温度が範囲外です。シャットダウンが行われる場合があります。
1.3.6.1.4.1.232.0.6019	温度が正常範囲に戻りました。
1.3.6.1.4.1.232.0.6005	温度が正常範囲に戻りました。
1.3.6.1.4.1.232.0.6040	SNMP Varbind 3 に含まれるシャーシ、SNMP Varbind 4 に含まれる位置の温度ステータスが障害になりました。
1.3.6.1.4.1.232.0.6041	SNMP Varbind 4 に含まれるシャーシ、SNMP Varbind 5 に含まれる位置の温度ステータスが機能低下になりました。
1.3.6.1.4.1.232.0.6041	SNMP Varbind 4 に含まれるシャーシ、SNMP Varbind 5 に含まれる位置の温度が範囲外です。間もなくシャットダウンが行われる場合があります。
1.3.6.1.4.1.232.0.6042	SNMP Varbind 3 に含まれるシャーシ、SNMP Varbind 4 に含まれる位置の温度ステータスが正常です。
1.3.6.1.4.1.232.0.6007	オプション ファンが正常に動作していません。
1.3.6.1.4.1.232.0.6021	オプション ファンが正常に動作していません。
1.3.6.1.4.1.232.0.6006	必須ファンが正常に動作していません。シャットダウンが行われる場合があります。
1.3.6.1.4.1.232.0.6020	必須ファンが正常に動作していません。
1.3.6.1.4.1.232.0.6020	システム ファンに障害が発生しました。
1.3.6.1.4.1.232.0.6022	システム ファンが正常動作に戻りました。
1.3.6.1.4.1.232.0.6008	システム ファンが正常動作に戻りました。
1.3.6.1.4.1.232.0.6009	CPU ファンに障害が発生しました。サーバーはシャットダウンします。
1.3.6.1.4.1.232.0.6010	CPU ファンが良好になりました。
1.3.6.1.4.1.232.0.6023	CPU ファンに障害が発生しました。サーバーはシャットダウンします。
1.3.6.1.4.1.232.0.6024	CPU ファンが良好になりました。

1.3.6.1.4.1.232.0.6035	SNMP Varbind 3 に含まれるシャーシ、SNMP Varbind 4 に含まれる位置でファンが機能低下になりました。
1.3.6.1.4.1.232.0.6036	SNMP Varbind 3 に含まれるシャーシ、SNMP Varbind 4 に含まれる位置でファンが障害になりました。
1.3.6.1.4.1.232.0.6037	SNMP Varbind 3 に含まれるシャーシでファンが冗長ではなくなりました。
1.3.6.1.4.1.232.0.6055	指定されたシャーシで耐障害ファンが冗長ステータスに戻りました。
1.3.6.1.4.1.232.0.6048	SNMP Varbind 3 のシャーシで電源は良好です。
1.3.6.1.4.1.232.0.6049	SNMP Varbind 3 のシャーシで電源が機能低下です。
1.3.6.1.4.1.232.0.6050	SNMP Varbind 3 のシャーシで電源が障害状態です。
1.3.6.1.4.1.232.0.6014	電源ステータスが機能低下になりました。
1.3.6.1.4.1.232.0.6028	電源ステータスが機能低下になりました。
1.3.6.1.4.1.232.0.6030	SNMP Varbind 3 に含まれるシャーシ、SNMP Varbind 4 に含まれるベイで電源が機能低下になりました。
1.3.6.1.4.1.232.0.6054	耐障害電源の電源冗長性が復旧しました。
1.3.6.1.4.1.232.0.6031	SNMP Varbind 3 に含まれるシャーシ、SNMP Varbind 4 に含まれるベイで電源が障害になりました。
1.3.6.1.4.1.232.0.6032	SNMP Varbind 3 に含まれるシャーシで電源が冗長ではなくなりました。
1.3.6.1.4.1.232.0.6043	SNMP Varbind 3 のシャーシ、SNMP Varbind 4 のスロット、SNMP Varbind 5 のソケットで電源コンバーターが機能低下になりました。
1.3.6.1.4.1.232.0.6044	SNMP Varbind 3 のシャーシ、SNMP Varbind 4 のスロット、SNMP Varbind 5 のソケットで電源コンバーターが障害になりました。
1.3.6.1.4.1.232.0.6045	SNMP Varbind 3 に含まれるシャーシで電源コンバーターが冗長ではなくなりました。
1.3.6.1.4.1.232.0.6012	サーバーは、熱によるシャットダウンの後に再度動作状態になりました。
1.3.6.1.4.1.232.0.6027	サーバーの再起動中にエラーが発生しました。
1.3.6.1.4.1.232.0.6059	メモリ ボードやカートリッジ バスのエラーが検出されました。
1.3.6.1.4.1.232.0.6063	管理プロセッサはリセットできませんでした。
1.3.6.1.4.1.232.0.6025	サーバーは、ASR によるシャットダウンの後に再度動作状態になりました。
1.3.6.1.4.1.232.0.6016	メモリ エラー数が多すぎるため、トラッキングが無効になりました。

1.3.6.1.4.1.232.0.6016	エラー トラッキングが有効になりました。
1.3.6.1.4.1.232.0.6002	メモリ エラー数が多すぎるため、トラッキングが無効になりました。
1.3.6.1.4.1.232.0.6026	サーバーは、熱によるシャットダウンの後に再度動作状態になりました。
1.3.6.1.4.1.232.0.6061	管理プロセッサが現在リセット状態です。
1.3.6.1.4.1.232.0.6062	管理プロセッサが準備を完了しました。
1.3.6.1.4.1.232.0.6013	サーバーの再起動中にエラーが発生しました。

このポリシーには、これらの各 SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

RAID Controller Traps Monitor ポリシー

SI-HPProLiant_CPQRCTraps

SI-HPProLiant_CPQRCTraps ポリシーは、RAID コントローラーのパフォーマンスと可用性に関連する SNMP トラップをインターセプトし、トラップが生成されるたびに HPOM コンソールにアラートを送信します。このポリシーが監視するトラップは以下のとおりです。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.141.3.8.0.27	拡張キャビネット内の温度により重大状態がトリガーされ、コントローラーにより検出されました。
1.3.6.1.4.1.232.141.3.8.6.26	cpqCrExpCabTemperatureWarningTrap。
1.3.6.1.4.1.232.141.3.8.0.22	拡張キャビネット内のいずれかの電源に障害が発生しました。
1.3.6.1.4.1.232.141.3.8.0.20	拡張キャビネット内のファンに障害が発生しました。
1.3.6.1.4.1.232.141.3.7.0.25	プライマリ エンクロージャ内の温度が正常に戻りました。
1.3.6.1.4.1.232.141.3.2.0.2	サブシステム内のプライマリ コントローラーが復旧しました。
1.3.6.1.4.1.232.141.3.8.0.29	拡張キャビネット内のいずれかの電源が復旧しました。
1.3.6.1.4.1.232.141.3.3.0.6	RAID set に障害が発生したか、オフラインです。
1.3.6.1.4.1.232.141.3.8.0.28	拡張キャビネット内の温度が正常に戻りました。
1.3.6.1.4.1.232.141.3.2.0.1	サブシステム内のプライマリ コントローラーに障害が発生しました。
1.3.6.1.4.1.232.141.3.7.0.16	プライマリ エンクロージャ内のいずれかの冷却ファンに障害が発生しました。

1.3.6.1.4.1.232.141.3.2.0.4	サブシステム内のセカンダリ コントローラーが復旧しました。
1.3.6.1.4.1.232.141.3.7.0.19	プライマリ エンクロージャ内のいずれかの電源が復旧しました。
.1.3.6.1.4.1.232.141.3.5.6.31	cpqCrPhyDiskFailureTrap。
1.3.6.1.4.1.232.141.3.7.0.24	プライマリ エンクロージャ内の温度により重大状態がトリガーされ、コントローラーにより検出されました。
1.3.6.1.4.1.232.141.3.5.0.10	ディスク デバイスが復旧しました。
1.3.6.1.4.1.232.141.3.7.0.17	プライマリ エンクロージャ内のいずれかの冷却ファンが復旧しました。
1.3.6.1.4.1.232.141.3.5.6.30	cpqCrPhyDiskInformationTrap。
1.3.6.1.4.1.232.141.3.2.0.3	サブシステム内のセカンダリ コントローラーに障害が発生しました。
1.3.6.1.4.1.232.141.3.8.0.21	拡張キャビネット内のいずれかの冷却ファンが復旧しました。
1.3.6.1.4.1.232.141.3.5.0.11	ディスク デバイスに障害が発生しました。
1.3.6.1.4.1.232.141.3.7.0.23	プライマリ エンクロージャの温度が警告レベルです。
1.3.6.1.4.1.232.141.3.7.0.18	プライマリ エンクロージャ内のいずれかの電源に障害が発生しました。

このポリシーには、これらの各 SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

NIC Traps Monitor ポリシー

SI-HPProLiant_CPQNICTraps

SI-HPProLiant_CPQNICTraps ポリシーは、ネットワーク インターフェイス カード (NIC) のパフォーマンスと可用性に関連する SNMP トラップをインターセプトし、トラップが生成されるたびに HPOM コンソールにアラートを送信します。このポリシーが監視するトラップは以下のとおりです。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.11005	NIC ステータスは良好です。
1.3.6.1.4.1.232.0.11006	NIC ステータスが障害です。
1.3.6.1.4.1.232.0.11007	NIC スイッチオーバーが発生しました。
1.3.6.1.4.1.232.0.11008	NIC ステータスは良好です。
1.3.6.1.4.1.232.0.11009	NIC ステータスが障害です。

1.3.6.1.4.1.232.0.11010	NIC スイッチオーバー。
1.3.6.1.2.1.11.6.2	linkDown。
1.3.6.1.2.1.11.6.3	linkUp。
1.3.6.1.4.1.232.0.18006	SNMP Varbind 3 に含まれるスロット、SNMP Varbind 4 に含まれるポートの論理アダプターで接続が失われました。
1.3.6.1.4.1.232.6.18012	cpqNic3ConnectivityLost。
1.3.6.1.4.1.232.6.18011	cpqNic3ConnectivityRestored.
1.3.6.1.4.1.232.0.18009	NIC ウイルス類似活動の検出トラップ。
1.3.6.1.4.1.232.0.18010	NIC ウイルス類似活動の検出なしトラップ。

このポリシーには、これらの各 SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

CMC Traps Monitor ポリシー

SI-HPProLiant_CPQCMCTraps

SI-HPProLiant_CPQCMCTraps ポリシーは、電力消費、煙、湿度、温度、ファンの観点から Console Management Controller (CMC) の正常性に関連する SNMP トラップをインターセプトします。また、トラップが生成されるたびに HPOM コンソールにアラートを送信します。

このポリシーが監視するトラップは以下のとおりです。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.153.0.153013	CMC により検出されたラック内煙有無のステータスが Present です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153013	CMC により検出されたラック内煙有無のステータスが Normal です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153005	CMC への供給電圧のステータスが OverMax です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153005	CMC への供給電圧のステータスが UnderMin です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153005	CMC への供給電圧のステータスが Normal です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153001	CMC 温度センサー 1 により検出されたラック内温度が高しきい値を上回りました。このステータスは SNMP Varbind 5 に含まれます。

1.3.6.1.4.1.232.153.0.153001	CMC 温度センサー 1 により検出されたラック内温度が最小しきい値を下回りました。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153002	CMC 温度センサー 1 により検出されたラック内温度は正常です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153002	CMC 温度センサー 2 により検出されたラック内温度が高しきい値を上回りました。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153002	CMC 温度センサー 2 により検出されたラック内温度が最小しきい値を下回りました。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153002	CMC 温度センサー 2 により検出されたラック内温度は正常です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153006	湿度のステータスが OverMax です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153006	湿度のステータスが UnderMin です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153006	湿度のステータスが Normal です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153003	ラック内ファン 1 のステータスが Normal です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153003	ラック内ファン 1 のステータスが AutoOff です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153003	ラック内ファン 1 のステータスが SmokeOff です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153003	ラック内ファン 1 のステータスが DoorOff です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153004	ラック内ファン 2 のステータスが AutoOn です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153004	ラック内ファン 2 のステータスが AutoOff です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153004	ラック内ファン 2 のステータスが SmokeOff です。このステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.153.0.153004	ラック内ファン 2 のステータスが DoorOff です。このステータスは SNMP Varbind 5 に含まれます。

このポリシーには、これらの各 SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

System Information Traps Monitor ポリシー

SI-HPProLiant_CPQSysInfoTraps

SI-HPProLiant_CPQSysInfoTraps ポリシーは、バッテリ、モニタ、ホット プラグ スロット ボード、フードの状態の観点から、システム情報に関連する SNMP トラップをインターセプトします。また、トラップが生成されるたびに HPOM コンソールにアラートを送信します。

このポリシーが監視するトラップは以下のとおりです。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.2012	バッテリ SNMP Varbind 3 の充電容量が機能低下になりました。
1.3.6.1.4.1.232.0.2011	バッテリ SNMP Varbind 3 に障害が発生しました。
1.3.6.1.4.1.232.0.2013	SNMP Varbind 3 に含まれるバッテリに調整エラーがあります。
1.3.6.1.4.1.232.0.2003	モニタの状態が機能低下に設定されました。
1.3.6.1.4.1.232.0.2004	モニタの状態が障害に設定されました。
1.3.6.1.4.1.232.0.2002	モニタの状態が良好に設定されました。
1.3.6.1.4.1.232.0.2006	メモリ モジュール ECC ステータスが良好に設定されました。
1.3.6.1.4.1.232.0.2005	メモリ モジュール ECC ステータスが機能低下に設定されました。
1.3.6.1.4.1.232.0.2009	SNMP Varbind 3 に含まれるシャーシ、SNMP Varbind 4 に含まれるスロットにホット プラグ スロット ボードが取り付けられました。
1.3.6.1.4.1.232.0.2010	SNMP Varbind 3 に含まれるシャーシ、SNMP Varbind 4 に含まれるスロットでホット プラグ スロット ボードに障害が発生しました。このエラーは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.2008)	シャーシからホット プラグ スロット ボードが取り外されました。
1.3.6.1.4.1.232.0.2007	システムのメモリ構成が変更されました。
1.3.6.1.4.1.232.0.2001	フードがユニットから取り外されています。

このポリシーには、これらの各 SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

Virtual Connect Domain Traps Monitor ポリシー

SI-HPProLiant_VCDomainTraps

SI-HPProLiant_VCDomainTraps ポリシーは、仮想接続ドメインに関連する SNMP トラップをインターセプトします。また、トラップが生成されるたびに HPOM コンソールにアラートを送信します。

このポリシーが監視するトラップは以下のとおりです。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.11.5.7.5.2.1.2.0.5	vcFcFabricManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.3	vcCheckpointCompleted
1.3.6.1.4.1.11.5.7.5.2.1.2.0.9	vcProfileManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.6	vcModuleManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.8	vcPhysicalServerManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.1	vcDomainManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.2	vcCheckpointTimeout

このポリシーには、これらの各 SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

Cluster Traps Monitor ポリシー

SI-HPProLiant_CPQCLUSTraps

SI-HPProLiant_CPQCLUSTraps ポリシーは、バッテリ、モニタ、ホット プラグ スロット ボード、フードの状態の観点から、クラスターに関連する SNMP トラップをインターセプトします。また、トラップが生成されるたびに HPOM コンソールにアラートを送信します。

このポリシーが監視するトラップは以下のとおりです。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.15001	SNMP Varbind 3 に含まれるクラスターが機能低下になりました。
1.3.6.1.4.1.232.0.15002	SNMP Varbind 3 に含まれるクラスターに障害が発生しました。
1.3.6.1.4.1.232.0.15003	SNMP Varbind 3 に含まれるノード上のクラスター サービスが低下になりました。
1.3.6.1.4.1.232.0.15004	SNMP Varbind 3 に含まれるノード上のクラスター サービスに障害が発生しました。
1.3.6.1.4.1.232.0.15007	SNMP Varbind 3 に含まれるクラスター リソースが低下になりました。
1.3.6.1.4.1.232.0.15005	SNMP Varbind 3 に含まれるクラスター リソースに障害が発生しました。
1.3.6.1.4.1.232.0.15008	SNMP Varbind 3 に含まれるクラスター ネットワークが機能低下状態になりました。

1.3.6.1.4.1.232.0.15006	SNMP Varbind 3 に含まれるクラスター ネットワークに障害が発生しました。

このポリシーには、これらの各 SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

Rack Power Manager Traps Monitor ポリシー

SI-HPProLiant_CPQRPMTraps

SI-HPProLiant_CPQRPMTraps ポリシーは、Rack Power Manager に関連する SNMP トラップをインターセプトします。また、トラップが生成されるたびに HPOM コンソールにアラートを送信します。

このポリシーが監視するトラップは以下のとおりです。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.154.2.1	UPS デバイスは、接続が失われたことを報告しています
1.3.6.1.4.1.232.154.2.2	UPS デバイスは、接続が失われたことを報告しています
1.3.6.1.4.1.232.154.2.3	CRPM は、デバイス ホスト名の IP アドレスを見つけられませんでした
1.3.6.1.4.1.232.154.2.4	CRPM はデバイスに接続できませんでした
1.3.6.1.4.1.232.154.2.5	cpqRPMTrapDeviceSettingsChanged
1.3.6.1.4.1.232.154.2.10001	CMC デバイスは、温度 1 が最小しきい値を下回っていることを報告しています
1.3.6.1.4.1.232.154.2.10002	CMC デバイスは、温度 1 が注意域しきい値を上回っていることを報告しています
1.3.6.1.4.1.232.154.2.10003	CMC デバイスは、温度 1 が最大しきい値を上回っていることを報告しています
1.3.6.1.4.1.232.154.2.10004	CMC デバイスは、温度 1 が正常に戻ったことを報告しています
1.3.6.1.4.1.232.154.2.10005	CMC デバイスは、温度 2 が最小しきい値を下回っていることを報告しています
1.3.6.1.4.1.232.154.2.10006	CMC デバイスは、温度 2 が注意域しきい値を上回っていることを報告しています
1.3.6.1.4.1.232.154.2.10007	CMC デバイスは、温度 2 が最大しきい値を上回っていることを報告しています
1.3.6.1.4.1.232.154.2.10008	CMC デバイスは、温度 2 が正常に戻ったことを報告しています

1.3.6.1.4.1.232.154.2.10011	CMC デバイスは、電圧が最小しきい値を下回っていることを報告しています
1.3.6.1.4.1.232.154.2.10012	CMC デバイスは、電圧が最大しきい値を上回っていることを報告しています
1.3.6.1.4.1.232.154.2.10013	CMC デバイスは、電圧が正常に戻ったことを報告しています
1.3.6.1.4.1.232.154.2.10021	CMC デバイスは、湿度が最小しきい値を下回っていることを報告しています
1.3.6.1.4.1.232.154.2.10022	CMC デバイスは、湿度が最大しきい値を上回っていることを報告しています
1.3.6.1.4.1.232.154.2.10023	CMC デバイスは、湿度が正常に戻ったことを報告しています
1.3.6.1.4.1.232.154.2.10031	CMC デバイスは、煙が検出されたことを報告しています
1.3.6.1.4.1.232.154.2.10032	CMC デバイスは、煙が検出されなくなったことを報告しています
1.3.6.1.4.1.232.154.2.10041	CMC デバイスは、衝撃が検出されたことを報告しています
1.3.6.1.4.1.232.154.2.10042	CMC デバイスは、衝撃が検出されなくなったことを報告しています
1.3.6.1.4.1.232.154.2.10051	CMC デバイスは、補助入力 1 でアラーム状態になりました
1.3.6.1.4.1.232.154.2.10052	CMC デバイスは、補助入力 1 のアラームが解決したことを報告しています
1.3.6.1.4.1.232.154.2.10053	CMC デバイスは、補助入力 2 でアラーム状態になりました
1.3.6.1.4.1.232.154.2.10054	CMC デバイスは、補助入力 2 のアラームが解決したことを報告しています
1.3.6.1.4.1.232.154.2.10101	CMC デバイスは、入力 1 が開いたことを報告しています
1.3.6.1.4.1.232.154.2.10102	CMC デバイスは、入力 1 が閉じたことを報告しています
1.3.6.1.4.1.232.154.2.10103	CMC デバイスは、入力 2 が開いたことを報告しています
1.3.6.1.4.1.232.154.2.10104	CMC デバイスは、入力 2 が閉じたことを報告しています
1.3.6.1.4.1.232.154.2.10105	CMC デバイスは、入力 3 が開いたことを報告しています
1.3.6.1.4.1.232.154.2.10106	CMC デバイスは、入力 3 が閉じたことを報告しています
1.3.6.1.4.1.232.154.2.10107	CMC デバイスは、入力 4 が開いたことを報告しています
1.3.6.1.4.1.232.154.2.10108	CMC デバイスは、入力 4 が閉じたことを報告しています

1.3.6.1.4.1.232.154.2.10111	CMC デバイスは、ロックセット 1 がロック解除されたことを報告しています
1.3.6.1.4.1.232.154.2.10112	CMC デバイスは、ロックセット 1 をロックできなかったことを報告しています
1.3.6.1.4.1.232.154.2.10113	CMC デバイスは、ロックセット 1 のエラーを報告しています
1.3.6.1.4.1.232.154.2.10114	CMC デバイスは、ロックセット 1 がロックされたことを報告しています
1.3.6.1.4.1.232.154.2.10116	CMC デバイスは、ロックセット 2 がロック解除されたことを報告しています
1.3.6.1.4.1.232.154.2.10117	CMC デバイスは、ロックセット 2 をロックできなかったことを報告しています
1.3.6.1.4.1.232.154.2.10118	CMC デバイスは、ロックセット 2 のエラーを報告しています
1.3.6.1.4.1.232.154.2.10119	CMC デバイスは、ロックセット 2 がロックされたことを報告しています
1.3.6.1.4.1.232.154.2.10134	CMC デバイスは、ロックセット 1 が正常であることを報告しています
1.3.6.1.4.1.232.154.2.10135	CMC デバイスは、ロックセット 2 が正常であることを報告しています
1.3.6.1.4.1.232.154.2.20001	cpqRPMTrapUPSInputVoltageBelowMin
1.3.6.1.4.1.232.154.2.20002	cpqRPMTrapUPSInputVoltageAboveMax
1.3.6.1.4.1.232.154.2.20003	cpqRPMTrapUPSInputVoltageNormal
1.3.6.1.4.1.232.154.2.20011	cpqRPMTrapUPSOutputVoltageBelowMin
1.3.6.1.4.1.232.154.2.20012	cpqRPMTrapUPSOutputVoltageAboveMax
1.3.6.1.4.1.232.154.2.20014	UPS デバイスは、過負荷状態を報告しています
1.3.6.1.4.1.232.154.2.20015	UPS デバイスは、過負荷状態が解決したことを報告しています
1.3.6.1.4.1.232.154.2.20022	cpqRPMTrapUPSBatteryDepleted
1.3.6.1.4.1.232.154.2.20023	cpqRPMTrapUPSBatteryLevelNormal
1.3.6.1.4.1.232.154.2.20032	cpqRPMTrapUPSOnBypass
1.3.6.1.4.1.232.154.2.20101	cpqRPMTrapUPSTemperatureLow
1.3.6.1.4.1.232.154.2.20102	cpqRPMTrapUPSTemperatureHigh
1.3.6.1.4.1.232.154.2.20103	UPS デバイスは、温度が正常であることを報告しています

1.3.6.1.4.1.232.154.2.20111	UPS デバイスは、一般 UPS 障害を報告しています
1.3.6.1.4.1.232.154.2.20112	UPS デバイスは、一般 UPS 障害が解決したことを報告しています
1.3.6.1.4.1.232.154.2.20121	UPS デバイスは、バッテリの障害を報告しています
1.3.6.1.4.1.232.154.2.20122	UPS デバイスは、バッテリの障害が解決したことを報告しています
1.3.6.1.4.1.232.154.2.20131	UPS デバイスは、診断テストが失敗したことを報告しています
1.3.6.1.4.1.232.154.2.20132	UPS デバイスは、診断テストが成功したことを報告しています
1.3.6.1.4.1.232.154.2.20141	UPS 用入力 (商用電源): 測定された入力の周波数が、正常動作のための周波数範囲から外れています
1.3.6.1.4.1.232.154.2.20142	UPS の測定された入力周波数は正常です
1.3.6.1.4.1.232.154.2.20151	UPS デバイスはバッテリ電源で起動しました
1.3.6.1.4.1.232.154.2.20152	UPS デバイスは商用電源で起動しました
1.3.6.1.4.1.232.154.2.20161	UPS デバイスは、バイパス機能が利用できないことを報告しています
1.3.6.1.4.1.232.154.2.20162	UPS デバイスは、バイパス機能利用不可エラーが解決したことを報告しています
1.3.6.1.4.1.232.154.2.20171	cpqRPMTrapUPSUtilityFail
1.3.6.1.4.1.232.154.2.20172	cpqRPMTrapUPSUtilityFailCleared
1.3.6.1.4.1.232.154.2.20181	cpqRPMTrapUPSUtilityNotPresent
1.3.6.1.4.1.232.154.2.20182	cpqRPMTrapUPSUtilityNotPresentCleared
1.3.6.1.4.1.232.154.2.20191	cpqRPMTrapUPSBypassManualTurnedOn
1.3.6.1.4.1.232.154.2.20192	cpqRPMTrapUPSBypassManualTurnedOff
1.3.6.1.4.1.232.154.2.20201	UPS デバイスは、入力配線の問題を報告しています
1.3.6.1.4.1.232.154.2.20202	UPS デバイスは、入力配線が正常であることを報告しています
1.3.6.1.4.1.232.154.2.21007	UPS デバイスは、温度が範囲外であることを報告しています
1.3.6.1.4.1.232.154.2.21008	UPS デバイスは、温度が正常であることを報告しています
1.3.6.1.4.1.232.154.2.21011	UPS デバイスがシャットダウン間近状態を報告しています
1.3.6.1.4.1.232.154.2.21012	UPS はシャットダウン間近状態ではなくなりました
1.3.6.1.4.1.232.154.2.21013	UPS デバイスは、シャットダウン切迫状態を報告しています

1.3.6.1.4.1.232.154.2.21014	UPS デバイスは、シャットダウン切迫状態が解決したことを報告しています
1.3.6.1.4.1.232.154.2.21019	UPS デバイスは、出力電圧が範囲外であることを報告しています
1.3.6.1.4.1.232.154.2.21020	UPS デバイスは、出力電圧が正常であることを報告しています
1.3.6.1.4.1.232.154.2.21021	UPS デバイスは、入力電圧が範囲外であることを報告しています
1.3.6.1.4.1.232.154.2.21021	UPS デバイスは、入力電圧が範囲外であることを報告しています
1.3.6.1.4.1.232.154.2.21023	UPS デバイスは、冗長性が失われたことを報告しています
1.3.6.1.4.1.232.154.2.21024	UPS デバイスは、冗長性が回復したことを報告しています
1.3.6.1.4.232.154.2.21029	UPS デバイスは、トリム状態を報告しています
1.3.6.1.4.232.154.2.21031	UPS デバイスは、ブースト状態を報告しています
1.3.6.1.4.1.232.154.2.21033	UPS は、ユーザー操作により電源がオフになりました
1.3.6.1.4.1.232.154.2.21034	UPS 出力が回復しました
1.3.6.1.4.1.232.154.2.21035	UPS デバイスは、ファンの障害が発生したことを報告しています
1.3.6.1.4.1.232.154.2.21036	UPS デバイスは、ファンの障害が解決したことを報告しています
1.3.6.1.4.1.232.154.2.21037	UPS デバイスは、緊急電源停止機能 (EPO) コマンドを報告しています
1.3.6.1.4.1.232.154.2.21041	UPS デバイスは、出力ブレーカーまたはリレーに障害が発生したことを報告しています
1.3.6.1.4.1.232.154.2.21042	UPS デバイスは、出力ブレーカーが正常に機能していることを報告しています
1.3.6.1.4.1.232.154.2.21045	UPS デバイスは、カバー パネルが取り外されたことを報告しています
1.3.6.1.4.1.232.154.2.21046	UPS デバイスは、カバー パネルが取り付けられたことを報告しています
1.3.6.1.4.1.232.154.2.21047	UPS デバイスは、自動バイパス モードで動作していることを報告しています
1.3.6.1.4.1.232.154.2.21048	UPS デバイスは、自動バイパス モードで動作していないことを報告しています
1.3.6.1.4.1.232.154.2.21053	UPS デバイスは、UPS にバッテリが接続されていないことを報告しています
1.3.6.1.4.1.232.154.2.21054	UPS デバイスは、UPS にバッテリが再接続されたことを報告しています

1.3.6.1.4.1.232.154.2.21055	UPS デバイスは、バッテリ残量低下を報告しています
1.3.6.1.4.1.232.154.2.21056	UPS デバイスは、バッテリ残量低下が解決したことを報告しています
1.3.6.1.4.1.232.154.2.21057	UPS デバイスは、バッテリが完全に放電したことを報告しています
1.3.6.1.4.1.232.154.2.21058	UPS デバイスは、バッテリが完全に放電したことを報告しています
1.3.6.1.4.1.232.154.2.21059	UPS デバイスは、手動バイパス モードで動作していることを報告しています
1.3.6.1.4.1.232.154.2.21060	UPS デバイスは、通常モードで動作していることを報告しています
1.3.6.1.4.1.232.154.2.21063	UPS デバイスは、バッテリ使用状態を報告しています
1.3.6.1.4.1.232.154.2.21064	UPS デバイスは、商用電源使用状態を報告しています
1.3.6.1.4.1.232.154.3.1	危険域アラームが発生しました
1.3.6.1.4.1.232.154.3.2	UPS に危険域アラームが発生しました
1.3.6.1.4.1.232.154.2.3	CRPM は、デバイス ホスト名の IP アドレスを見つけられませんでした
1.3.6.1.4.1.232.154.3.4	UPS のアラームが解決しました
1.3.6.1.4.1.232.154.2.50001	cpqRPMTestTrap
1.3.6.1.4.1.232.154.2.29999	cpqRPMTrapUPSDCStartOccurredCleared
1.3.6.1.4.1.232.154.2.29998	cpqRPMTrapUPSDCStartOccurred

このポリシーには、これらの各 SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

Intelligent Drive Array Traps Monitor ポリシー

SI-HPProLiant_FwdDriveArrayTraps

SI-HPProLiant_FwdDriveArrayTraps ポリシーは、Compaq の Intelligent Drive Array に関連する SNMP トラップをインターセプトします。また、トラップが生成されるたびに HPOM コンソールにアラートを送信します。

このポリシーが監視するトラップは以下のとおりです。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3001	インテリジェント ドライブ アレイの論理ドライブ ステータスは正常です。ステータスは SNMP Varbind 1 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3001	インテリジェント ドライブ アレイの論理ドライブ ステータスが障害です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3001	インテリジェント ドライブ アレイの論理ドライブ ステータスが回復中です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3001	インテリジェント ドライブ アレイの論理ドライブ ステータスが READY for REBUILD (再構築可) です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3001	インテリジェント ドライブ アレイの論理ドライブ ステータスが再構築中です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3001	インテリジェント ドライブ アレイの論理ドライブ ステータスが WRONG DRIVE (間違ったドライブ) です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3001	インテリジェント ドライブ アレイの論理ドライブ ステータスが BAD CONNECTION (接続不良) です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3001	インテリジェント ドライブ アレイの論理ドライブ ステータスが過熱中です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3001	インテリジェント ドライブ アレイの論理ドライブ ステータスがシャットダウンです。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3001	インテリジェント ドライブ アレイの論理ドライブ ステータスが NOT AVAILABLE (利用不可) です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3001	インテリジェント ドライブ アレイの論理ドライブ ステータスが未構成です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3001	インテリジェント ドライブ アレイの論理ドライブ ステータスが拡張中です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3001	インテリジェント ドライブ アレイの論理ドライブ ステータスが QUEUED FOR EXPANSION (拡張キュー登録済み) です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3002	インテリジェント ドライブ アレイのスペア ドライブ ステータスがアクティブです。ステータスは SNMP Varbind 1 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3002	インテリジェント ドライブ アレイのスペア ドライブ ステータスが無効です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3002	インテリジェント ドライブ アレイのスペア ドライブ ステータスが非アクティブです。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3002	インテリジェント ドライブ アレイのスペア ドライブ ステータスが障害です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3002	インテリジェント ドライブ アレイのスペア ドライブ ステータスが構築中です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3003	インテリジェント ドライブ アレイの物理ドライブ ステータスは良好です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3003	インテリジェント ドライブ アレイの物理ドライブ ステータスが障害です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3003	インテリジェント ドライブ アレイの物理ドライブ ステータスが PREDICTIVEFAILURE (障害予測) です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3004	インテリジェント ドライブ アレイの物理ドライブがしきい値を超過しました。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3005	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが無効です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3005	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが有効です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3005	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが TEMPORARILY DISABLED (一時的に無効) です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3005	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが PERMANENTLY DISABLED (完全に無効) です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3006	インテリジェント ドライブ アレイのアクセラレーターのバッテリ電源が失われました。データ損失の可能性があります。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3007	インテリジェント ドライブ アレイのアクセラレーター ボード バッテリ ステータスが充電中です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3007	インテリジェント ドライブ アレイのアクセラレーター ボード バッテリ ステータスが NOT PRESENT (なし) です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3007	インテリジェント ドライブ アレイのアクセラレーター ボード バッテリ ステータスは良好です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3007	インテリジェント ドライブ アレイのアクセラレーター ボード バッテリ ステータスが障害です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3007	インテリジェント ドライブ アレイのアクセラレーター ボード バッテリ ステータスが機能低下です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3008	インテリジェント ドライブ アレイの論理ドライブ ステータスが未構成です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3008	インテリジェント ドライブ アレイの論理ドライブ ステータスが拡張中です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3008	インテリジェント ドライブ アレイの論理ドライブ ステータスが QUEUED FOR EXPANSION (拡張キュー登録済み) です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3008	インテリジェント ドライブ アレイの論理ドライブ ステータスは正常です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3008	インテリジェント ドライブ アレイの論理ドライブ ステータスが障害です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3008	インテリジェント ドライブ アレイの論理ドライブ ステータスが回復中です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3008	インテリジェント ドライブ アレイの論理ドライブ ステータスが READY for REBUILD (再構築可) です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3008	インテリジェント ドライブ アレイの論理ドライブ ステータスが再構築中です。ステータスは SNMP Varbind 3 に含まれます

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3008	インテリジェント ドライブ アレイの論理ドライブ ステータスが WRONG DRIVE (間違ったドライブ) です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3008	インテリジェント ドライブ アレイの論理ドライブ ステータスが BAD CONNECTION (接続不良) です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3008	インテリジェント ドライブ アレイの論理ドライブ ステータスが過熱中です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3008	インテリジェント ドライブ アレイの論理ドライブ ステータスがシャットダウンです。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3008	インテリジェント ドライブ アレイの論理ドライブ ステータスが NOT AVAILABLE (利用不可) です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3009	インテリジェント ドライブ アレイのスペア ドライブ ステータスが無効です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3009	インテリジェント ドライブ アレイのスペア ドライブ ステータスが非アクティブです。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3009	インテリジェント ドライブ アレイのスペア ドライブ ステータスがアクティブです。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3009	インテリジェント ドライブ アレイのスペア ドライブ ステータスが障害です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3009	インテリジェント ドライブ アレイのスペア ドライブ ステータスが構築中です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3010	インテリジェント ドライブ アレイの物理ドライブ ステータスは良好です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3010	インテリジェント ドライブ アレイの物理ドライブ ステータスが障害です。ステータスは SNMP Varbind 3 に含まれ、SCSI バスは Varbind 4 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3010	SCSI バス上のインテリジェント ドライブ アレイの物理ドライブ ステータスが PREDICTIVEFAILURE (障害予測) です。ステータスは SNMP Varbind 3 に含まれ、SCSI バス番号は Varbind 4 に含まれます。
1.3.6.1.4.1.232.0.3011	インテリジェント ドライブ アレイの物理ドライブがしきい値を超過しました。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3012	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが無効です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3012	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが有効です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3012	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが TEMPORARILY DISABLED (一時的に無効) です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3012	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが PERMANENTLY DISABLED (完全に無効) です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3013	インテリジェント ドライブ アレイのアクセラレーターのバッテリ電源が失われました。データ損失の可能性があります。
1.3.6.1.4.1.232.0.3014	インテリジェント ドライブ アレイのアクセラレーター ボード バッテリ ステータスが充電中です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3014	インテリジェント ドライブ アレイのアクセラレーター ボード バッテリ ステータスが NOT PRESENT (なし) です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3014	インテリジェント ドライブ アレイのアクセラレーター ボード バッテリ ステータスは良好です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3014	インテリジェント ドライブ アレイのアクセラレーター ボード バッテリ ステータスが障害です。ステータスは SNMP Varbind 3 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3014	インテリジェント ドライブ アレイのアクセラレーター ボード バッテリ ステータスが機能低下です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3015	インテリジェント ドライブ アレイのコントローラー ステータスは良好です。ステータスは SNMP Varbind 4 に含まれます。
1.3.6.1.4.1.232.0.3015	インテリジェント ドライブ アレイのコントローラー ステータスが障害です。ステータスは SNMP Varbind 4 に含まれます。
1.3.6.1.4.1.232.0.3015	インテリジェント ドライブ アレイのコントローラーにケーブルの問題があります。ステータスは SNMP Varbind 4 に含まれます。
1.3.6.1.4.1.232.0.3015	インテリジェント ドライブ アレイのコントローラーの電源がオフです。ステータスは SNMP Varbind 4 に含まれます。
1.3.6.1.4.1.232.0.3016	スロット内のコントローラーがアクティブになりました。
1.3.6.1.4.1.232.0.3017	インテリジェント ドライブ アレイのスペア ドライブ ステータスが無効です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3017	インテリジェント ドライブ アレイのスペア ドライブ ステータスが非アクティブです。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3017	インテリジェント ドライブ アレイのスペア ドライブ ステータスがアクティブです。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3017	インテリジェント ドライブ アレイのスペア ドライブ ステータスが障害です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3017	インテリジェント ドライブ アレイのスペア ドライブ ステータスが構築中です。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.3018	インテリジェント ドライブ アレイの物理ドライブ ステータスは良好です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3018	インテリジェント ドライブ アレイの物理ドライブ ステータスが障害です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3018	インテリジェント ドライブ アレイの物理ドライブ ステータスが PREDICTIVEFAILURE (障害予測) です。ステータスは SNMP Varbind 3 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3019	インテリジェント ドライブ アレイの物理ドライブがしきい値を超過しました。
1.3.6.1.4.1.232.0.3020	インテリジェント ドライブ アレイのテープ ライブラリ ステータスは良好です。テープ ライブラリのステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3020	インテリジェント ドライブ アレイのテープ ライブラリ ステータスが障害です。テープ ライブラリのステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3020	インテリジェント ドライブ アレイのテープ ライブラリ ステータスが機能低下です。テープ ライブラリのステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3020	インテリジェント ドライブ アレイのテープ ライブラリ ステータスがオフラインです。テープ ライブラリのステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3021	インテリジェント ドライブ アレイのテープ ライブラリのドア ステータスがオープンです。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3021	インテリジェント ドライブ アレイのテープ ライブラリのドア ステータスがクローズです。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3021	インテリジェント ドライブ アレイのテープ ライブラリのドア ステータスが NOT SUPPORTED (サポート外) です。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3022	インテリジェント ドライブ アレイのテープ ドライブ ステータスは良好です。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3022	インテリジェント ドライブ アレイのテープ ドライブ ステータスが機能低下です。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3022	インテリジェント ドライブ アレイのテープ ドライブ ステータスが障害です。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3022	インテリジェント ドライブ アレイのテープ ドライブ ステータスがオフラインです。ステータスは SNMP Varbind 7 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3022	インテリジェント ドライブ アレイのテープ ドライブ ステータスが MISSING WAS OK (現在なし、以前は良好) です。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3022	インテリジェント ドライブ アレイのテープ ドライブ ステータスが MISSING WAS OFFLINE (現在なし、以前はオフライン) です。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3023	インテリジェント ドライブ アレイのテープ ドライブのクリーニングが必要です。
1.3.6.1.4.1.232.0.3024	クリーニング テープの交換が必要です。
1.3.6.1.4.1.232.0.3025	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが無効です。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3025	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが有効です。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3025	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが TEMPORARILY DISABLED (一時的に無効) です。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3025	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが PERMANENTLY DISABLED (完全に無効) です。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3026	インテリジェント ドライブ アレイのアクセラレーターのバッテリ電源が失われました。データ損失の可能性があります。
1.3.6.1.4.1.232.0.3027	インテリジェント ドライブ アレイのアクセラレーター バッテリに障害が発生しました。
1.3.6.1.4.1.232.0.3028	インテリジェント ドライブ アレイのコントローラー ボード ステータスは良好です。ステータスは SNMP Varbind 4 に含まれます。
1.3.6.1.4.1.232.0.3028	インテリジェント ドライブ アレイのコントローラー ボードに障害が発生しました。ステータスは SNMP Varbind 4 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3028	インテリジェント ドライブ アレイのコントローラー ボードにケーブルの問題があります。ステータスは SNMP Varbind 4 に含まれます。
1.3.6.1.4.1.232.0.3028	インテリジェント ドライブ アレイのコントローラー ボードが POWEREDOFF (電源オフ) です。ステータスは SNMP Varbind 4 に含まれます。
1.3.6.1.4.1.232.0.3029	インテリジェント ドライブ アレイの物理ドライブ ステータスは良好です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3029	インテリジェント ドライブ アレイの物理ドライブ ステータスが障害です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3029	インテリジェント ドライブ アレイの物理ドライブ ステータスが PREDICTIVEFAILURE (障害予測) です。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.3030	インテリジェント ドライブ アレイの物理ドライブがしきい値を超過しました。
1.3.6.1.4.1.232.0.3031	インテリジェント ドライブ アレイのテープ ライブラリ ステータスが障害です。テープ ライブラリのステータスは SNMP Varbind 10 に含まれます。
1.3.6.1.4.1.232.0.3031	インテリジェント ドライブ アレイのテープ ライブラリ ステータスは良好です。テープ ライブラリのステータスは SNMP Varbind 10 に含まれます。
1.3.6.1.4.1.232.0.3031	インテリジェント ドライブ アレイのテープ ライブラリ ステータスが機能低下です。テープ ライブラリのステータスは SNMP Varbind 10 に含まれます。
1.3.6.1.4.1.232.0.3031	インテリジェント ドライブ アレイのテープ ライブラリ ステータスがオフラインです。テープ ライブラリのステータスは SNMP Varbind 10 に含まれます。
1.3.6.1.4.1.232.0.3032	インテリジェント ドライブ アレイのテープ ドライブ ステータスは良好です。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3032	インテリジェント ドライブ アレイのテープ ドライブ ステータスがオフラインです。ステータスは SNMP Varbind 7 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3032	インテリジェント ドライブ アレイのテープ ドライブ ステータスが機能低下です。ステータスは SNMP Varbind 7 に含まれます。
1.3.6.1.4.1.232.0.3032	インテリジェント ドライブ アレイのテープ ドライブ ステータスが障害です。ステータスは SNMP Varbind 10 に含まれます。
1.3.6.1.4.1.232.0.3032	インテリジェント ドライブ アレイのテープ ドライブ ステータスが MISSING WAS OK (現在なし、以前は良好) です。ステータスは SNMP Varbind 10 に含まれます。
1.3.6.1.4.1.232.0.3032	インテリジェント ドライブ アレイのテープ ドライブ ステータスが MISSING WAS OFFLINE (現在なし、以前はオフライン) です。ステータスは SNMP Varbind 10 に含まれます。
1.3.6.1.4.1.232.0.3033	インテリジェント ドライブ アレイのコントローラー ステータスが GENERAL FAILURE (一般障害) です。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.3033	インテリジェント ドライブ アレイのコントローラーにケーブルの問題があります。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.3033	インテリジェント ドライブ アレイのコントローラーの電源がオフです。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.3033	インテリジェント ドライブ アレイのコントローラーは良好です。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.3034	インテリジェント ドライブ アレイの論理ドライブ ステータスが未構成です。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3034	インテリジェント ドライブ アレイの論理ドライブ ステータスが QUEUED FOR EXPANSION (拡張キュー登録済み) です。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3034	インテリジェント ドライブ アレイの論理ドライブ ステータスは正常です。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3034	インテリジェント ドライブ アレイの論理ドライブ ステータスが障害です。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3034	インテリジェント ドライブ アレイの論理ドライブ ステータスが回復中です。ステータスは SNMP Varbind 6 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3034	インテリジェント ドライブ アレイの論理ドライブ ステータスが READY for REBUILD (再構築可) です。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3034	インテリジェント ドライブ アレイの論理ドライブ ステータスが再構築中です。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3034	インテリジェント ドライブ アレイの論理ドライブ ステータスが WRONG DRIVE (間違ったドライブ) です。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3034	インテリジェント ドライブ アレイの論理ドライブ ステータスが BAD CONNECTION (接続不良) です。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3034	インテリジェント ドライブ アレイの論理ドライブ ステータスが過熱中です。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3034	インテリジェント ドライブ アレイの論理ドライブ ステータスがシャットダウンです。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3034	インテリジェント ドライブ アレイの論理ドライブ ステータスが拡張中です。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3034	インテリジェント ドライブ アレイの論理ドライブ ステータスが NOT AVAILABLE (利用不可) です。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3035	インテリジェント ドライブ アレイのスペア ドライブ ステータスが無効です。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3035	インテリジェント ドライブ アレイのスペア ドライブ ステータスが非アクティブです。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3035	インテリジェント ドライブ アレイのスペア ドライブ ステータスがアクティブです。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3035	インテリジェント ドライブ アレイのスペア ドライブ ステータスが障害です。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.3035	インテリジェント ドライブ アレイのスペア ドライブ ステータスが構築中です。ステータスは SNMP Varbind 6 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3036	インテリジェント ドライブ アレイの物理ドライブ ステータスは良好です。ステータスは SNMP Varbind 12 に含まれます。
1.3.6.1.4.1.232.0.3036	インテリジェント ドライブ アレイの物理ドライブ ステータスが障害です。ステータスは SNMP Varbind 12 に含まれます。
1.3.6.1.4.1.232.0.3036	インテリジェント ドライブ アレイの物理ドライブ ステータスが PREDICTIVEFAILURE (障害予測) です。ステータスは SNMP Varbind 12 に含まれます。
1.3.6.1.4.1.232.0.3037	インテリジェント ドライブ アレイの物理ドライブがしきい値を超過しました。物理ドライブ インデックスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.3038	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが無効です。ステータスは SNMP Varbind 8 に含まれます。
1.3.6.1.4.1.232.0.3038	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが有効です。ステータスは SNMP Varbind 8 に含まれます。
1.3.6.1.4.1.232.0.3038	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが TEMPORARILY DISABLED (一時的に無効) です。ステータスは SNMP Varbind 8 に含まれます。
1.3.6.1.4.1.232.0.3038	インテリジェント ドライブ アレイのアクセラレーター ボード ステータスが PERMANENTLY DISABLED (完全に無効) です。ステータスは SNMP Varbind 8 に含まれます。
1.3.6.1.4.1.232.0.3039	インテリジェント ドライブ アレイのアクセラレーターのバッテリ電源が失われました。データ損失の可能性があります。
1.3.6.1.4.1.232.0.3040	インテリジェント ドライブ アレイのアクセラレーター バッテリに障害が発生しました。
1.3.6.1.4.1.232.0.3041	インテリジェント ドライブ アレイのテープ ライブラリ ステータスは良好です。テープ ライブラリのステータスは SNMP Varbind 11 に含まれます。
1.3.6.1.4.1.232.0.3041	インテリジェント ドライブ アレイのテープ ライブラリ ステータスが機能低下です。テープ ライブラリのステータスは SNMP Varbind 11 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3041	インテリジェント ドライブ アレイのテープ ライブラリ ステータスが障害です。テープ ライブラリのステータスは SNMP Varbind 11 に含まれます。
1.3.6.1.4.1.232.0.3041	インテリジェント ドライブ アレイのテープ ライブラリ ステータスがオフラインです。テープ ライブラリのステータスは SNMP Varbind 11 に含まれます。
1.3.6.1.4.1.232.0.3042	インテリジェント ドライブ アレイのテープ ライブラリのドア ステータスがオープンです。ステータスは SNMP Varbind 11 に含まれます。
1.3.6.1.4.1.232.0.3042	インテリジェント ドライブ アレイのテープ ライブラリのドア ステータスがクローズです。ステータスは SNMP Varbind 11 に含まれます。
1.3.6.1.4.1.232.0.3042	インテリジェント ドライブ アレイのテープ ライブラリのドア ステータスが NOT SUPPORTED (サポート外) です。ステータスは SNMP Varbind 11 に含まれます。
1.3.6.1.4.1.232.0.3043	インテリジェント ドライブ アレイのテープ ドライブ ステータスが機能低下です。ステータスは SNMP Varbind 11 に含まれます。
1.3.6.1.4.1.232.0.3043	インテリジェント ドライブ アレイのテープ ドライブ ステータスは良好です。ステータスは SNMP Varbind 11 に含まれます。
1.3.6.1.4.1.232.0.3043	インテリジェント ドライブ アレイのテープ ドライブ ステータスが障害です。ステータスは SNMP Varbind 11 に含まれます。
1.3.6.1.4.1.232.0.3043	インテリジェント ドライブ アレイのテープ ドライブ ステータスがオフラインです。ステータスは SNMP Varbind 11 に含まれます。
1.3.6.1.4.1.232.0.3043	インテリジェント ドライブ アレイのテープ ドライブ ステータスが MISSING WAS OK (現在なし、以前は良好) です。ステータスは SNMP Varbind 11 に含まれます。
1.3.6.1.4.1.232.0.3043	インテリジェント ドライブ アレイのテープ ドライブ ステータスが MISSING WAS OFFLINE (現在なし、以前はオフライン) です。ステータスは SNMP Varbind 11 に含まれます。
1.3.6.1.4.1.232.0.3044	インテリジェント ドライブ アレイのテープ ドライブのクリーニングが必要です。
1.3.6.1.4.1.232.0.3045	クリーニング テープの交換が必要です。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.3046	物理ドライブ ステータスは良好です。ステータスは SNMP Varbind 12 に含まれます。
1.3.6.1.4.1.232.0.3046	物理ドライブ ステータスが障害です。ステータスは SNMP Varbind 12 に含まれます。
1.3.6.1.4.1.232.0.3046	物理ドライブ ステータスが PREDICTIVEFAILURE (障害予測) です。ステータスは SNMP Varbind 12 に含まれます。
1.3.6.1.4.1.232.0.3047	スペア ステータスが変更されました。

このポリシーには、これらの各 SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

Rack Information Traps Monitor ポリシー

SI-HPProLiant_CPQRackTraps

SI-HPProLiant_CPQRackTraps ポリシーは、温度、電力、ステータスの観点から、ラック情報に関連する SNMP トラップをインターセプトします。また、トラップが生成されるたびに HPOM コンソールにアラートを送信します。

このポリシーが監視するトラップは以下のとおりです。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.22002	ラック SNMP Varbind 3 のエンクロージャ名が SNMP Varbind 5 に変更されました。
1.3.6.1.4.1.232.0.22003	エンクロージャ SNMP Varbind 5 がラック SNMP Varbind 3 から取り外されました。
1.3.6.1.4.1.232.0.22004	エンクロージャ SNMP Varbind 5 がラック SNMP Varbind 3 に取り付けられました。
1.3.6.1.4.1.232.0.22005	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の温度センサーが障害に設定されました。
1.3.6.1.4.1.232.0.22006	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の温度センサーが機能低下に設定されました。
1.3.6.1.4.1.232.0.22007	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の温度センサーが良好に設定されました。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.22008	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 のファンが障害に設定されました。
1.3.6.1.4.1.232.0.22009	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 のファンが機能低下に設定されました。
1.3.6.1.4.1.232.0.22010	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 のファンが良好に設定されました。
1.3.6.1.4.1.232.0.22011	エンクロージャ SNMP Varbind 5 のファンがラック SNMP Varbind 3 から取り外されました。
1.3.6.1.4.1.232.0.22012	エンクロージャ SNMP Varbind 5 のファンがラック SNMP Varbind 3 に取り付けられました。
1.3.6.1.4.1.232.0.22013	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の電源 SNMP Varbind 7 が障害に設定されました。
1.3.6.1.4.1.232.0.22014	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の電源 SNMP Varbind 7 が機能低下に設定されました。
1.3.6.1.4.1.232.0.22015	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の電源 SNMP Varbind 7 が良好に設定されました。
1.3.6.1.4.1.232.0.22016	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 から、電源 SNMP Varbind 7 が取り外されました。
1.3.6.1.4.1.232.0.22017	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 に、電源 SNMP Varbind 7 が取り付けられました。
1.3.6.1.4.1.232.0.22018	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の電源サブシステムが冗長ではなくなりました。
1.3.6.1.4.1.232.0.22019	ラックの電源が、ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の電源 SNMP Varbind 6 で入力電圧の問題を検出しました。
1.3.6.1.4.1.232.0.22020	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の電源サブシステムが過負荷状態にあります。
1.3.6.1.4.1.232.0.22021	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 のブレード SNMP Varbind 6 で電力不足が発生したため、サーバーがシャットダウンしました。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.22022	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 のブレード SNMP Varbind 6 で、冗長性が維持されないままサーバーの電源がオンになっています。
1.3.6.1.4.1.232.0.22023	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 のブレード SNMP Varbind 6 の電源をオンにするのに十分な電力がありません。
1.3.6.1.4.1.232.0.22024	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 のブレード SNMP Varbind 6 の電源をオンにするのに十分な電力がありません。
1.3.6.1.4.1.232.0.22025	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 のブレード SNMP Varbind 6 の電源をオンにするのに十分な電力がありません。
1.3.6.1.4.1.232.0.22026	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 のブレード SNMP Varbind 6 のマニュアル オーバーライドで、サーバーの電源がオンになりました。
1.3.6.1.4.1.232.0.22027	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 のブレード SNMP Varbind 6 のヒューズが切断しています。
1.3.6.1.4.1.232.0.22028	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の場所 SNMP Varbind 7 から、サーバー ブレード SNMP Varbind 6 が取り外されました。
1.3.6.1.4.1.232.0.22029	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の場所 SNMP Varbind 7 に、サーバー ブレード SNMP Varbind 6 が取り付けられました。
1.3.6.1.4.1.232.0.22030	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の電源サブシステムの負荷が不均衡です。
1.3.6.1.4.1.232.0.22031	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の電源サブシステムの直流電源に問題があります。
1.3.6.1.4.1.232.0.22033	ラック SNMP Varbind 3 で、不明な電力消費があります。
1.3.6.1.4.1.232.0.22032	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の電源サブシステムの交流入力電力が上限を超えました。
1.3.6.1.4.1.232.0.22034	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の電源サブシステムの負荷分散用ワイヤーが存在しません。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.22035	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の電源サブシステムに取り付けられた電源エンクロージャが多すぎます。
1.3.6.1.4.1.232.0.22036	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の電源サブシステムが、適切に構成されていません。
1.3.6.1.4.1.232.0.22037	オンボード アドミニストレーターのステータスが機能低下に設定されました。
1.3.6.1.4.1.232.0.22038	オンボード アドミニストレーターのステータスが良好に設定されました。
1.3.6.1.4.1.232.0.22039	オンボード アドミニストレーターが取り外されました。
1.3.6.1.4.1.232.0.22042	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5、場所 SNMP Varbind 7 にあるブレード Blade SNMP Varbind 6 で、サーバー ブレード E-Keying に障害が発生し、サーバー メザニン カードとインターコネクト間でポート マッピングの問題があります。
1.3.6.1.4.1.232.0.22040	オンボード アドミニストレーターが取り付けられました。
1.3.6.1.4.1.232.0.22041	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 で、オンボード アドミニストレーターがプライマリ ロールを取得しました。
1.3.6.1.4.1.232.0.22043	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の場所 SNMP Varbind 7、サーバー ブレード SNMP Varbind 6 で、サーバー ブレード E-Keying が正常動作に戻りました。
1.3.6.1.4.1.232.0.22044	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の場所 SNMP Varbind 7 のインターコネクト SNMP Varbind 6 で、エンクロージャからインターコネクトが取り外されました。
1.3.6.1.4.1.232.0.22045	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の場所 SNMP Varbind 7 のインターコネクト SNMP Varbind 6 で、エンクロージャにインターコネクトが取り付けられました。
1.3.6.1.4.1.232.0.22046	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の場所 SNMP Varbind 7 のインターコネクト SNMP Varbind 6 で、インターコネクト ステータスが障害に設定されました。
1.3.6.1.4.1.232.0.22047	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の場所 SNMP Varbind 7 のインターコネクト SNMP Varbind 6 で、インターコネクト ステータスが機能低下に設定されました。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.22048	ラック SNMP Varbind 3 に設置されたエンクロージャ SNMP Varbind 5 の場所 SNMP Varbind 7 のインターコネクト SNMP Varbind 6 で、インターコネクト ステータスが良好に設定されました。
1.3.6.1.4.1.232.0.22049	サーバー ブレードが電力の低下を要求しました
1.3.6.1.4.1.232.0.22050	エンクロージャからサーバー ブレードが取り外されました
1.3.6.1.4.1.232.0.22051	エンクロージャにサーバー ブレードが取り付けられました
1.3.6.1.4.1.232.0.22052	cpqRackServerBladeStatusRepaired
1.3.6.1.4.1.232.0.22053	cpqRackServerBladeStatusDegraded
1.3.6.1.4.1.232.0.22054	cpqRackServerBladeStatusCritical
1.3.6.1.4.1.232.0.22055	cpqRackServerBladeGrpCapTimeout
1.3.6.1.4.1.232.0.22056	cpqRackServerBladeUnexpectedShutdown
1.3.6.1.4.1.232.0.22057	cpqRackServerBladeMangementControllerFirmwareUpdating
1.3.6.1.4.1.232.0.22058	cpqRackServerBladeMangementControllerFirmwareUpdateComplete
1.3.6.1.4.1.232.0.22059	cpqRackServerBladeSystemBIOSFirmwareUpdating
1.3.6.1.4.1.232.0.22060	cpqRackServerBladeSystemBIOSFirmwareUpdateCompleted
1.3.6.1.4.1.232.0.22061	cpqRackServerBladeFrontIOBlankingActive
1.3.6.1.4.1.232.0.22062	cpqRackServerBladeRemoteFrontIOBlankingInactive
1.3.6.1.4.1.232.0.22063	cpqRackServerBladeDiagnosticAdaptorInserted
1.3.6.1.4.1.232.0.22064	cpqRackServerBladeDiagnosticAdaptorRemoved
1.3.6.1.4.1.232.0.22064	cpqRackServerBladeDiagnosticAdaptorRemoved
1.3.6.1.4.1.232.0.22065	cpqRackServerBladeEnteredPXEBootMode
1.3.6.1.4.1.232.0.22066	cpqRackServerBladeExitedPXEBootMode
1.3.6.1.4.1.232.0.22067	cpqRackServerBladeWarmReset
1.3.6.1.4.1.232.0.22068	cpqRackServerBladePOSTCompleted
1.3.6.1.4.1.232.0.22069	cpqRackServerBladePoweredOn
1.3.6.1.4.1.232.0.22070	cpqRackServerBladePoweredOff

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.22071	cpqRackInformationalEAETrap
1.3.6.1.4.1.232.0.22072	cpqRackMinorEAETrap
1.3.6.1.4.1.232.0.22073	cpqRackMajorEAETrap
1.3.6.1.4.1.232.0.22074	cpqRackCriticalEAETrap
1.3.6.1.4.1.232.0.22075	cpqRackPowerMinorEAETrap
1.3.6.1.4.1.232.0.22076	cpqRackPowerMajorEAETrap
1.3.6.1.4.1.232.0.22077	cpqRackPowerCriticalEAETrap

このポリシーには、これらの各 SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

UPS Traps Monitor ポリシー

SI-HPProLiant_CPQUPSTraps

SI-HPProLiant_CPQUPSTraps ポリシーは、ステータス、バッテリ、無停電電源装置 (UPS) によって開始された動作の観点から、UPS に関連する SNMP トラップをインターセプトします。また、トラップが生成されるたびに HPOM コンソールにアラートを送信します。

このポリシーが監視するトラップは以下のとおりです。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.12001	UPS は AC 電源に障害が発生したことを報告します。
1.3.6.1.4.1.232.0.12002	UPS は AC 電源が回復したことを報告します。
1.3.6.1.4.1.232.0.12003	UPS はサーバーのシャットダウンを開始しました。
1.3.6.1.4.1.232.0.12004	サーバーは、UPS によるシャットダウンから回復しました。
1.3.6.1.4.1.232.0.12005	UPS バッテリの残量低下により、サーバーへの供給電力が間もなく失われます。
1.3.6.1.4.1.232.0.12006	UPS は AC 電源に障害が発生したことを報告します。
1.3.6.1.4.1.232.0.12007	UPS は AC 電源が回復したことを報告します。
1.3.6.1.4.1.232.0.12008	UPS はサーバーのシャットダウンを開始しました。
1.3.6.1.4.1.232.0.12009	サーバーは、UPS によるシャットダウンから回復しました。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.12010	UPS バッテリの残量低下により、サーバーへの供給電力が間もなく失われます。
1.3.6.1.4.1.232.0.12011	UPS は過負荷状態になりました。
1.3.6.1.4.1.232.0.12012	UPS バッテリに障害の兆候があります。
1.3.6.1.4.1.232.0.12013	cpqUpsGenericCritical
1.3.6.1.4.1.232.0.12014	cpqUpsGenericInfo

このポリシーには、これらの各 SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

Blade Type 2 Traps Monitor ポリシー

SI-HPProLiant_BladeType2Traps

SI-HPProLiant_BladeType2Traps ポリシーは、Blade Type 2 に関連する SNMP トラップをインターセプトします。また、トラップが生成されるたびに HPOM コンソールにアラートを送信します。

このポリシーが監視するトラップは以下のとおりです。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.1	bt2SwPrimaryPowerSupplyFailure
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.35	bt2SwUfdfoLtMUP
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.32	bt2SwFanFailure
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.48	bt2SwHotlinksBackupUp
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.46	bt2SwHotlinksMasterUp
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.17	bt2SwVrrpNewBackup
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.36	bt2SwUfdfoGlobalEna
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.28	bt2SwSaveComplete
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.37	bt2SwUfdfoGlobalDis
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.2	bt2SwDefGwUp
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.47	bt2SwHotlinksMasterDn
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.38	bt2SwUfdfoLtDAutoEna

1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.5	bt2SwDefGwNotInService
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.41	bt2SwCubeRemoved
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.49	bt2SwHotlinksBackupDn
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.27	bt2SwApplyComplete
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.45	bt2SwCistTopologyChanged
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.16	bt2SwVrrpNewMaster
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.40	bt2SwCubeInserted
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.29	bt2SwFwDownloadSucess
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.18	bt2SwVrrpAuthFailure
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.34	bt2SwUfdfoLtMFailure
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.44	bt2SwStgTopologyChanged
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.3	bt2SwDefGwDown
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.4	bt2SwDefGwInService
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.42	bt2SwStgNewRoot
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.50	bt2SwHotlinksNone
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.22	bt2SwTempExceedThreshold
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.31	bt2SwTempReturnThreshold
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.39	bt2SwUfdfoLtDAutoDis
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.30	bt2SwFwDownloadFailure
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.33	bt2SwFanFailureFixed
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.43	bt2SwCistNewRoot
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.26	bt2SwRackLocationChange
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.19	bt2SwLoginFailure

このポリシーには、これらの各 SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

Storage Systems Traps Monitor ポリシー

SI-HPProLiant_CPQSSTraps

SI-HPProLiant_CPQSSTraps ポリシーは、ファンのステータス、温度、電源の観点から、ストレージ システムに関連する SNMP トラップをインターセプトします。また、トラップが生成されるたびに HPOM コンソールにアラートを送信します。

このポリシーが監視するトラップは以下のとおりです。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.8001	ストレージ システム ファン ステータスが良好に変更されました。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.8001	ストレージ システム ファン ステータスが障害に変更されました。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.8001	ストレージ システム ファン ステータスが機能低下に変更されました。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.8001	このユニットではファンの監視はサポートされません。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.8002	ストレージ システムは温度の障害によりシャットダウンします。
1.3.6.1.4.1.232.0.8003	ストレージ システム温度が機能低下になりました。
1.3.6.1.4.1.232.0.8004	ストレージ システム温度は良好です。
1.3.6.1.4.1.232.0.8005	ストレージ システムのサイド パネルがユニットに元通り取り付けられました。
1.3.6.1.4.1.232.0.8006	ストレージ システムのサイド パネルがユニットから取り外されました。
1.3.6.1.4.1.232.0.8007	ストレージ システムの電源ユニットが機能低下になりました。
1.3.6.1.4.1.232.0.8008	ストレージ システム ファン ステータスが良好に変更されました。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.8008	ストレージ システム ファン ステータスが障害に変更されました。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.8008	ストレージ システム ファン ステータスが機能低下に変更されました。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.8008	ストレージ システム ファン ステータスがファンなしに変更されました。ステータスは SNMP Varbind 3 に含まれます。
1.3.6.1.4.1.232.0.8009	ストレージ システム温度で障害が発生しました。
1.3.6.1.4.1.232.0.8010	ストレージ システム温度が機能低下になりました。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.8011	ストレージ システム温度は良好です。
1.3.6.1.4.1.232.0.8012	ストレージ システムのサイド パネルがユニットに元通り取り付けられました。
1.3.6.1.4.1.232.0.8013	ストレージ システムのサイド パネルがユニットから取り外されました。
1.3.6.1.4.1.232.0.8014	ストレージ システムの電源ユニットが機能低下になりました。
1.3.6.1.4.1.232.0.8015	ストレージ システムの電源ユニットが機能低下になりました。
1.3.6.1.4.1.232.0.8016	ストレージ システム ファン ステータスがなしに変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8016	ストレージ システム ファン ステータスが良好に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8016	ストレージ システム ファン ステータスが機能低下に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8016	ストレージ システム ファン ステータスが障害に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8017	ストレージ システムの電源ステータスがなしに変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8017	ストレージ システムの電源ステータスが良好に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8017	ストレージ システムの電源ステータスが障害に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8017	ストレージ システムの電源ステータスが機能低下に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8018	ストレージ システムの電源 UPS ステータスが良好に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8018	ストレージ システムの電源 UPS ステータスが UPS なしに変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8018	ストレージ システムの電源 UPS ステータスが電源障害に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8018	ストレージ システムの電源 UPS ステータスがバッテリ残量低下に変更されました。ステータスは SNMP Varbind 6 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.8019	ストレージ システムの温度センサー ステータスが良好に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8019	ストレージ システムの温度センサー ステータスが機能低下に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8019	ストレージ システムの温度センサー ステータスが障害に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8020	ストレージ システム ファン ステータスが良好に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8020	ストレージ システム ファン ステータスがなしに変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8020	ストレージ システム ファン ステータスが機能低下に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8020	ストレージ システム ファン ステータスが障害に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8021	ストレージ システムの電源ステータスが良好に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8021	ストレージ システムの電源ステータスが障害に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8021	ストレージ システムの電源ステータスがなしに変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8021	ストレージ システムの電源ステータスが機能低下に変更されました。ステータスは SNMP Varbind 6 に含まれます。
1.3.6.1.4.1.232.0.8022	ストレージ システム ファン ステータスが良好に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8022	ストレージ システム ファン ステータスが機能低下に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8022	ストレージ システム ファン ステータスが障害に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8022	ストレージ システム ファン ステータスがサポート対象外に変更されました。ステータスは SNMP Varbind 9 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.8022	ストレージ システム ファン ステータスが degraded-Fan1Failed (機能低下-ファン 1 障害) に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8022	ストレージ システム ファン ステータスが degraded-Fan2Failed (機能低下-ファン 2 障害) に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8023	ストレージ システムの温度ステータスが良好に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8023	ストレージ システムの温度ステータスが機能低下に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8023	ストレージ システムの温度ステータスが障害に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8023	ストレージ システムの温度ステータスが温度なしに変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8023	ストレージ システムの温度ステータスがサポート外に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8024	ストレージ システムの電源ステータスが良好に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8024	ストレージ システムの電源ステータスが機能低下に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8024	ストレージ システムの電源ステータスが障害に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8024	ストレージ システムの電源ステータスが noFltTolPower (耐障害電源なし) に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8024	ストレージ システムの電源ステータスがサポート外に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8024	ストレージ システムの電源ステータスが noFltTolPower-Bay1Missing (耐障害電源なし-ベイ 1 なし) に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8024	ストレージ システムの電源ステータスが noFltTolPower-Bay2Missing (耐障害電源なし-ベイ 2 なし) に変更されました。ステータスは SNMP Varbind 9 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.8024	ストレージ システムの電源ステータスが良好に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.8.0.1	ストレージ システム ファン ステータスが良好に変更されました。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.8.0.1	ストレージ システム ファン ステータスが障害に変更されました。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.8.0.1	ストレージ システム ファン ステータスが機能低下に変更されました。ステータスは SNMP Varbind 1 に含まれます。
1.3.6.1.4.1.232.0.8025	ストレージ システム回復サーバー オプション ステータスが DEAMON DOWN DISABLED (デーモン ダウン無効) に変更されました。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.8025	ストレージ システム回復サーバー オプション ステータスが良好に変更されました。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.8025	ストレージ システム回復サーバー オプション ステータスが DEAMON DOWN ACTIVE (デーモン ダウン アクティブ) に変更されました。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.8025	ストレージ システム回復サーバー オプション ステータスがセカンダリなしに変更されました。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.8025	ストレージ システム回復サーバー オプション ステータスが DEAMON DOWN NOSECONDARY (デーモン ダウン セカンダリなし) に変更されました。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.8025	ストレージ システム回復サーバー オプション ステータスがリンクダウンに変更されました。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.8025	ストレージ システム回復サーバー オプション ステータスが DEAMON DOWN LINKDOWN (デーモン ダウン リンクダウン) に変更されました。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.8025	ストレージ システム回復サーバー オプション ステータスが SECONDARY RUNNING AUTO (セカンダリ実行中、自動制御) に変更されました。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.8025	ストレージ システム回復サーバー オプション ステータスが SECONDARY RUNNING USER (セカンダリ実行中、ユーザー制御) に変更されました。ステータスは SNMP Varbind 5 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.8025	ストレージ システム回復サーバー オプション ステータスが構成なしに変更されました。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.8025	ストレージ システム回復サーバー オプション ステータスがサポート外に変更されました。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.8025	ストレージ システム回復サーバー オプション ステータスが無効に変更されました。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.8025	ストレージ システム回復サーバー オプション ステータスが evTimeOutError (環境変数タイムアウトエラー) に変更されました。ステータスは SNMP Varbind 5 に含まれます。
1.3.6.1.4.1.232.0.8026	ストレージ システム ファン ステータスが良好に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8026	ストレージ システム ファン ステータスが障害に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8026	ストレージ システム ファン ステータスが機能低下に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8026	ストレージ システム ファン ステータスがファンなしに変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8027	ストレージ システムの温度ステータスが機能低下です。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8027	ストレージ システムの温度ステータスが障害です。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8027	ストレージ システムの温度ステータスは良好です。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8027	ストレージ システムの温度ステータスが温度なしに変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8028	ストレージ システムの電源ユニット ステータスが機能低下です。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8028	ストレージ システムの電源ユニット ステータスが障害です。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8028	ストレージ システムの電源ユニット ステータスは良好です。ステータスは SNMP Varbind 9 に含まれます。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.232.0.8028	ストレージ システムの電源ユニット ステータスが noFltTolPower (耐障害電源なし) です。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8029	ストレージ システム ファン ステータスが良好に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8029	ストレージ システム ファン ステータスが障害に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8029	ストレージ システム ファン ステータスが機能低下に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8029	ストレージ システム ファン ステータスがファンなしに変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8030	ストレージ システムの温度ステータスが良好に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8030	ストレージ システムの温度ステータスが機能低下に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8030	ストレージ システムの温度ステータスが障害に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8030	ストレージ システムの温度ステータスが温度なしに変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8031	ストレージ システムの電源ステータスが機能低下に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8031	ストレージ システムの電源ステータスが障害に変更されました。ステータスは SNMP Varbind 9 に含まれます。
1.3.6.1.4.1.232.0.8031	ストレージ システムの電源ステータスが noFltTolPower (耐障害電源なし) に変更されました。ステータスは SNMP Varbind 9 に含まれます。

このポリシーには、これらの各 SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

Virtual Connect Module Traps Monitor ポリシー

SI-HPProLiant_VCModuleTraps

SI-HPProLiant_VCModuleTraps ポリシーは、仮想接続モジュールに関連する SNMP トラップをインターセプトします。また、トラップが生成されるたびに HPOM コンソールにアラートを送信します。

このポリシーが監視するトラップは以下のとおりです。

MIB ID	SNMP トラップの説明
1.3.6.1.4.1.11.5.7.5.2.3.2.11	vcModPortInputUtilizationUp

このポリシーには、この SNMP トラップのルールが含まれています。問題が解決されると、前のアラート メッセージが自動的に確認されます。

SIM Agent Process Monitoring ポリシー

SI-SIMAgentProcessMonitor

SI-SIMAgentProcessMonitor ポリシーは Measurement Threshold ポリシーで、IM エージェントがインストールされているかどうかをチェックします。このポリシーは 5 分ごとに実行され、IM エージェントがアンインストールされているか、ダウンしている場合にメッセージを HPOM コンソールに送信します。

容量ポリシー

容量監視は、要求に合ったサービス レベルとコストでパフォーマンスを提供するのに役立ちます。容量監視を行うことで、IT インフラストラクチャの容量が進化するビジネス ニーズに対応できるようになります。また、使用率が低いリソースや高いリソースを特定するのにも役立ちます。一定の期間にわたってこれらの要素を監視することは、IT リソースの使用率に対する影響を理解する上で役に立ちます。システム リソースの現在のパフォーマンスと履歴データを分析することによって、将来的なニーズを正確に予測することができます。これらのポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Capacity]

Disk Capacity Monitor ポリシー

SI-DiskCapacityMonitor

このポリシーは、管理ノード上のディスクの容量パラメータを監視します。このポリシーは、使用率、使用可能な空き容量、および inode 使用率をディスクごとにチェックします。領域使用率が特定のしきい値を超えるか、下回ると、ポリシーは HPOM コンソールにアラートを送信します。

SI-DiskCapacityMonitorConfig ファイル ポリシー:

SI-DiskCapacityMonitorConfig ファイル ポリシーは、SI-DiskCapacityMonitor 用に作成された設定ファイル ポリシーです。この設定ファイル ポリシーで、以下を指定します。

- 必要なしきい値と共に監視するすべてのファイル システム。
- `osspi_global_fsmon.cfg` ファイルの場所。SI-DiskCapacityMonitor にある Config FilePath スクリプト パラメータにも、同じ場所を入力してください。

SI-DiskCapacityMonitorConfig ファイル ポリシーの配布後に、`osspi_global_fsmon.cfg` ファイルが、SI-DiskCapacityMonitorConfig ファイル ポリシーで指定された場所に、ファイルシステムおよび

指定されたしきい値と共に作成されます (存在しない場合)。osspi_global_fsmon.cfg ファイルが存在する場合、そのファイルは、配布される SI-DiskCapacityMonitorConfig ファイル ポリシーに記載されているファイルシステムとしきい値で上書きされます。

Fsmon 機能を使用すると、ファイルシステムを監視し、定義されているしきい値に基づいてアラート メッセージを送信できます。このポリシーは、次の設定ファイルにリストされているファイルシステムを読み取ります。

- osspi_fsmon.cfg
- osspi_global_fsmon.cfg
- osspi_local_fsmon.cfg

注:

osspi_fsmon.cfg は、/var/opt/OV/conf/osspi/osspi_fsmon.cfg に格納されています。

osspi_global_fsmon.cfg ファイルは、好ましい場所に作成して、GlobalConfigFilePath スクリプト パラメータでそのパスを指定することができます。

osspi_local_fsmon.cfg ファイルは、好ましい場所に作成して、LocalConfigFilePath スクリプト パラメータでそのパスを指定することができます。

注: osspi_fsmon.cfg は、OSSPI をインストールした場合にのみ利用可能です。

デフォルトの設定ファイル osspi_fsmon.cfg は、編集しないでください。

osspi_fsmon.cfg ファイルを変更または上書きするには、osspi_global_fsmon.cfg ファイルを使用します。

osspi_global_fsmon.cfg ファイルを変更または上書きするには、osspi_local_fsmon.cfg ファイルを使用します。

OSSPI をインストールした場合、設定ファイルのプリファレンスの順序は次のようになります。

デフォルト osspi_fsmon.cfg > グローバル osspi_global_fsmon.cfg > ローカル osspi_local_fsmon.cfg。

OSSPI をインストールしなかった場合、設定ファイルのプリファレンスの順序は次のようになります。

グローバル osspi_global_fsmon.cfg > ローカル osspi_local_fsmon.cfg。

このポリシーは、すべてのスクリプト パラメータのデフォルト値、および「*」や「?」などのワイルドカード文字をサポートします。詳細については、「すべてのスクリプト パラメータに対するワイルドカード文字の使用」および「すべてのスクリプト パラメータに対するデフォルト値の使用」を参照してください。

使用するメトリック	FS_MAX_SIZE FS_SPACE_USED FS_SPACE_UTIL FS_TYPE FS_DIRNAME FS_SPACE_RESERVED FS_INODE_UTIL
サポートされているプラットフォーム	Microsoft Windows Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM AIX Oracle Solaris Debian Ubuntu
スクリプト パラメータ	**説明**
SpaceUtilCriticalThreshold	このしきい値には、ディスクの使用済み容量を指定します。危険域メッセージを受信する基準となるしきい値を設定します。
SpaceUtilMajorThreshold	重要危険域メッセージを受信する基準となるしきい値を設定します。
SpaceUtilMinorThreshold	警戒域メッセージを受信する基準となるしきい値を設定します。
SpaceUtilWarningThreshold	注意域メッセージを受信する基準となるしきい値を設定します。
FreeSpaceCriticalThreshold	このしきい値には、ディスクまたはファイル システムで使用可能な空き容量 (MB 単位) を指定します。ディスクの空き容量の最小値にしきい値を設定します。しきい値を下回ると、危険域メッセージが受信されます。
FreeSpaceMajorThreshold	ディスクの空き容量の最小値にしきい値を設定します。しきい値を下回ると、重要警戒域メッセージが受信されます。
FreeSpaceMinorThreshold	ディスクの空き容量の最小値にしきい値を設定します。しきい値を下回ると、警戒域メッセージが受信されます。

FreeSpaceWarningThreshold	ディスクの空き容量の最小値にしきい値を設定します。しきい値を下回ると、注意域メッセージが受信されます。
InodeUtilCriticalThreshold	しきい値は、ファイルシステムのインデックス ノード (inode) 使用率で表され、UNIX にのみ使用可能です。危険域メッセージを受信する基準となるしきい値を設定します。
InodeUtilMajorThreshold	重要危険域メッセージを受信する基準となるしきい値を設定します。
InodeUtilMinorThreshold	警戒域メッセージを受信する基準となるしきい値を設定します。
InodeUtilWarningThreshold	注意域メッセージを受信する基準となるしきい値を設定します。
MessageGroup	送信メッセージのメッセージ グループ。**OS** は、このポリシーからのすべてのアラートのデフォルトのメッセージ グループです。異なるファイル システムに対して別のメッセージ グループを指定することもできます。例については、メッセージ グループの例を参照してください。
ExcludeFilesystems	監視から除外するファイルシステムまたはファイルシステムのタイプを指定します。ファイルシステムとファイルシステムのタイプの両方が指定されている場合、ファイルシステムのタイプがファイルシステムより優先されます。
Debug	トレース メッセージを無効にするには、この値を **0** に設定します。コンソールでトレース メッセージを受信するには **1**、管理ノードのトレース ファイルにメッセージを記録するには **2** に設定します。詳細については、「トレース」(22ページ)を参照してください。
UseFsmonConfigSettings	**Fsmon** 設定ベースのしきい値を有効にするには、TRUE に設定します。 **注:** 定義されている各しきい値に対して、連続生成アクションを有効にしてください。 SI-DiskCapacitiyMonitor ポリシーのデフォルトの動作を有効にするには、False に設定します。
GlobalConfigFilePath	`fsmon global` 設定ファイルのパスを設定します。
LocalConfigFilePath	`fsmon local` 設定ファイルのパスを設定します。

管理ノード上のドライブまたはファイル システムに複数のしきい値を設定することができます。しきい値を複数設定する場合には、ポリシー パラメータをカンマで区切ります。次に、いくつかの例を示します。

- **FreeSpaceMinorThreshold=45**

  管理ノード上にあるすべてのディスクまたはファイル システムについて、45 MB をしきい値として設定します。ディスクまたはファイル システムの空き容量がこのしきい値を下回ると、ポリシーは重要度が警戒域のメッセージを送信します。

- **SpaceUtilCriticalThreshold=80,/=65,c:=65**

  管理ノード上で、'/' ドライブと 'C:' ドライブには 65%、その他のドライブ/ファイル システムには 80% をしきい値として設定しています。ディスク/ファイル システムの使用率がこのしきい値を超えると、ポリシーは重要度が危険域のメッセージを送信します。

- **FreeSpaceMajorThreshold=256,E:=200,F:=512,c:=1024,/=1024**

  管理ノード上で、'E:' ドライブには 200、'F:' ドライブには 512、'C:' ドライブには 1024、'/' ドライブには 1024、その他ドライブには 256 をしきい値として設定します。空き容量がこのしきい値を下回ると、ポリシーは重要警戒域メッセージを送信します。

設定ファイルの構文

ファイル システムは、次の図に示すように設定ファイルに入力されます。

```
/var    80/,85/,90/,95/ OS_Linux        ORA
/tmp    80,85,90,95
/usr    /80,/85,/90,/95
/opt    80/70,85/75,90/80,95/85 OS_Linux        ORA
```

スクリーンショットにマークされているインスタンスの場合、次のようになります。

/usr	ファイル システム
80	警告しきい値
85	警戒域しきい値
90	重要警戒域しきい値
95	危険域しきい値
,	しきい値を区切るために使用

次に、ファイル システムとそのしきい値を定義するために使用される構文を示します。

カラム 1	カラム 2	カラム 3	カラム 4	カラム 5
File systems	注意域	警戒域	重要警戒域	危険域

注: SI-DiskCapacityMonitorConfig ファイル ポリシーでは、ファイルシステムとしきい値は、タブ スペース 1 つで区切り、しきい値はコンマで区切る必要があります。

しきい値テーブル	
n/m	スペース (n) と inode (m) に別々の限度あり
n/	スペースに限度あり、inode に限度なし
/m	スペースに限度なし、inode に限度あり
n	スペースと inode に同じ限度あり

すべてのスクリプト パラメータに対するワイルドカード文字「*」と「?」の使用

1 つ以上の文字との一致には、「*」を使用し、正確に 1 つの文字との一致には、「?」を使用します。次に、いくつかの例を示します。

- **ExcludeFilesystems=/,/boot,/v*/?log**

  この例では、ファイルシステムの「/」、「/boot」およびパターン「/v*/?log」に一致する「/var/vlog」などのファイルシステムが監視から除外されます。

  次の例では、ファイル システムのワイルドカード文字の使用方法を示します。

  - **/var/*** は、**/var/l**、**/var/log**、**/var/log/tmp** という名前のファイルシステムと一致します。
  - **/var/?** は、**/var/a**、**/var/b** という名前のファイルシステムと一致しますが、**/var/abc**、**/var/xyzh** という名前のファイルシステムとは一致しません。
  - **/var/??log** は、**/var/ablog**、**/var/fslog** という名前のファイルシステムと一致しますが、**/var/alog**、**/var/log** という名前のファイルシステムとは一致しません。
  - **/var*/?log** は、**<b>var1/alog**、**/var123/blog** という名前のファイルシステムと一致しますが、**/var/log**、**/var123/log**、**/var/1log** という名前のファイルシステムとは一致しません。

すべてのスクリプト パラメータに対するデフォルト値の使用

すべてのスクリプト パラメータにデフォルト値を使用します。ポリシーは、ファイル システム名をオーバーライドせずに、デフォルト値がある場合にのみ動作します。次に、いくつかの例を示します。

- **SpaceUtilMinorThreshold=80,/=30,/boot=40**

  この例では、30 が「/」のしきい値で、40 が「/boot」のしきい値であり、80 が残りのファイルシステムのデフォルトのしきい値になります。

- **SpaceUtilMinorThreshold=/=30**

  この例で指定されているパラメータは正しくありません。常にデフォルト値を指定する必要があります。

- **MessageGroup=OS,/tmp=unix_admin,/ora/*=dba,/var/log?=unix_admin**

  この例では次のようになります。

unix_admin は、**tmp** ファイルシステムに対して生成されるアラートに割り当てられるメッセージ グループです。

dba は、**/ora/** で始まり、その後に 1 文字以上が続くファイルシステムに対して生成されるアラートに割り当てられるメッセージ グループです。

unix_admin は、**/var/log** で始まり、その後にちょうど 1 文字が続くファイルシステムに対して生成されるアラートに割り当てられるメッセージ グループです。

OS は、上記以外のファイルシステムに対して生成されるアラートに割り当てられるメッセージ グループです。

注: このポリシーのしきい値は、整数または 10 進数 (小数点の右側が最大 2 桁) に設定する必要があります。

SI-SwapCapacityMonitor

このポリシーは、システム上のスワップ領域の使用率を監視します。

使用するメトリック	GBL_SWAP_SPACE_AVAIL GBL_SWAP_SPACE_UTIL
サポートされているプラットフォーム	Microsoft Windows Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM AIX Oracle Solaris
スクリプト パラメータ	**説明**
SwapSpaceUtilCriticalThreshold	このしきい値は、ノード上のスワップ領域の使用率をパーセンテージ (0 ~ 100%) で指定します。ディスク上にある空きスワップ領域の最小値にしきい値を設定します。しきい値を下回ると、重要度が危険域のメッセージが受信されます。
SwapSpaceUtilMajorThreshold	ノード上の使用済みスワップ領域の最小値にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
SwapSpaceUtilMinorThreshold	ノード上の使用済み容量の最小値にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。

SwapSpaceUtilWarningThreshold	ノード上の使用済み容量の最小値にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
FreeSwapSpaceAvailCriticalThreshold	このしきい値には、ディスク/ファイル システムで使用可能な空きスワップ領域 (MB 単位) を指定します。ディスク上にある空き領域の最小値にしきい値を設定します。しきい値を下回ると、重要度が危険域のメッセージが受信されます。
FreeSwapSpaceAvailMajorThreshold	ディスク上にある空きスワップ領域の最小値にしきい値を設定します。しきい値を下回ると、重要度が重要警戒域のメッセージが受信されます。
FreeSwapSpaceAvailMinorThreshold	ディスク上にある空きスワップ領域の最小値にしきい値を設定します。しきい値を下回ると、重要度が警戒域のメッセージが受信されます。
FreeSwapSpaceAvailWarningThreshold	ディスク上にある空きスワップ領域の最小値にしきい値を設定します。しきい値を下回ると、重要度が注意域のメッセージが受信されます。
MessageGroup	送信メッセージのメッセージ グループ。
Debug	トレース メッセージを無効にするには、この値を **0** に設定します。コンソールでトレース メッセージを受信するには **1**、管理ノードのトレース ファイルにメッセージを記録するには **2** に設定します。詳細については、「トレース」(22ページ)を参照してください。

Remote Drive Space Utilization Monitor ポリシー

SI-MSWindowsRemoteDriveSpaceUtilization

SI-MSWindowsRemoteDriveSpaceUtilization ポリシーは、Microsoft Windows プラットフォーム上にあるリモート ドライブの容量の使用率レベルを監視します。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Capacity] → [Windows]

ソース タイプ	WMI
サポートされているプラットフォーム	Microsoft Windows
スクリプト パラメータ	**説明**

SpaceUtilCriticalThreshold	このしきい値には、監視対象のリモート ドライブの容量の使用率をパーセンテージ (0 ~ 100%) で指定します。ドライブ上にある空き領域の最小値にしきい値を設定します。この値に達すると、重要度が危険域のメッセージが受信されます。
SpaceUtilMajorThreshold	ドライブ上にある空き領域の最小値にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
SpaceUtilMinorThreshold	ドライブ上にある空き領域の最小値にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。
SpaceUtilWarningThreshold	ドライブ上にある空き領域の最小値にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
MessageGroup	送信メッセージのメッセージ グループ。
Debug	トレース メッセージを無効にするには、この値を **0** に設定します。コンソールでトレース メッセージを受信するには **1**、管理ノードのトレース ファイルにメッセージを記録するには **2** に設定します。詳細については、「トレース」(22ページ)を参照してください。
AssignMessageToRemoteHost	アラート メッセージの送信元をリモート ホストとして表示するには、この値を 1 に設定します。デフォルトでは、メッセージはメッセージの送信元の管理ノードに割り当てられます。

NFS ファイル システム用の Remote Drive Space Utilization Monitor ポリシー

SI-LinuxNfsUtilizationMonitor

SI-LinuxNfsUtilizationMonitor ポリシーは、Linux プラットフォーム上にある NFS リモート ファイル システムの容量の使用率レベルを監視します。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Capacity] → [Linux]

サポートされているプラットフォーム	Red Hat Enterprise Linux Suse Linux Enterprise Server

スクリプト パラメータ	説明
SpaceUtilCriticalThreshold	このしきい値には、監視対象のリモート ファイル システムの容量の使用率をパーセンテージ (0 ~ 100%) で指定します。ファイル システム上にある空き領域の最小値にしきい値を設定します。この値に達すると、重要度が危険域のメッセージが受信されます。
SpaceUtilMajorThreshold	ファイルシステム上にある空き領域の最小値にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
SpaceUtilMinorThreshold	ファイルシステム上にある空き領域の最小値にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。
SpaceUtilWarningThreshold	ファイルシステム上にある空き領域の最小値にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
NfsFileSystemType	容量の使用率を監視する対象となるファイル システムのタイプを指定します。たとえば、NFS と指定すると、すべての NFS リモート ファイル システムが容量使用率監視の対象になります。
AssignMessageToRemoteHost	アラート メッセージの送信元をリモート ホストとして表示するには、この値を 1 に設定します。デフォルトでは、メッセージはメッセージの送信元の管理ノードに割り当てられます。
MessageGroup	送信メッセージのメッセージ グループ。
Debug	トレース メッセージを無効にするには、この値を **0** に設定します。コンソールでトレース メッセージを受信するには **1**、管理ノードのトレース ファイルにメッセージを記録するには **2** に設定します。詳細については、「トレース」(22ページ)を参照してください。

CIFS ファイル システム用の Remote Drive Space Utilization Monitor ポリシー

SI-LinuxCifsUtilizationMonitor

SI-LinuxCifsUtilizationMonitor ポリシーは、Linux プラットフォーム上にある CIFS リモート ファイルシステムの容量の使用率レベルを監視します。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Capacity] → [Linux]

サポートされているプラットフォーム	Red Hat Enterprise Linux Suse Linux Enterprise Server
スクリプト パラメータ	**説明**
SpaceUtilCriticalThreshold	このしきい値には、監視対象のリモート ファイル システムの容量の使用率をパーセンテージ (0 ~ 100%) で指定します。ファイル システム上にある空き領域の最小値にしきい値を設定します。この値に達すると、重要度が危険域のメッセージが受信されます。
SpaceUtilMajorThreshold	ファイルシステム上にある空き領域の最小値にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
SpaceUtilMinorThreshold	ファイルシステム上にある空き領域の最小値にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。
SpaceUtilWarningThreshold	ファイルシステム上にある空き領域の最小値にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
CifsFileSystemType	容量の使用率を監視する対象となるファイル システムのタイプを指定します。たとえば、CIFS と指定すると、すべての CIFS リモート ファイル システムが容量使用率監視の対象になります。このポリシーで監視できるファイルシステムのタイプは、cifs と smb です。
AssignMessageToRemoteHost	アラート メッセージの送信元をリモート ホストとして表示するには、この値を 1 に設定します。デフォルトでは、メッセージはメッセージの送信元の管理ノードに割り当てられます。
MessageGroup	送信メッセージのメッセージ グループ。
Debug	トレース メッセージを無効にするには、この値を **0** に設定します。コンソールでトレース メッセージを受信するには **1**、管理ノードのトレース ファイルにメッセージを記録するには **2** に設定します。詳細については、「トレース」(22ページ)を参照してください。

Paged and Nonpaged Pool Utilization ポリシー

SI-MSWindowsPagedPoolUtilization と **SI-MSWindowsNonPagedPoolUtilization**

SI-MSWindowsPagedPoolUtilization ポリシーは、レジストリ データがページング ファイルに書き込まれるときのメモリを監視します。SI-MSWindowsNonPagedPoolUtilization ポリシーは、システムが

ページ フォールトを処理できないときにデータを格納するメモリを監視します。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Capacity] → [Windows]

使用するメトリック	GBL_MEM_PAGED_POOL_BYTES GBL_MEM_NONPAGED_POOL_BYTES
サポートされているプラットフォーム	Microsoft Windows
スクリプト パラメータ	**説明**
BaselinePeriod	ベースライン期間として定義する時間を入力します (例: 900 秒)。現在の時間から遡って、この時間が現在の基準として使用されます。過去 900 秒が現在のベースライン期間になります。
WarningDeviations	正常値からの標準偏差の数であり、この値に達するとポリシーは HPOM コンソールに注意域メッセージを送信します。このパラメータに適切な値を設定します。パラメータを無効にするには、この値を 4.5 に設定します。
MinorDeviations	正常値からの標準偏差の数であり、この値に達するとポリシーは HPOM コンソールに警告域メッセージを送信します。このパラメータには、WarningDeviations に指定した値より大きい適切な値を設定します。パラメータを無効にするには、この値を 5.5 に設定します。
MajorDeviations	正常値からの標準偏差の数であり、この値に達するとポリシーは HPOM コンソールに重要危険域メッセージを送信します。このパラメータには、MinorDeviations に指定した値より大きい適切な値を設定します。パラメータを無効にするには、この値を 7.5 に設定します。

ログ監視ポリシー

SI SPI では、管理ノードの重要なログを監視するために、ログ ファイル ポリシーが用意されています。これらのポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Logs]

Linux システム サービス ログ ファイル ポリシー

Linux システム サービス ログ ファイル ポリシーは、Red Hat および Suse Enterprise Linux エディションの重要なシステム サービス ログを監視します。これらのポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Logs] → [Linux]

Boot Log ポリシー

SI-LinuxBootLog

このポリシーは、ブート ログファイル /var/log/boot.log と、システム ブート エラー発生時のアラートを監視します。デフォルトのポーリング間隔は 5 分です。

このポリシーは、以下の条件をチェックします。

条件	説明
サービスの起動に失敗	ブート ログ ファイルに、[<*> <@.service>:<@.daemon> の起動に失敗] のパターンと一致するエラー条件があるかどうかをチェックします。一致が見つかった場合、適切なメッセージ属性と共に重要度が警戒域のメッセージが HPOM コンソールに送信されます。
サービスの失敗	ブート ログ ファイルに、[<*> <@.service>:<*.msg> に失敗] のパターンと一致するエラー条件があるかどうかをチェックします。一致が見つかった場合、適切なメッセージ属性と共に重要度が危険域のメッセージが HPOM コンソールに送信されます。

Secure Log ポリシー

SI-LinuxSecureLog

このポリシーは、/var/log/secure および /var/log/messages 内のログ ファイルと、セキュリティで保護されたログインでのエラー発生時のアラートを監視します。デフォルトのポーリング間隔は 5 分です。

このポリシーは、以下の条件をチェックします。

条件	説明
認証の失敗	セキュリティで保護されたログインのファイルに、[<*> sshd\[<#>\]:<*.host> ポート <#> ssh2 からの <@.user> のパスワードが失敗] のパターンと一致するエラー条件があるかどうかをチェックします。一致が見つかった場合、適切なメッセージ属性と共に重要度が警戒域のメッセージが HPOM コンソールに送信されます。

Kernel Log ポリシー

SI-LinuxKernelLog

このポリシーは、カーネル ログ ファイル /var/log/messages と、カーネル サービスでのエラー発生時のアラートを監視します。デフォルトのポーリング間隔は 5 分です。

このポリシーは、以下の条件をチェックします。

条件	説明
カーネル サービスの失敗	カーネル ログ ファイルに、[<*> kernel:<@.service>:<*.msg> が失敗] のパターンと一致するエラー条件があるかどうかをチェックします。一致が見つかった場合、適切なメッセージ属性と共に重要度が警戒域のメッセージが HPOM コンソールに送信されます。

Windows システム サービス ログ ファイル ポリシー

Windows Server logfile ポリシーは、Microsoft Windows 2008 以降のバージョンで使用される重要なシステム サービス ログを監視します。これらのポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Logs] → [MS Windows Server]

NFS Log ポリシー

SI-MSWindowsServer_NFSWarnError

このポリシーは、NFS サーバー プロセスの NFS ログ ファイルを監視し、エラーのログ エントリを、注意域またはエラーの重要度レベルで HPOM コンソールに転送します。デフォルトのポーリング間隔は 1 分です。このポリシーは、NFS ログ ファイルに記録されている以下のエラーを検索します。

- 空き領域が不足しているため、NFS サーバーは、監査の記録を停止しました
- 監査ログが最大ファイル サイズに達しました
- NFS サーバーは、RPC ポート マッパーに登録できませんでした
- サーバーはフェーズ 2 の初期化中に NFS ドライバからエラーを受信しました

DNS Log ポリシー

SI-MSWindowsServer_DNSWarnError

このポリシーは、Microsoft DNS サーバー サービスと関連プロセスのログ ファイルを監視し、エラーのログ エントリを、注意域またはエラーの重要度レベルで HPOM コンソールに転送します。デフォルトのポーリング間隔は 1 分です。このポリシーは、DNS ログ ファイルに記録されている以下のエラーを検索します。

- DNS サーバーは、リソース レコード用にメモリを割り当てることができませんでした
- DNS サーバーは、利用可能なメモリが不足していたためクライアント要求を処理できませんでした
- DNS サーバーは、ゾーン転送スレッドを作成できませんでした
- DNS サーバーにファイル書き込みエラーが発生しました
- DNS サーバーは、リモート プロシージャ コール (RPC) サービスを初期化できませんでした

Windows Logon ポリシー

SI-MSWindowsServer_WindowsLogonWarnError

このポリシーは、Windows ログオンおよび初期化のイベント ログを監視し、エラーのログ エントリを、注意域またはエラーの重要度レベルで HPOM コンソールに転送します。デフォルトのポーリング間隔は 1 分です。このポリシーは、Windows ログ ファイルに記録されている以下のエラーを検索します。

- Windows のライセンスが無効です
- Windows のライセンス認証の手続きが失敗しました
- Windows のログオン プロセスによって、デスクトップを切り替えることができませんでした
- Windows のログオン プロセスは予期しない原因により終了しました
- Windows のログオン プロセスは、ユーザー アプリケーションを起動できませんでした
- Windows のログオン プロセスは、現在ログオンしているユーザーのプロセスを終了できませんでした
- Windows のログオン プロセスは、ユーザー セッションを切断できませんでした

Terminal Service Log ポリシー

SI-MSWindowsServer_TerminalServiceWarnError

このポリシーは、Windows ターミナル サービスと関連プロセスのログ ファイルを監視し、エラーのログ エントリを、注意域またはエラーの重要度レベルで HPOM コンソールに転送します。デフォルトのポーリング間隔は 1 分です。このポリシーは、Windows Terminal サービス ログ ファイルに記録されている以下のエラーを検索します。

- ターミナル サーバーは現在接続を受け入れないように構成されているため、接続要求が拒否されました
- 認証に失敗したため、ユーザーをセッションに再接続できませんでした
- ターミナル サービスの起動に失敗しました
- ターミナル サーバーは多数の不完全な接続を受信しました

Windows Server DHCP

SI-MSWindowsServer_DHCPWarnError

このポリシーは、DHCP サーバーおよびクライアント サービス、関連プロセスのログ ファイルを監視し、エラーのログ エントリを、注意域またはエラーの重要度で HPOM コンソールに転送します。デフォルトのポーリング間隔は 1 分です。このポリシーは、Windows Terminal サービス ログ ファイルに記録されている以下のエラーを検索します。

- `Iashlpr` が NPS サービスと通信できません
- スコープまたはスーパースコープの BOOTP クライアントに使用できる IP アドレスはありません

- DHCP サーバーが、クライアントの NAP アクセス状態を判定するために NPS サーバーにアクセスできません
- スコープまたはスーパースコープのリースに使用できる IP アドレスはありません
- ローカル コンピューターの DHCP/BINL サービスは、起動権限がないと判断しました
- DHCP サービスは監査ログを初期化できませんでした
- このワークグループ サーバーの DHCP/BINL サービスは、次の IP アドレスの別のサーバーを検出しました
- DHCP サービスはレジストリ構成の復元に失敗しました
- DHCP サービスはレジストリからグローバル BOOTP ファイル名を読み取ることができませんでした
- アクティブなインターフェイスがないため、DHCP サービスはクライアントにサービスを提供していません
- DHCP サーバーにバインドされた静的 IP アドレスがありません
- DHCP サーバー サービスがサービス コントローラーへの登録に失敗しました
- DHCP サーバー サービスがレジストリ パラメータの初期化に失敗しました

AIX システム ログ ファイル監視ポリシー

AIX システム ログ ファイル監視ポリシーは、重大なシステム障害を監視します。

ERRPT Log Monitoring ポリシー

SI-AIXErrptLog

「errpt」コマンドの出力は、`errpt.log` ファイルにシステム エラーとして保存されます。SI-AIXErrptLog ポリシーはログ ファイルを監視し、重要度が注意域のメッセージとしてログ エントリを HPOM コンソールに送信します。この警告には、エラー コード、クラス、機能停止が含まれます。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Logs] → [AIX]

パフォーマンス ポリシー

パフォーマンス監視により、パフォーマンス低下を阻止したり、インフラストラクチャの問題によってサービス品質が低下する可能性がある状況を特定できます。収集したパフォーマンス データを元に、サーバー、オペレーティング システム、ネットワーク デバイス、アプリケーションなどインフラストラクチャ全体で発生しているイベントとの相関関係を把握することによって、パフォーマンスの問題の根本原因を解消または特定することができます。

これらのポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Performance]

Network Usage and Performance ポリシー

SI-NetworkUsageAndPerformance

このポリシーは、システムのネットワーク使用率を監視し、エラー率、競合率、バイト率、および送信キューの長さを表示することによって、潜在的なネットワーク ボトルネックを特定します。SI-NetworkUsageAndPerformance ポリシーは、vMA マシンのみの物理 NIC を監視します。

Windows オペレーティング システムでは、BYNETIF_COLLISION メトリックを使用できないため、このポリシーでパッケージ競合に関するパフォーマンス データを監視することはできません。

注: このポリシーで使用する BYNETIF_UTIL メトリックと BYNETIF_QUEUE メトリックを参照するためには、管理ノード上で HP Performance Agent を実行する必要があります。

使用するメトリック	BYNETIF_IN_PACKET BYNETIF_ID BYNETIF_OUT_PACKET BYNETIF_ERROR BYNETIF_COLLISION BYNETIF_OUT_BYTE_RATE BYNETIF_IN_BYTE_RATE BYNETIF_UTIL BYNETIF_QUEUE BYNETIF_NAME BYNETIF_NET_TYPE
サポートされているプラットフォーム	Microsoft Windows Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM AIX Oracle Solaris Debian Ubuntu スクリプト パラメータは、各パラメータの説明で特に指定がない場合、上記のプラットフォームすべてで使用できます。

スクリプト パラメータ	説明
NICByteRateCriticalThreshold	このパラメータは、1 秒あたりの転送バイト数の平均値を監視し、この値がしきい値を超えた場合は、重要度が危険域のメッセージを送信します。メッセージを受信する基準となるしきい値を設定できます。
NICByteRateMajorThreshold	1 秒あたりに転送される平均バイト数にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
NICByteRateMinorThreshold	1 秒あたりに転送される平均バイト数にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。
NICByteRateWarningThreshold	1 秒あたりに転送される平均バイト数にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
NICErrPktRatePctCriticalThreshold	パケット エラー率とは、送信に失敗したパケット数を、送信パケットの総数に対する比率 (パーセント) で示したものです。このパラメータは、パケット エラー率を監視し、この値がしきい値を超えた場合は、重要度が危険域のメッセージを送信します。
NICErrPktRatePctMajorThreshold	パケット エラー率にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
NICErrPktRatePctMinorThreshold	パケット エラー率にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。
NICErrPktRatePctWarningThreshold	パケット エラー率にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
NICCollisionRatePctCriticalThreshold	このパラメータは、送信パケットの総数に対する競合パケットの比率 (パーセンテージ) を監視します。競合率にしきい値を設定します。この値に達すると、重要度が危険域のメッセージが受信されます。 このパラメータは、Windows では使用できません。

NICCollisionRatePctMajorThreshold	競合率にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。 このパラメータは、Windows では使用できません。
NICCollisionRatePctMinorThreshold	競合率にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。 このパラメータは、Windows では使用できません。
NICCollisionRatePctWarningThreshold	競合率にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。 このパラメータは、Windows では使用できません。
NICOutBoundQueueLengthCriticalThreshold	このパラメータは、すべてのネットワーク インターフェイスを対象に、送信キュー内で待機するパケット数を示します。送信キューの長さにしきい値を設定すると、このしきい値に達した時点で、重要度が危険域のメッセージが受信されます。 このパラメータは、HP-UX と Windows では使用できません。
NICOutBoundQueueLengthMajorThreshold	送信キューの長さにしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。 このパラメータは、HP-UX と Windows では使用できません。
NICOutBoundQueueLengthMinorThreshold	送信キューの長さにしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。 このパラメータは、HP-UX と Windows では使用できません。
NICOutBoundQueueLengthWarningThreshold	送信キューの長さにしきい値を設定すると、しきい値に達した時点で、重要度が注意域のメッセージが受信されます。 このパラメータは、HP-UX と Windows では使用できません。

NICBandwidthUtilCriticalThreshold	このパラメータは、使用可能な総帯域幅に対する使用済み帯域幅の比率 (パーセンテージ) を示します。帯域幅の使用率にしきい値を設定すると、このしきい値に達した時点で、重要度が危険域のメッセージが受信されます。 このパラメータは、HP-UX、AIX、Windows で使用できます。
NICBandwidthUtilMajorThreshold	帯域幅の使用率にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。 このパラメータは、HP-UX、AIX、Windows で使用できます。
NICBandwidthUtilMinorThreshold	帯域幅の使用率にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。 このパラメータは、HP-UX、AIX、Windows で使用できます。
NICBandwidthUtilWarningThreshold	帯域幅の使用率にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。 このパラメータは、HP-UX、AIX、Windows で使用できます。
NICThresholdMultiplier	このパラメータを使用して、高帯域幅ネットワークカードを処理するためのしきい値を因子 X だけ増加させます。パラメータを明示的に指定していない場合、乗数値が自動的に計算されます。
MessageGroup	このポリシーによって管理コンソールに送信されるメッセージを特定できるように、わかりやすい値を指定してください。しきい値の違反が発生すると、このポリシーは、パラメータの値をメッセージに付加してから管理コンソールに送信します。
Debug	トレース メッセージを無効にするには、この値を **0** に設定します。コンソールでトレース メッセージを受信するには **1**、管理ノードのトレース ファイルにメッセージを記録するには **2** に設定します。詳細については、「トレース」(22ページ)を参照してください。

注: このポリシーのしきい値は、デフォルト値として指定できます。また、個別のネットワーク インターフェイス名、ネットワーク インターフェイス タイプ、またはこの両方として指定することもできます。1 つのパラメータにネットワーク インターフェイス名とネットワーク インターフェイス タイプの両方を指定した場合、ネットワーク インターフェイス タイプがネットワーク インターフェイス名より優先されます。

スクリプト パラメータに対するワイルドカード文字「*」の使用

複数の NIC 名を指定する場合、1 つ以上の文字との一致には、「*」を使用できます。

例: **NICBandwidthUtilWarningThreshold= 4500, eth*=0**.

このインスタンスでは、最初の 3 文字が eth に一致するすべての NIC 名に、しきい値 0 が適用されます。

Memory Bottleneck Diagnosis ポリシー

SI-MemoryBottleneckDiagnosis

このポリシーは、物理メモリの使用率とボトルネックを監視します。メモリ使用率が高く、使用可能なメモリ容量が非常に少なくなると、メモリ ボトルネックが発生します。メモリ ボトルネックが発生すると、システムの処理速度が低下し、全体的なパフォーマンスに影響を与えます。メモリ使用率が高くなると、ページアウトが過剰に発生したり、ページ スキャン率、スワップアウト バイト率、ページ要求率が高くなってしまい、最終的にはシステム速度の低下につながります。

このポリシーは、メモリ ボトルネックのしきい値に違反していないかをチェックし、違反がない場合は、メモリ使用率のしきい値に違反していないかをチェックします。メモリ ボトルネックとメモリ使用率のいずれにも問題がない場合、空きページ テーブルの状態をチェックします。空きページ テーブルのしきい値には、Microsoft が推奨する Windows システム向けの値がデフォルトで設定されています。メモリの使用に関するしきい値のうち、複数に違反している場合には、適切なメッセージ属性のメッセージが HPOM コンソールに送信されます。送付されたメッセージには、メモリを占有している上位 10 のプロセスが表示されます。

メモリ ボトルネックのチェックに使用される各種メトリックは、プラットフォームごとに異なるしきい値の値を使用します。各プラットフォームで適正なしきい値を使用するために、管理ノードにしきい値のオーバーライド ポリシーを配布します。

ThresholdOverrides_Linux は、Linux プラットフォーム上で、メモリ メトリックに対して適切なしきい値を定義します。

ThresholdOverrides_Windows は、Windows プラットフォーム上で、メモリ メトリックに対して適切なしきい値を定義します。

使用するメトリック	GBL_MEM_UTIL GBL_MEM_PAGEOUT_RATE GBL_MEM_PAGEOUT_BYTE_RATE GBL_MEM_PAGE_REQUEST_RATE* GBL_MEM_CACHE_FLUSH_RATE * GBL_MEM_PG_SCAN_RATE GBL_MEM_PHYS GBL_MEM_PAGE_REQUEST_RATE GBL_MEM_CACHE_FLUSH_RATE GBL_MEM_SWAPOUT_BYTE_RATE GBL_MEM_PG_SCAN_RATE * 上記のメトリックが使用されるのは、HP Performance Agent が管理ノードにインストールされている場合のみです。
サポートされているプラットフォーム	Microsoft Windows Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM AIX Oracle Solaris
スクリプト パラメータ	**説明**
MemPageOutRateCriticalThreshold	このしきい値には、物理メモリからスワップアウトされた 1 秒あたりの総ページ数で指定します。スワップアウトされたページ数にしきい値を設定します。この値に達すると、重要度が危険域のメッセージが受信されます。
MemPageOutRateMajorThreshold	スワップアウトされたページ数にしきい値を設定します。このしきい値に達すると、重要度が重要警戒域のメッセージが受信されます。
MemPageOutRateMinorThreshold	スワップアウトされたページ数にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。

MemPageOutRateWarningThreshold	スワップアウトされたページ数にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
MemUtilCriticalThreshold	このしきい値には、ノード上の物理メモリ使用率をパーセンテージ (0 ~ 100%) で指定します。ディスクの使用済みメモリ容量の最小値にしきい値を設定します。この値に達すると、重要度が危険域のメッセージが受信されます。
MemUtilMajorThreshold	ノードの使用済みメモリ容量の最小値にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
MemUtilMinorThreshold	ノード上の使用済みメモリ容量の最小値にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。
MemUtilWarningThreshold	ノード上の使用済みメモリ容量の最小値にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
MemPageScanRateCriticalThreshold	このしきい値には、物理メモリからディスクへスワップインされた 1 秒あたりの総ページ数で指定します。スワップインされたページ数にしきい値を設定します。この値に達すると、重要度が危険域のメッセージが受信されます。
MemPageScanRateMajorThreshold	スワップインされたページ数にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
MemPageScanRateMinorThreshold	スワップインされたページ数にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。
MemPageScanRateWarningThreshold	スワップインされたページ数にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
MemPageReqRateHighThreshold	1 秒あたりに発生したディスクからのページ要求数にしきい値を設定します。
MemCacheFlushRateHighThreshold	キャッシュ フラッシュ率にしきい値を設定します。この値に達すると、ファイル システム キャッシュがデータをディスクにフラッシュします。

FreeMemAvailCriticalThreshold	このしきい値には、ディスクまたはファイル システムで使用可能な空き物理メモリ容量 (MB 単位) を指定します。ディスク上にある空きメモリ容量の最小値にしきい値を設定します。この値に達すると、重要度が危険域のメッセージが受信されます。
FreeMemAvailMajorThreshold	ディスク上にある空きメモリ容量の最小値にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
FreeMemAvailMinorThreshold	ディスク上にある空きメモリ容量の最小値にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。
FreeMemAvailWarningThreshold	ディスク上にある空きメモリ容量の最小値にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
MemSwapoutByteRateCriticalThreshold	このしきい値は、ページアウト デーモンが 1 秒あたりにスキャンするページ数 (MB 単位) で指定します。ディスク上にある空きメモリ容量の最小値にしきい値を設定します。この値に達すると、重要度が危険域のメッセージが受信されます。
MemSwapoutByteRateMajorThreshold	ディスク上にある空きメモリ容量の最小値にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
MemSwapoutByteRateMinorThreshold	ディスク上にある空きメモリ容量の最小値にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。
MemSwapoutByteRateWarningThreshold	ディスク上にある空きメモリ容量の最小値にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
FreePageTableCriticalThreshold	このしきい値には、システムで使用可能な空きページ テーブルの数を指定します。ディスク上にある空きページ テーブル エントリ数の最小値にしきい値を設定します。このしきい値に達すると、重要度が危険域のメッセージが受信されます。 このパラメータは、Windows のみで使用できます。

FreePageTableMajorThreshold	ディスク上にある空きページ テーブル エントリ数の最小値にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。 このパラメータは、Windows のみで使用できます。
FreePageTableMinorThreshold	ディスク上にある空きページ テーブル エントリ数の最小値にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。 このパラメータは、Windows のみで使用できます。
FreePageTableWarningThreshold	ディスク上にある空きページ テーブル エントリ数の最小値にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。 このパラメータは、Windows のみで使用できます。
MessageGroup	このポリシーによって管理コンソールに送信されるメッセージを特定できるように、わかりやすい値を指定してください。しきい値の違反が発生すると、このポリシーは、パラメータの値をメッセージに付加してから管理コンソールに送信します。
Debug	トレース メッセージを無効にするには、この値を **0** に設定します。コンソールでトレース メッセージを受信するには **1**、管理ノードのトレース ファイルにメッセージを記録するには **2** に設定します。詳細については、「トレース」(22ページ)を参照してください。

CPU Spike Check ポリシー

SI-CPUSpikeCheck

これは、プロセッサのパフォーマンスを監視するポリシーです。CPU スパイクとは、CPU 使用率が急増した直後に低減する現象です。SI-CPUSpikeCheck ポリシーは、システム モードでの CPU ビジー時間あたりの CPU スパイク、ユーザー モードでの CPU ビジー時間あたりの CPU スパイク、CPU ごとの総ビジー時間を監視します。

使用するメトリック	BYCPU_CPU_USER_MODE_UTIL BYCPU_CPU_SYS_MODE_UTIL BYCPU_ID BYCPU_CPU_TOTAL_UTIL BYCPU_INTERRUPT_RATE

サポートされているプラットフォーム	Microsoft Windows Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM AIX Oracle Solaris Debian Ubuntu
スクリプト パラメータ	**説明**
CpuUtilCriticalThreshold	このしきい値は、CPU がビジー状態の CPU 時間の合計で指定します。つまり、CPU 使用時間の合計です。これには、ユーザー モードとシステム モードで CPU を使用した時間の合計が含まれます。CPU の総使用時間の最小値にしきい値を設定します。この値に達すると、重要度が危険域のメッセージが受信されます。
CpuUtilMajorThreshold	CPU の総使用時間の最小値にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
CpuUtilMinorThreshold	CPU の総使用時間の最小値にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。
CpuUtilWarningThreshold	CPU の総使用時間の最小値にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
CpuUtilUsermodeCriticalThreshold	このしきい値は、CPU がユーザー モードでビジー状態のときの CPU 時間の比率をパーセンテージ (0 ~ 100%) で指定します。CPU のビジー時間の最小値にしきい値を設定します。この値に達すると、重要度が危険域のメッセージが受信されます。
CpuUtilUsermodeMajorThreshold	ユーザー モードでの CPU ビジー時間の最小値にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
CpuUtilUsermodeMinorThreshold	ユーザー モードでの CPU ビジー時間の最小値にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。

CpuUtilUsermodeWarningThreshold	ユーザー モードでの CPU ビジー時間の最小値にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
CpuUtilSysmodeCriticalThreshold	このしきい値には、CPU がシステム モードでビジー状態のときの CPU 時間の比率をパーセンテージ (0 ~ 100%) で指定します。CPU のビジー時間の最小値にしきい値を設定します。この値に達すると、重要度が危険域のメッセージが受信されます。
CpuUtilSysmodeMajorThreshold	システム モードでの CPU ビジー時間の最小値にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
CpuUtilSysmodeMinorThreshold	システム モードでの CPU ビジー時間の最小値にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。
CpuUtilSysmodeWarningThreshold	システム モードでの CPU ビジー時間の最小値にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
InterruptRateCriticalThreshold	このしきい値は、サンプリング期間内に発生した 1 秒あたりのデバイス割り込みの平均数で指定します。CPU の割り込み率の最小値にしきい値を設定します。この値に達すると、重要度が危険域のメッセージが受信されます。
InterruptRateMajorThreshold	CPU の割り込み率の最小値にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
InterruptRateMinorThreshold	CPU の割り込み率の最小値にしきい値を設定します。この値に達すると、重要度が警戒域のメッセージが受信されます。
InterruptRateWarningThreshold	CPU の割り込み率の最小値にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。
MessageGroup	送信メッセージのメッセージ グループ。
Debug	トレース メッセージを無効にするには、この値を **0** に設定します。コンソールでトレース メッセージを受信するには **1**、管理ノードのトレース ファイルにメッセージを記録するには **2** に設定します。詳細については、「トレース」(22ページ)を参照してください。

CPU Bottleneck Diagnosis ポリシー

SI-CPUBottleneckDiagnosis

このポリシーは、CPU 使用率、プロセッサ キューの長さ、システムに搭載されている CPU の総数、オペレーティング システムに関するしきい値の超過など、CPU のボトルネックを検出します。

CPU 使用率のしきい値と、CPU 時間をキュー内で待機するプロセス数のしきい値に違反した場合、このポリシーは、適切な属性を含むメッセージを HPOM コンソールに送信します。このメッセージには、CPU を占有している上位 10 のプロセスが表示されます。

DataSource SCOPE が有効なマシンに使用されるメトリック	GBL_CPU_TOTAL_UTIL GBL_ACTIVE_CPU GBL_CPU_QUEUE* GBL_LOADAVG GBL_INTERRUPT_RATE GBL_CSWITCH_RATE * このメトリックは、HP-UX プラットフォームのみで使用できます。
DataSource SCOPE が有効でないマシンに使用されるメトリック	GBL_CPU_TOTAL_UTIL GBL_ACTIVE_CPU GBL_RUN_QUEUE GBL_INTERRUPT_RATE
サポートされているプラットフォーム	Microsoft Windows Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM AIX Oracle Solaris
スクリプト パラメータ	**説明**
GlobalCpuUtilCriticalThreshold	このしきい値は、全体的な CPU 使用率で指定します。全体的な CPU 使用率の最小値にしきい値を設定します。この値に達すると、危険域メッセージが受信されます。

GlobalCpuUtilMajorThreshold	全体的な CPU 使用率の最小値にしきい値を設定します。この値に達すると、重要警戒域メッセージが受信されます。
GlobalCpuUtilMinorThreshold	全体的な CPU 使用率の最小値にしきい値を設定します。この値に達すると、警戒域メッセージが受信されます。
GlobalCpuUtilWarningThreshold	全体的な CPU 使用率の最小値にしきい値を設定します。この値に達すると、注意域メッセージが受信されます。
MessageGroup	このポリシーによって管理コンソールに送信されるメッセージを特定できるように、わかりやすい値を指定してください。しきい値の違反が発生すると、このポリシーは、パラメータの値をメッセージに付加してから管理コンソールに送信します。
Debug	トレース メッセージを無効にするには、この値を **0** に設定します。コンソールでトレース メッセージを受信するには **1**、管理ノードのトレース ファイルにメッセージを記録するには **2** に設定します。詳細については、「トレース」(22ページ)を参照してください。

Sample Performance ポリシー

SI SPI では、システム上で実行されるプロセスのパフォーマンスの監視に使用可能なパフォーマンス ポリシーのサンプルが用意されています。このポリシーをテンプレートとしてコピーしてから、各ユーザーのニーズに合わせて変更することができます。

スクリプト パラメータ	**説明**
ProcessName	監視対象となるプロセスの名前を入力します。
ProcessArguments	必要に応じて、プロセス引数を入力します。
MessageGroup	送信メッセージのメッセージ グループ。
CPUUsageHighWaterMark または MemoryUsageHighWaterMark	プロセスの CPU 使用率またはメモリ使用率にしきい値を設定します。この値に達すると、アラートが受信されます。
Debug	トレース メッセージを無効にするには、この値を **0** に設定します。コンソールでトレース メッセージを受信するには **1**、管理ノードのトレース ファイルにメッセージを記録するには **2** に設定します。詳細については、「トレース」(22ページ)を参照してください。

次のようなサンプル ポリシーが提供されています。

SI-JavaProcessMemoryUsageTracker ポリシーは、システム上で実行される Java プロセスのメモリ使用率を監視します。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Performance] → [Process Resource Usage Monitor Samples]

SI-JavaProcessCPUUsageTracker ポリシーは、システム上で実行される Java プロセスの CPU 使用率を監視します。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Performance] → [Process Resource Usage Monitor Samples]

SI-MSWindowsSvchostCPUUsageTracker ポリシーは、システム上で実行される svchost プロセスの CPU 使用率を監視します。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Performance] → [Process Resource Usage Monitor Samples] → [Windows]

SI-MSWindowsSvchostMemoryUsageTracker ポリシーは、システム上で実行される svchost プロセスのメモリ使用率を監視します。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Performance] → [Process Resource Usage Monitor Samples] → [Windows]

Disk Peak Utilization Monitor ポリシー

SI-DiskPeakUtilMonitor

このポリシーは、システム上のディスクの使用率レベルを監視します。使用率レベルが一杯かどうかを確認します。ディスク使用率レベルが指定されたしきい値を超えると、ポリシーは HPOM コンソールにアラート メッセージを送信します。

使用するメトリック	GBL_FS_SPACE_UTIL_PEAK
サポートされているプラットフォーム	Microsoft Windows Red Hat Enterprise Linux Suse Linux Enterprise Server HP-UX IBM AIX Oracle Solaris
スクリプト パラメータ	**説明**
DiskPeakUtilCriticalThreshold	このしきい値は、満杯のディスクの使用率レベルをパーセンテージで指定します。危険域メッセージを受信する基準となるしきい値を設定します。

DiskPeakUtilMajorThreshold	重要危険域メッセージを受信する基準となるしきい値を設定します。
DiskPeakUtilMinorThreshold	警戒域メッセージを受信する基準となるしきい値を設定します。
DiskPeakUtilWarningThreshold	注意域メッセージを受信する基準となるしきい値を設定します。
MessageGroup	送信メッセージのメッセージ グループ。
Debug	トレース メッセージを無効にするには、この値を **0** に設定します。コンソールでトレース メッセージを受信するには **1**、管理ノードのトレース ファイルにメッセージを記録するには **2** に設定します。詳細については、「トレース」(22ページ)を参照してください。

コンソール ツリーでは、SI-DiskPeakUtilMonitor ポリシーは以下の場所にあります。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Policies Grouped by Vendor] → [<すべてのプラットフォーム> - QuickStart]

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Performance]

RealTimeAlerts ポリシー

RealtimeAlerts ポリシーは、CPU、ディスク、メモリ、およびネットワークのボトルネックを検出します。Realtime Configuration ポリシーは、これらのパラメータのしきい値を定義します。しきい値侵害が発生すると、アラート メッセージによってその由が遅延なくシステム管理者に通知され、実運用環境でのダウンタイムが減少します。

注: RealTimeAlerts ポリシーがリアルタイム データをフェッチするには、HP Operations Agent ノード上で RTMA ライセンスを有効にする必要があります。

アラート メッセージを受信するには、ノード上で RealTime Configuration ポリシーを配布し、ノード上で **perfd** デーモン プロセスおよび cpsh プログラムが実行中であることを確認する必要があります。

注: 次のコマンドを実行すると、**perfd** プロセスを開始できます。

Windows の場合:

```
%ovinstalldir%bin\ovpacmd stop RTMA
%ovinstalldir%bin\ovpacmd start RTMA
```

HP-UX/Linux/Solaris の場合:

```
/opt/perf/bin/pctl restart
```

AIX の場合:

```
/usr/lpp/perf/bin/pctl restart
```

配布後のアクションとして、このポリシーは Perl スクリプト (`advisor.pl`) を実行し、advisor 出力を `adv.out` ファイルに送信します。ノード上で次のログ ファイル監視ポリシーが実行され、`adv.out` ファイルからデータが読み込まれ、アラートが HPOM コンソールに送信されます。

- Windows - SI-MSWindowsRealtimeAlerts
- Linux または UNIX - SI-LinuxRealtimeAlerts

詳細については、『HP Operations Agent ユーザー ガイド』の「RTMA コンポーネントのアドバイザ」を参照してください。

サポートされているプラットフォーム	HPUX RHEL MS Windows Sun Solaris IBM AIX

SI-AIXRealTimeConfig ポリシー

SI-AIXRealTimeConfig ポリシーは、CPU、ディスク、メモリ、およびネットワークのしきい値を定義します。

サポートされているプラットフォーム	IBM AIX
使用するメトリック	GBL_SWAP_SPACE_UTIL
CPU に使用されるメトリック	GBL_LOADAVG GBL_ACTIVE_CPU GBL_CPU_TOTAL_UTIL
ディスクに使用されるメトリック	GBL_DISK_UTIL_PEAK GBL_BLOCKED_IO_QUEUE
メモリに使用されるメトリック	GBL_MEM_UTIL GBL_MEM_PG_SCAN_RATE GBL_MEM_PAGEOUT_BYTE_RATE
ネットワークに使用されるメトリック	GBL_NET_UTIL_PEAK GBL_NET_COLLISON_PCT GBL_NET_PACKET_RATE

SI-HPUXRealTimeConfig ポリシー

SI-HPUXRealTimeConfig ポリシーは、CPU、ディスク、メモリ、およびネットワークのしきい値を定義します。

サポートされているプラットフォーム	HP-UX
使用するメトリック	GBL_SWAP_SPACE_UTIL
CPU に使用されるメトリック	GBL_ACTIVE_CPU GBL_CPU_TOTAL_UTIL GBL_CPU_QUEUE
ディスクに使用されるメトリック	GBL_DISK_UTIL_PEAK GBL_DISK_SUBSYSTEM_QUEUE
メモリに使用されるメトリック	GBL_MEM_UTIL GBL_MEM_PG_SCAN_RATE GBL_MEM_PAGEOUT_BYTE_RATE GBL_MEM_SWAPOUT_BYTE_RATE
ネットワークに使用されるメトリック	GBL_NET_UTIL_PEAK GBL_NET_COLLISION_PCT GBL_NET_PACKET_RATE GBL_NET_OUTQUEUE

SI-LinuxRealTimeConfig ポリシー

SI-LinuxRealtimeConfig ポリシーは、CPU、ディスク、メモリ、およびネットワークのしきい値を定義します。

サポートされているプラットフォーム	Linux
使用するメトリック	GBL_SWAP_SPACE_UTIL
CPU に使用されるメトリック	GBL_LOADAVG GBL_ACTIVE_CPU GBL_CPU_TOTAL_UTIL
ディスクに使用されるメトリック	GBL_DISK_UTIL_PEAK GBL_DISK_REQUEST_QUEUE
メモリに使用されるメトリック	GBL_MEM_UTIL GBL_MEM_PAGEOUT_BYTE_RATE

ネットワークに使用されるメトリック	GBL_NET_PACKET_RATE GBL_NET_COLLISION_PCT GBL_NFS_CALL_RATE

SI-MSWindowsRealTimeConfig ポリシー

SI-MSWindowsRealtimeConfig ポリシーは、CPU、ディスク、メモリ、およびネットワークのしきい値を定義します。

サポートされているプラットフォーム	MS Windows
使用するメトリック	GBL_SWAP_SPACE_UTIL
CPU に使用されるメトリック	GBL_CPU_TOTAL_UTIL GBL_LOADAVG
ディスクに使用されるメトリック	GBL_DISK_UTIL_PEAK GBL_DISK_REQUEST_QUEUE
メモリに使用されるメトリック	GBL_MEM_UTIL GBL_MEM_PAGE_REQUEST_RATE GBL_MEM_CACHE_FLUSH_RATE GBL_MEM_PAGEOUT_RATE
ネットワークに使用されるメトリック	GBL_NET_UTIL_PEAK GBL_NET_PACKET_RATE GBL_NET_OUTQUEUE

SI-SunSolarisRealTimeConfig ポリシー

SI-SunSolarisRealTimeConfig ポリシーは、CPU、ディスク、メモリ、およびネットワークのしきい値を定義します。

サポートされているプラットフォーム	Sun Solaris
使用するメトリック	GBL_SWAP_SPACE_UTIL
CPU に使用されるメトリック	GBL_LOADAVG GBL_ACTIVE_CPU GBL_CPU_TOTAL_UTIL
ディスクに使用されるメトリック	GBL_DISK_UTIL_PEAK GBL_BLOCKED_IO_QUEUE

メモリに使用されるメトリック	GBL_MEM_UTIL GBL_MEM_PG_SCAN_RATE GBL_MEM_PAGEOUT_BYTE_RATE
ネットワークに使用されるメトリック	GBL_NET_PACKET_RATE GBL_NET_COLLISION_PCT GBL_NFS_CALL_RATE

SI-CPUStealtimeUtilMonitor

このポリシーは、仮想 CPU が物理 CPU を待機する時間を監視します。この時間は「スチール タイム」と呼ばれます。スチール タイムは、物理 CPU が別の仮想 CPU に対する要求の処理にビジーな場合に発生します。

使用するメトリック	GBL_CPU_STOLEN_UTIL
サポートされているプラットフォーム	Linux RHEL Ubuntu Debian
ルール	**説明**
CpuUtilMajorThreshold	CPU の総使用時間の最小値にしきい値を設定します。この値に達すると、重要度が重要警戒域のメッセージが受信されます。
CpuUtilWarningThreshold	CPU の総使用時間の最小値にしきい値を設定します。この値に達すると、重要度が注意域のメッセージが受信されます。

Adaptive Thresholding ポリシー

注:

Infrastructure SPI 12.00 (AdaptiveThresholding) ポリシーは、HP Operations Agent バージョン 11.xx では機能しません。

HP Operations Agent で計算されたベースライン データは、SI-AdaptiveThresholdingMonitor ポリシーで使用され、パフォーマンスとリソースの使用率を監視します。

注: HP Operations Agent ノードでベースラインを有効にするには、コマンド ライン オプションを使用します。詳細については、『HP Operations Agent ユーザー ガイド』のトピック

「HP Operations Agent ノードでのベースラインの設定」を参照してください。

XPL の設定を使用して、ベースラインを有効にすることもできます。以下の手順を実行します。

1. HPOM コンソールで、**[ポリシー管理] → [ポリシー グループ] → [Infrastructure Management] →[v12.0] → [Settings and Thresholds] → [Agent Settings] → [OPC_PERL_INCLUDE_INSTR_DIR]** を選択します。
2. ENABLE_BASELINE を TRUE に設定し、ポリシーを必要なすべてのノードに配布します。

ベースライン データは、毎時間の最後に計算されます。ベースラインを有効化した直後にベースライン データを計算する場合は、**oacore** プロセスを再起動する必要があります。**oacore** を再起動するには、以下のコマンドを実行します。

```
ovc -restart oacore
```

ベースライン データは、SI-ConfigureBaselining ポリシーまたは SI-AdaptiveThresholdingMonitor ポリシーで設定された偏差 (N) と共に使用され、適応監視または適応しきい値を有効にします。 適応しきい値は、最適なしきい値を動的に計算する場合に役に立ちます。

HP Operations Agent ノードで適応しきい値を有効にするには、以下の手順を実行します。

1. ベースラインを設定する ノードでの SI-ConfigureBaselining ポリシーの設定と配布
2. HP Operations Agent ノードでの SI-AdaptivethresholdingMonitor ポリシーの設定と配布

SI-ConfigureBaselining ポリシーの設定と配布

注: HP Operations Agent ノードでベースラインが有効になっていることを確認します。ベースラインの有効化の詳細については、『HP Operations Agent ユーザー ガイド』の「HP Operations Agent ノード上でベースラインを有効にします」を参照してください。

以下の手順を実行して、ノード上で SI-ConfigureBaselining ポリシーを設定および配布します。

1. HPOM コンソールで、次を選択します。**[ポリシー管理] → [ポリシーグループ] → [Infrastructure Management] →[v12.0] → [<言語>] → [Systems Infrastructure] → [Performance] → [Adaptive Thresholding] → [SI-ConfigureBaselining policy]**
2. **[SI-ConfigureBaselining]** ポリシー → **[データ]** タブを開き、監視するメトリックを次のいずれかの形式で定義します。
   - メトリックのみを定義するには:

     ```
     [Baseline]
     <Class>:<Metrics>
     ```

   - メトリックと偏差を定義するには:

     ```
     [Baseline]
     <Class>:<Metrics>,<Warning Deviation>,<Minor Deviation>,<Major Deviation>
     ```

偏差の設定の詳細については、「偏差の設定」を参照してください。

3. ノードに SI-ConfigureBaselining ポリシーを配布します。

SI-ConfigureBaselining の配布後に、`baseline.cfg` ファイルが次のディレクトリに作成されます。

Windows の場合

`%ovdatadir%`

UNIX (および Linux) の場合

`/var/opt/perf/`

注: この `baseline.cfg` ファイルは、ノードでのベースラインの設定中に作成された `baseline.cfg` ファイルを上書きします。『HP Operations Agent ユーザー ガイド』の「HP Operations Agent ノードでのベースラインの設定」を参照してください。

SI-ConfigureBaselining ポリシーを配布したら、ベースライン データがポリシーで定義したメトリック用のデータベースに記録されているかどうかを確認します。

SI-AdaptiveThresholdingMonitor ポリシーの設定と配布

以下の手順を実行して、ノード上で SI-AdaptiveThresholdingMonitor ポリシーを設定および配布します。

1. HPOM コンソールで、**[ポリシー管理]** → **[ポリシーグループ]** → **[Infrastructure Management]** → **[v12.0]** → **[<言語>]** → **[Systems Infrastructure]** → **[Performance]** → **[Adaptive Thresholding]** → **[SI-AdaptiveThresholdingMonitor policy]** を選択します。
2. **[SI-AdaptivethresholdingMonitor]** ポリシー → **[スクリプト パラメータ]** タブを開きます。**[スクリプト パラメータ]** タブに、すべての監視対象メトリックの標準設定偏差がリストされます。
3. 新しい偏差を設定し、SI-AdaptiveThresholdingMonitor ポリシーを配布します。

注: SI-AdaptiveThresholdingMonitor ポリシーを使用して適応しきい値を設定するには、少なくとも 1 週間のベースライン データが利用可能である必要があります。

偏差の設定の詳細については、「偏差の設定」を参照してください。

HP Operations Agent で計算されたベースライン データは、SI-ConfigureBaselining ポリシーまたは SI-AdaptiveThresholdingMonitor ポリシーで設定された偏差 (N) と共に使用され、リソースの使用率を監視するための適応しきい値を設定します。

偏差の設定

偏差は、SI-ConfigureBaselining ポリシーまたは SI-AdaptivethresholdingMonitor ポリシーのいずれかで設定できます。

注:

特定のメトリックの偏差を設定するには、SI-ConfigureBaselining ポリシーで偏差を設定します。

すべてのメトリックの偏差を設定するには、SI-AdaptivethresholdingMonitor ポリシーの **[スクリプト パラメータ]** タブで偏差を設定します。

SI-ConfigureBaselining ポリシーのメトリックに偏差が設定されていない場合、SI-AdaptiveThresholdingMonitor ポリシーに設定されている偏差が適応しきい値の計算に使用されます。

SI-ConfigureBaselining ポリシーでの偏差の設定

1. HPOM コンソールで、**[ポリシー管理]** → **[ポリシー グループ]** → **[Infrastructure Management]** → **[v12.0]** → **[<言語>]** → **[Systems Infrastructure]** → **[Performance]** → **[Adaptive Thresholding]** → **[SI-ConfigureBaselining policy]** を選択します。
2. **[SI-ConfigureBaselining]** ポリシー → **[データ]** タブを開き、メトリックと偏差を次の形式で定義します。

   ```
   [Baseline]

   <Class>:<Metrics>,<Warning Deviation>,<Minor Deviation>,<Major
   Deviation>,<Minimum Value>,<Maximum Value>,<CutOff>
   ```

   例:

   ```
   [Baseline]

   Global:GBL_MEM_UTIL,-1,0,1,0,100,15
   ```

インスタンスベースの監視

特定のインスタンスの偏差を設定して、インスタンスベースの監視を有効にすることもできます。

注: インスタンスベースの監視は、次のメトリック クラス、ファイルシステム、netif、およびディスクに対してのみサポートされています。

以下の手順を実行して、特定のインスタンスの偏差を設定します。

1. HPOM コンソールで、**[ポリシー管理]** → **[ポリシーグループ]** → **[Infrastructure Management]** → **[v12.0]** → **[<言語>]** → **[Systems Infrastructure]** → **[Performance]** → **[Adaptive Thresholding]** → **[SI-ConfigureBaselining policy]** を選択します。
2. [SI-ConfigureBaselining] ポリシー → **[データ]** タブを開き、メトリックと偏差を次の形式で定義します。

   ```
   [Baseline]

   <Class>:<Metric>
   ```

3. 次の形式で特定のインスタンスの偏差を設定します。

   ```
   [<Class>:<Metric>]
   ```

```
<Instance>,<Warning Deviation>,<Minor Deviation>,<Major Deviation>,<Minimum
Value>,<Maximum Value>,<CutOff>
```

例:

dsk0、dsk1、dsk2 の 3 つのディスクを監視しているとします。各ディスクの特定の偏差は、次のように設定できます。

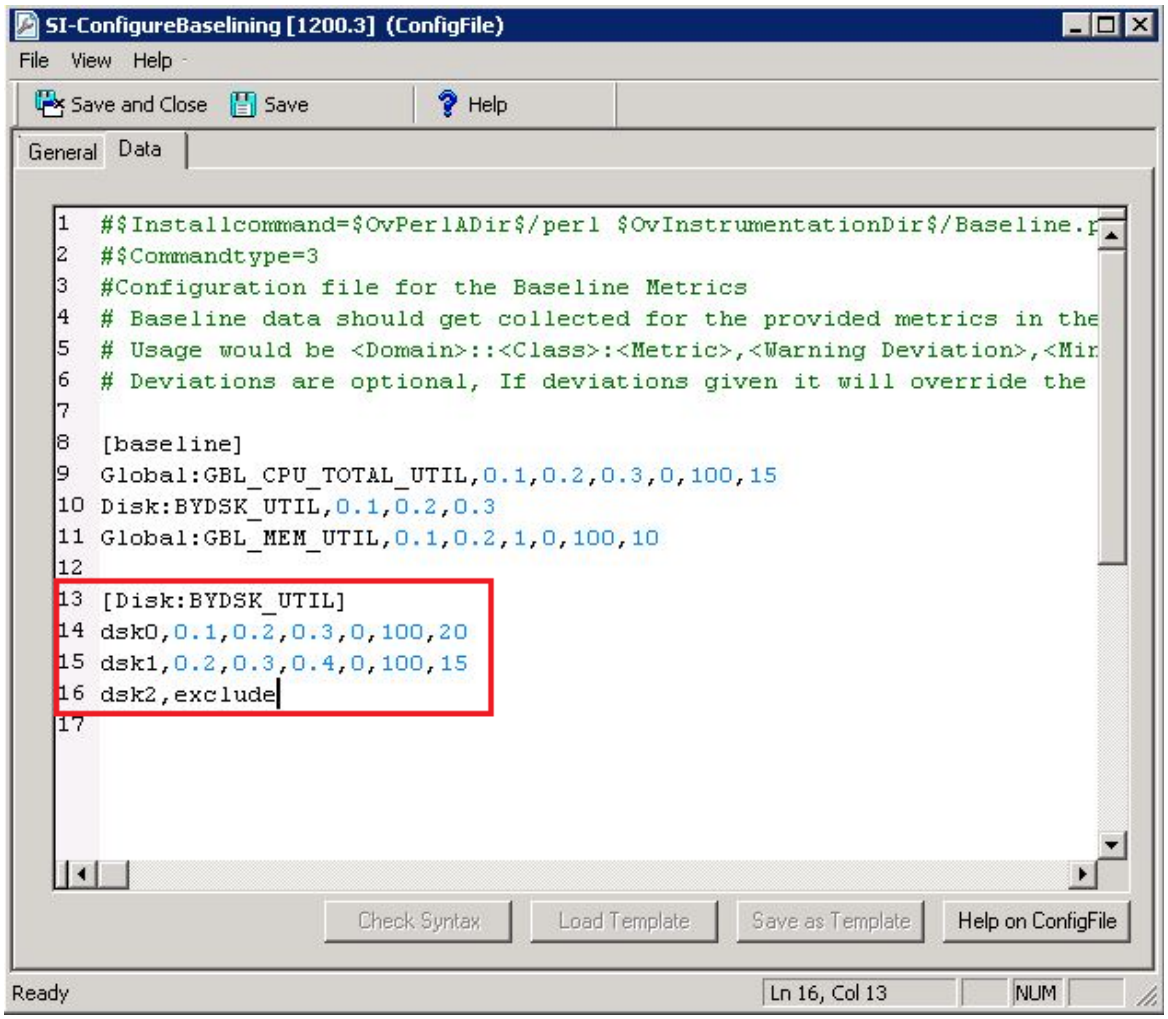
```
[Baseline]
Disk:BYDSK_UTIL


[Disk:BYDSK_UTIL]
 dsk0,0.1,0.2,0.3,0,100,20
 dsk1,0.2,0.3,0.4,0,100,15
 dsk2:exclude
```

上記の設定について:

監視対象ディスク	注意域偏差	警戒域偏差	重要警戒域偏差	最小値	最大値	カットオフ
dsk0	0.1	0.2	0.3	0	100	20
dsk1	0.2	0.3	0.4	0	100	15
dsk2	監視対象外					

SI-ConfigureBaselining ポリシーのしきい値の変更例

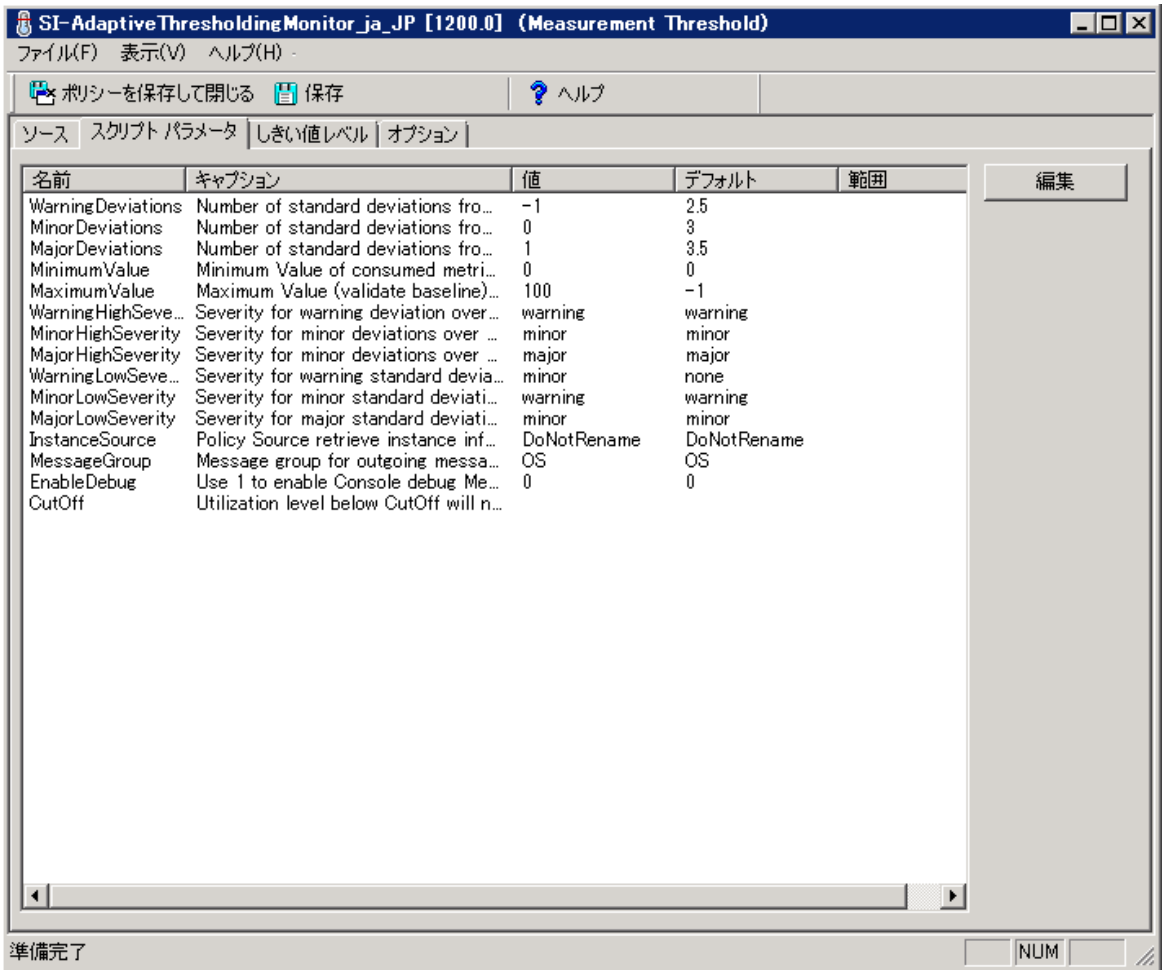


注: インスタンスベースの監視がポリシーで定義されている場合、対応する .cfg ファイルが作成されます。ポリシーからインスタンス レベルのメトリックを削除すると、対応する .cfg ファイルも削除されます。

SI-AdaptiveThresholdingMonitor ポリシーでの偏差の設定

1. HPOM コンソールで、**[ポリシー管理] → [ポリシーグループ] → [Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Performance] → [Adaptive Thresholding] → [SI-AdaptivethresholdingMonitor policy]** を選択します。
2. [SI-AdaptivethresholdingMonitor] ポリシー → **[スクリプト パラメータ]** タブを開きます。すべての監視対象メトリックの注意域、警戒域、および重要警戒域偏差がリストされます。
3. 新しいしきい値を設定します。

SI-AdaptiveThresholdingMonitor ポリシーのしきい値の変更例



アラート メッセージの生成

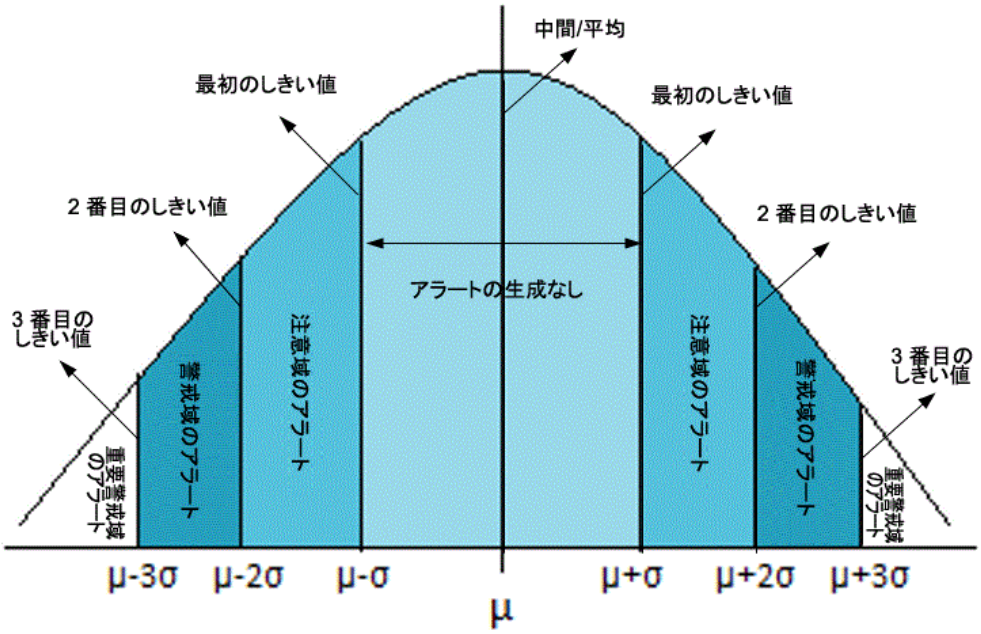
HP Operations Agent によって計算されたベースライン データ (平均偏差と標準偏差の値) は、SI-ConfigureBaselining ポリシーおよび SI-AdaptiveThresholdingMonitor ポリシーで設定された偏差 (N) と共に、しきい値を設定するために次の計算式で使用されます。

正常域の動作の範囲 = 履歴の平均 ± N * 履歴標準偏差

このインスタンスの場合:

- 履歴の平均は、ベースライン プロセスを使用して計算された履歴データの平均です。
- N は、注意域、警戒域、または重要警戒域偏差の値です。
- 履歴標準偏差は、ベースライン プロセスを使用して計算された標準偏差です。

グラフに示すように、計算されたしきい値に違反すると、常にアラートが生成されます。



警告タイプ	説明
注意域	最初のしきい値、つまり μ ± σ に違反すると、重要度が注意域のアラート メッセージが生成されます。 このインスタンスでは、注意域偏差は 1 です。
警戒域	2 番目のしきい値、つまり μ ± 2 σ に違反すると、重要度が警戒域のアラート メッセージが生成されます。 このインスタンスでは、警戒域偏差は 2 です。
重要警戒域	3 番目のしきい値、つまり μ ± 3 σ に違反すると、重要度が重要警戒域のアラート メッセージが生成されます。 このインスタンスでは、重要警戒域偏差は 3 です。

使用例: 適応監視に対するベースライン データの使用

John は、HP Operations Agent を使用してベースライン データを収集しているシステム管理者です。適応監視を有効にするために、彼はインフラストラクチャ ポリシーの SI-ConfigureBaselining ポリシーと SI-AdaptivethresholdingMonitor ポリシーをノードに配布します。

HP Operations Agent で計算されたベースライン データは、SI-ConfigureBaselining ポリシー (または SI-AdaptiveThresholdingMonitor ポリシー) で設定された偏差 (N) と共に使用され、リソースの使用率を監視するための適応しきい値を計算します。

John は、月曜日の午前 10:00 ~ 11:00 時の間に CPU 使用率を監視することにしました。

CPU 使用率の監視

毎月曜日の午前 10:00 ~ 11:00 時の間に、次のベースライン データがデータ ストアに記録されている履歴データを使用して計算されるとします。

最小	最大	履歴の平均 (μ)	標準偏差 (σ)
5	75	39.03	17.02

John は、SI-AdaptivethresholdingMonitor ポリシーの [**スクリプト パラメータ**] タブに設定されている次の偏差を使用するとします。

偏差 (N)	値
注意域	1
警戒域	2
重要警戒域	3

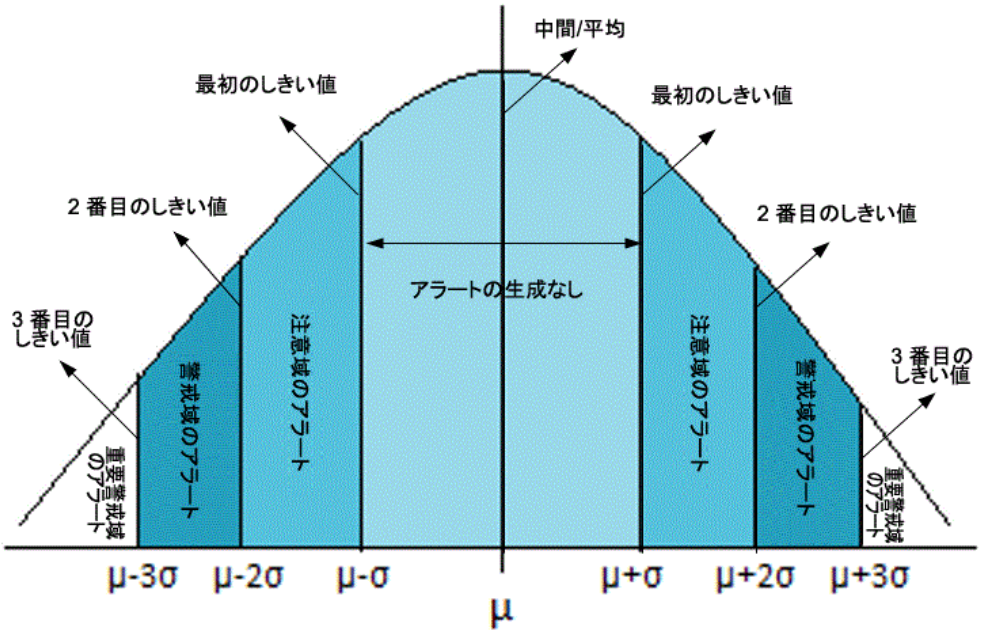
次の計算式で履歴の平均 (39.03)、標準偏差 (17.02)、および偏差 (N) の値が使用され、しきい値を設定します。

正常域の動作の範囲 = 履歴の平均 ± N * 履歴標準偏差

このインスタンスの場合:

- 履歴の平均は、ベースライン プロセスを使用して計算された履歴データの平均です。
- N は、注意域、警戒域、または重要警戒域偏差の値です。
- 履歴標準偏差は、ベースライン プロセスを使用して計算された標準偏差です。

グラフに示すように、計算されたしきい値に違反すると、常にアラートが生成されます。



警告タイプ	説明
注意域	最初のしきい値、つまり μ ± σ に違反すると、重要度が注意域のアラート メッセージが生成されます。 この例では、CPU 使用率が 56.05% を超えるか、22.01% を下回ると、常に注意域のアラートが生成されます。
警戒域	2 番目のしきい値、つまり μ ± 2 σ に違反すると、重要度が警戒域のアラート メッセージが生成されます。 この例では、CPU 使用率が 73.07% を超えるか、4.99% を下回ると、常に警戒域のアラートが生成されます。
重要警戒域	3 番目のしきい値、つまり μ ± 3 σ に違反すると、重要度が重要警戒域のアラート メッセージが生成されます。 この例では、CPU 使用率が 90.09% を超えるか、0% に到達すると、常に重要警戒域のアラートが生成されます。

セキュリティ ポリシー

使用例: 権限がないユーザーが、自動スクリプトで別のユーザー名とパスワードの組み合わせを入力して、システムへのアクセスを試みることがあります。これにより、ログイン試行が何度か失敗することがあります。このようなリスクを把握し、回避する方法として、Systems Infrastructure のセキュリティ ポリシーでログインの失敗回数を定期的にチェックすることができます。これらのポリシーは、失敗したログイン試行に関するデータを収集し、最大の試行回数を超過後にアラートを送信します。

注: セキュリティ コレクタ ポリシーを配布したら、必要なデータを収集するために、ポリシーを 5 分以上実行してください。

Windows 用の Failed Login Collector ポリシー

SI-MSWindowsFailedLoginsCollector

これは、Scheduled Task ポリシーであり、Microsoft Windows 上で失敗したログインの試行回数をチェックします。管理ノード上で、不明なユーザー名やパスワード誤りのいずれかが原因で無効なログインが発生していないかどうかをチェックします。このポリシーは、ログイン失敗の個々のインスタンスを、組み込みパフォーマンス コンポーネント (Embedded Performance Component: EPC) の GBL_NUM_FAILED_LOGINS メトリックに一定の間隔で記録します。デフォルトでは、1 時間おきに記録します。EPC に記録された情報に基づいて、コンソールにアラートを送信したり、所定の時間内で発生した無効なログイン回数を示すレポートを作成できます。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [Windows]

または

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Policies grouped by Vendor] → [MS Windows - QuickStart]

Windows 用の Last Logon Collector ポリシー

SI-MSWindowsLastLogonsCollector

これは、Scheduled Task ポリシーであり、Microsoft Windows 上でアクティブなすべてのローカル ユーザー アカウントのログインの詳細をチェックします。このポリシーは、ユーザー ログインの個々のインスタンスを、組み込みパフォーマンス コンポーネント (Embedded Performance Component: EPC) の SECONDS_SINCE_LASTLOGIN メトリックに一定の間隔で記録します。デフォルトでは、1 時間おきに記録します。EPC に記録された情報に基づいて、コンソールにアラートを送信したり、所定の時間内で発生したユーザー ログイン回数を示すレポートを作成できます。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [Windows]

または

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Policies grouped by Vendor] → [MS Windows - QuickStart]

Linux 用の Failed Login Collector ポリシー

SI-UNIXFailedLoginsCollector

これは、Scheduled Task ポリシーであり、RHEL および SLES Linux システム、HP-UX、AIX、Solaris 上で失敗したログインの試行回数をチェックします。管理ノード上で、不明なユーザー名やパスワード誤りのいずれかが原因で無効なログインが発生していないかどうかをチェックします。このポリシーは、ログイン失敗の個々のインスタンスを、組み込みパフォーマンス コンポーネント (Embedded Performance Component: EPC) の GBL_NUM_FAILED_LOGINS メトリックに一定の間隔で記録します。デフォルトでは、1 時間おきに記録します。EPC に記録された情報に基づいて、コンソールにアラートを送信したり、所定の時間内で発生した無効なログイン回数を示すレポートを作成できます。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [Linux]

または

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Policies grouped by vendor] → [<os> - QuickStart]

<os> は AIX、Debian、HP-UX、Windows、SLES、RHEL、Solaris、Ubuntu のいずれかです。

注: Solaris ノードで SI-UNIXFailedLoginsCollector ポリシーが正しく機能するには、次の条件を満たす必要があります。

- Solaris ノード上の `etc/default/login` ファイルで、次の設定を行う必要があります。
  ```
  SYSLOG=YES
  SYSLOG_FAILED_LOGINS=1
  ```
- `/etc/syslog.conf` ファイルの次の行がコメントになっている場合は解除するか、存在しない場合は行を追加します。
  ```
  auth.notice ifdef(LOGHOST', /var/log/authlog, @loghost)
  ```
- 次のコマンドを実行して、`syslogd` を更新します。
  ```
  svcadm refresh system/system-log
  ```

次に、**SI-UNIXFailedLoginsCollector** ポリシーが他のノードに配布された場合のノードを示します。

ノード	失敗したログインを表示するコマンド/ログ ファイル
Solaris	`/var/log/authlog` ファイルを使用して、失敗したログインを表示します。
Linux および HP-UX	コマンド プロンプトで、`lastb` コマンドを実行して失敗したログインを表示します。
AIX	`/etc/security/failedlogin` ファイルを使用して、失敗したログインを表示します。

Linux 用の Last Logon Collector ポリシー

SI-LinuxLastLogonsCollector

これは、Scheduled Task ポリシーであり、RHEL、Debian、Ubuntu、SLES Linux システム上でアクティブなすべてのローカル ユーザー アカウントのログオンの詳細をチェックします。このポリシー

は、ログイン試行の個々のインスタンスを、組み込みパフォーマンス コンポーネント (Embedded Performance Component: EPC) の SECONDS_SINCE_LASTLOGIN メトリックに一定の間隔で記録します。デフォルトでは、1 時間おきに記録します。EPC に記録された情報を使用して、コンソールにアラートが送信されたり、所定の時間内のレポートが生成されたりします。このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [Linux]

または

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Policies grouped by vendor] → [<os> - QuickStart]

Linux 用の Bad Login ポリシー

SI-LinuxBadLogins

これはログ ファイル監視ポリシーで、`/var/log/btmp` ファイルに対する不正なログインを監視し、不正なログインが発生した場合にユーザーにアラートを送信します。デフォルトでは、ポーリング間隔は 10 秒です。このポリシーは、不正なログイン条件を `/var/log/btmp` ファイル内の `<*name> <*.tty> <@.datetime> - <@>\(<*>\)<*.machine>` パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [Linux]

または

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Policies grouped by vendor] → [<os> - QuickStart]

AIX 用の Bad Login ポリシー

SI-AIXBadLogs

これはログ ファイル監視ポリシーで、`/etc/security/failedlogin` ファイルに対する不正なログインを監視し、不正なログインが発生した場合にユーザーにアラートを送信します。デフォルトでは、ポーリング間隔は 10 秒です。このポリシーは、ローカルおよびリモートのユーザーに適用可能です。

ローカル ログインの失敗: このポリシーは、不正なログイン条件を `badlogs.log` ファイル内の `LOGIN <@.user> <@.tty>` パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

リモート ログインの失敗: このポリシーは、不正なログイン条件を `badlogs.log` ファイル内の `LOGIN <@.user> <@.tty> <@.host>` パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [AIX]

または

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Policies grouped by Vendor] → [AIX - QuickStart]

AIX 用の Logins ポリシー

SI-AIXLogins

これはログ ファイル監視ポリシーで、ログイン履歴の `/var/adm/wtmp` ファイルを監視し、正常なリモート ログイン、正常なローカル ログイン、システム ブート、ユーザー用のシステム シャットダウン、システム シャットダウンなどの発生時にユーザーにアラートを送信します。デフォルトでは、ポーリング間隔は 10 秒です。

リモート ログインの成功: このポリシーは、正常なリモート ログイン条件を `wtmp` ファイル内の `LOGIN<@.user> <@.tty> <@.host>` パターンと照合します。条件が満たされると、アラート メッセージが HPOM コンソールに送信されます。

ローカル ログインの成功: このポリシーは、正常なローカル ログイン条件を `wtmp` ファイル内の `LOGIN<@.user> <@.tty> <@.host>` パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

システム ブート: このポリシーは、システム ブート条件を `wtmp` ファイル内の `BOOT` パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

ユーザー用のシステム シャットダウン: このポリシーは、ユーザー用のシステム シャットダウン条件を `wtmp` ファイル内の `SHUTDOWN<@.user><@.tty>` パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

システム シャットダウン: このポリシーは、システム シャットダウン条件を `wtmp` ファイル内の `SHUTDOWN` パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [AIX]

または

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Policies grouped by Vendor] → [AIX - QuickStart]

AIX 用の Switch User ポリシー

SI-AIXSU

これはログ ファイル監視ポリシーで、ユーザー切り替え履歴の /var/adm/sulog ファイルを監視します。デフォルトでは、ポーリング間隔は 20 秒です。SU コマンドが実行されると (成否を問わず)、アラートがユーザーに送信されます。

SU の失敗: このポリシーは、失敗した SU コマンド実行の条件を SU ファイル内の SU<*> - <@.tty> <*.from> - <*.to> パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

SU の成功: このポリシーは、成功した SU コマンド実行の条件を SU ファイル内の SU<*> + <@.tty> <*.from> - <*.to> パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [AIX]

または

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Policies grouped by Vendor] → [AIX - QuickStart]

AIX 用の Sys Log ポリシー

SI-AIXSysLog

これはログ ファイル監視ポリシーで、/tmp/syslog ファイルに送信されるメッセージを監視します。デフォルトでは、ポーリング間隔は 1 分です。

プリンタ用紙切れ: /etc/syslog.conf ファイルでの記録を有効にすると、このポリシーは、送信されるメッセージを syslog ファイル内の <*> パターンと照合します。条件が満たされると、アラート メッセージが HPOM コンソールに送信されます。監視対象のファイルの正確な名前が、設定ファイルとポリシーに記載されていることを確認してください。

このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [AIX]

HP-UX 用の Bad Logins ポリシー

SI-HPUXBadLogs

これはログ ファイル監視ポリシーで、/var/adm/btmps ファイルに対する不正なログインを監視し、不正なログインが発生した場合にユーザーにアラートを送信します。デフォルトでは、ポーリング間隔は 10 秒です。

ローカル ログインの失敗: このポリシーは、不正なログイン条件を btmps ファイル内の FAILED<@.user> <@.tty> <*.date> <*.time> パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

リモート ログインの失敗:このポリシーは、不正なログイン条件を btmps ファイル内の FAILED<@.user> <@.tty><@.host> <*.date> <*.time> パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [HP-UX]

HP-UX 用の Logins ポリシー

SI-HPUXLogins

これはログ ファイル監視ポリシーで、/var/adm/wtmps ファイルに対するログインを監視し、不正なログインが発生した場合にユーザーにアラートを送信します。デフォルトでは、ポーリング間隔は 10 秒です。

ローカル ログインの成功:このポリシーは、正常なログイン条件を wtmps ファイル内の LOGIN<@.user> <@.tty> <*.date> <*.time> パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

リモート ログインの成功:このポリシーは、正常なログイン条件を wtmps ファイル内の LOGIN<@.user> <@.tty> <@.host> <*.date> <*.time> パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

システム ブート:このポリシーは、システム ブート条件を wtmps ファイル内の BOOT パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

システム シャットダウン:このポリシーは、システム シャットダウン条件を wtmps ファイル内の SHUTDOWN<@.user><@.tty> パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [HP-UX]

HP-UX 用の Switch User ポリシー

SI-HPUXSu

これはログ ファイル監視ポリシーで、ユーザー切り替えイベントの /var/adm/sulog ファイルを監視し、何らかのユーザー切り替えイベントが発生した場合にユーザーにアラートを送信します。デフォルトでは、ポーリング間隔は 10 秒です。

mondbfile モニタによって発生したメッセージの除外: このポリシーは、ユーザー切り替えイベント条件を SU ファイル内の SU<*> + <@.tty> root - oracle パターンと照合します。条件が満たされると、アラート メッセージが HPOM コンソールに送信されます。

HP-UX 用の Syslog ポリシー

SI-HPUXSyslog

これはログ ファイル監視ポリシーで、var/adm/syslog/syslog.log に入るメッセージを監視します。デフォルトでは、ポーリング間隔は 20 秒です。

このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [HP-UX]

Sun Solaris Bad Logins

SI-SunSolarisBadLogs

これはログ ファイル監視ポリシーで、/var/adm/loginlog ファイルに対する失敗したログインを監視し、不正なログインが発生した場合にユーザーにアラートを送信します。デフォルトでは、ポーリング間隔は 10 秒です。

以下の手順を実行して、Solaris 10 プラットフォーム上での失敗したログインの記録を有効にします。

1. 次のコマンドを実行して、/var/adm ディレクトリに loginlog ファイルを作成します。

   ```
   touch /var/adm/loginlog
   ```

2. 次のコマンドを実行して、loginlog ファイル上でルートに対する読み取りおよび書き込み権限を設定します。

   ```
   chmod 600 /var/adm/loginlog
   ```

3. loginlog ファイル上で、グループ メンバーシップを sys に変更します。

   ```
   chgrp sys /var/adm/loginlog
   ```

4. /etc/syslog.conf 設定ファイルで auth debug を設定します。

   ```
   auth.debug                        ifdef(`LOGHOST', /var/adm/loginlog, @loghost)
   ```

5. 次のコマンドを実行して、記録を開始します。

   ```
   svcadm restart svc:/system/system-log:default
   ```

6. /var/adm/loginlog で失敗したログインの記録を確認し、ポリシーを配布します。

ローカル/リモート ログインの失敗: このポリシーは、失敗したログイン条件を <*.date> <*.ip> ポート <*.port> から <*.user> の失敗した keyboard-interactive 認証と照合します。条件が満たされると、アラート メッセージが HPOM コンソールに送信されます。

このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [Solaris]

Sun Solaris Logins

注: [SI-SunSolarisLogins [1200.0] (Logfile Entry)] ウィンドウの **[ソース]** タブでは、**[実行するファイル*]** ボックスにプリプロセス スクリプトが指定されています。アラートを生成するには、プリプロセス スクリプトの名前を `/usr/bin/sh/var/opt/OV/bin/instrumentation/osspisecurity.sh w` に変更するようにしてください。

SI-SunSolarisLogins

これはログ ファイル監視ポリシーで、`/var/adm/wmptx` ファイルのログイン詳細を監視し、正常なリモート ログイン、ローカル ログイン、システム ログイン、システム ブート、システム シャットダウンなどの発生時にユーザーにアラートを送信します。デフォルトでは、ポーリング間隔は 10 秒です。

ローカル ログインの成功:このポリシーは、正常なローカル ログイン条件を `wtmpx` ファイル内の `LOGIN<@.user> <@.tty> <@.host>` パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

リモート ログインの成功:このポリシーは、正常なリモート ログイン条件を `wtmpx` ファイル内の `LOGIN<@.user> <@.tty> <@.host>` パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

システム ブート:このポリシーは、システム ブート条件を `wtmpx` ファイル内の `BOOT` パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

リモート ユーザー用のシステム シャットダウン: このポリシーは、システム シャットダウン条件を `wtmpx` ファイル内の `SHUTDOWN <@.user> <@,tty>` パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

ローカル ユーザー用のシステム シャットダウン: このポリシーは、システム シャットダウン条件を `wtmpx` ファイル内の `SHUTDOWN` パターンと照合します。条件が満たされると、重要度が注意域のアラート メッセージが HPOM コンソールに送信されます。

このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [Solaris]

Sun Solaris snmp Log ポリシー

SI-SunSolarissnmplog

これはログ ファイル監視ポリシーで、`var/adm/messages` ファイル内の SNMP ログ ファイル エントリを監視します。デフォルトでは、ポーリング間隔は 10 分です。このポリシーは、必要な条件が正常に照合されると、ユーザーにアラートを送信します。

Snmpd ログ ファイル エントリ: SI-SunSolarissnmplog は、matches the snmp ログ ファイル エントリを、snmplog ファイル内の「SNMP メッセージの認証に失敗しました」<*> IP address :<@.ipaddy>, <*>name used:<@. comname>, パターンと照合します。条件が満たされると、アラート メッセージが HPOM コンソールに送信されます。

このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [Solaris]

Sun Solaris Syslog ポリシー

SI-SunSolarisSyslog

これはログ ファイル監視ポリシーで、システム ログ ファイル var/adm/messages に入るメッセージを監視し、必要な条件が正常に照合されると、ユーザーにアラートを送信します。デフォルトでは、ポーリング間隔は 1 分です。

このポリシーのデフォルトのポリシー グループは以下のとおりです。

[Infrastructure Management] → [v12.0] → [<言語>] → [Systems Infrastructure] → [Security] → [Solaris]

HPOM for Windows 管理サーバーからの SI SPI ポリシーの配布

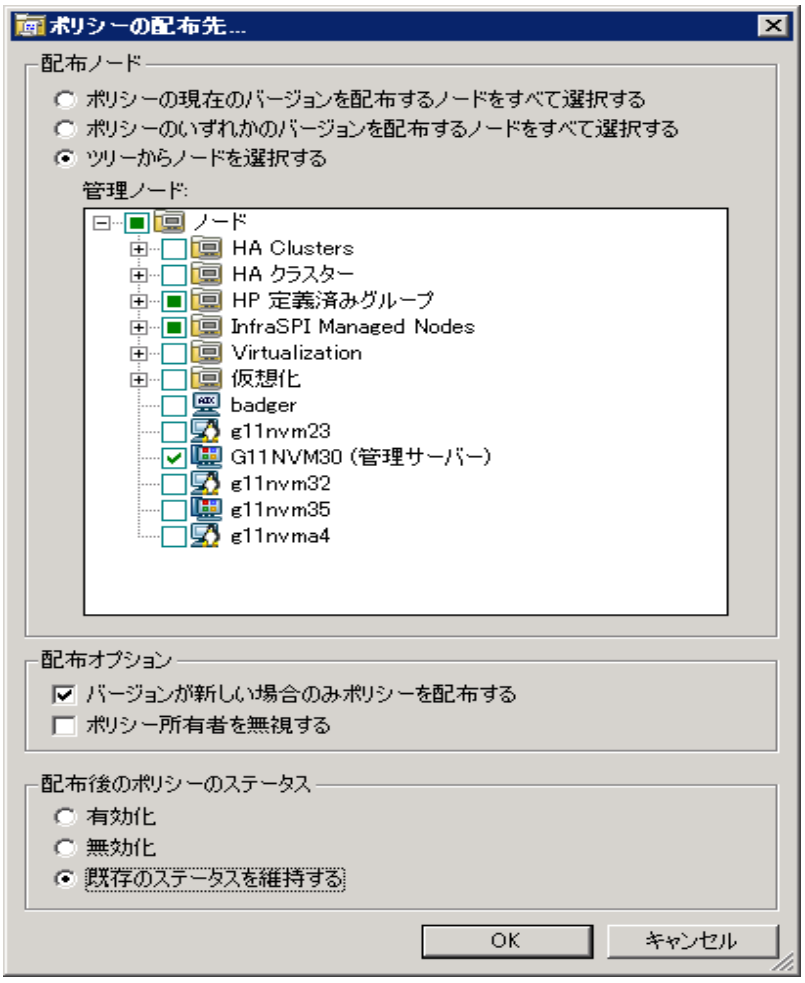
ポリシーを手動で配布するか、ポリシーの自動配布を有効にできます。

ポリシーの自動配布を有効にするには、以下の手順を実行します。

1. サーバー上で自動配布を有効にするには、次のコマンドを実行します。
   /opt/OV/contrib/OpC/autogranting/enableAutoGranting.sh
2. XPL の設定を変更して Infra SPI の自動配布を有効にするには、次のコマンドを実行します。
   ovconfchg -ns infraspi -set AUTODEPLOYMENT true
3. ノードをアクティブにするには、管理サーバー上で次のコマンドを実行します。
   opcactivate -srv <HPOM Server> -cert_srv <HPOM Server> -f
4. 証明書を承諾します。
5. ノードが適切なノード グループに追加されているかどうかを確認します。
6. ノードへのポリシーの自動配布を検証します。

管理サーバーからポリシーを手動で配布するには、以下の手順を実行します。

1. 配布するポリシーを右クリックします。
2. メニューから **[すべてのタスク]** を選択します。
3. **[配布先ノード]** を選択します。[ポリシーの配布先] ダイアログ ボックスが開きます。



4. **[ツリーからノードを選択する]** オプションを選択します。管理ノードのリストから、ポリシーを配布するノードを選択します。
5. **[OK]** をクリックします。

HPOM for UNIX 管理サーバーからの SI SPI ポリシーの配布

ポリシーを配布する前に、管理サーバーに既にノードが追加された状態であり、HP Operations Agent ソフトウェアがインストールされていることを確認してください。管理サーバーにノードを追加する方法の詳細は、『HP Operations Manager for Unix オンライン ヘルプ』を参照してください。

HPOM for UNIX (HP-UX、Linux、Solaris) 管理サーバーからポリシーを配布するには、以下の手順を実行します。

タスク 1: ポリシーまたはポリシー グループの割り当て

1. 管理者として HPOM にログオンします。HPOM 管理者 UI が表示されます。
2. [登録オブジェクト] カテゴリの **[登録ポリシー]** をクリックします。[登録ポリシー] ウィンドウが開きます。
3. [登録ポリシー] ウィンドウで、ノードまたはノード グループに割り当てるポリシーまたはポリシー グループを選択します。
4. **[ノード/ノード グループに割り当て...]** を**[アクションを選択]** ドロップダウン ボックスから選択し、[submit] をクリックします。選択ウィンドウが開きます。
5. ノードまたはノード グループを選択し、**[OK]** をクリックします。選択したポリシーがノードに割り当てられます。

タスク 2: ポリシーの配布

1. HPOM 管理者用インターフェイスから、[登録オブジェクト] カテゴリの **[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。
2. [登録ノード] ウィンドウで、ポリシーの配布先となるノードまたはノード グループを選択します。
3. **[アクションを選択]** ドロップダウン ボックスから **[設定を配布...]** を選択し、[submit] をクリックします。選択ウィンドウが開きます。
4. **[ポリシーの配布]** チェック ボックスをオンにし、**[OK]** をクリックします。このポリシーは、選択したノードに配布されます。

Systems Infrastructure SPI ツール

ツールでは、管理ノード上のサービスを管理したり、特定の管理ノードの収集データを一覧表示できます。

HPOM for Windows で SI SPI ツールにアクセスするには、次を選択します。

[ツール] → **[システム インフラストラクチャ]**

HPOM for UNIX/Linux のコンソール/管理者用インターフェイスからツールにアクセスするには、次を選択します。

[登録ツール] → **[システム インフラストラクチャ]**

ユーザーの前回のログイン ツール

[ユーザーの前回のログイン] ツールを管理ノードで起動すると、すべてのアクティブ ユーザーと、前回のログインに関する詳細情報が一覧表示されます。このツールを起動する前に、対応する Last

Logon Collector ポリシーを導入しておいてください。Last Logon Collector ポリシーの詳細は、「セキュリティ ポリシー」(130ページ)および「セキュリティ ポリシー」(130ページ)を参照してください。

HPOM for Windows 管理サーバーからツールを起動するには、以下の手順を実行します。

1. コンソール ツリーの **[ツール]** フォルダで、**[システム インフラストラクチャ]**フォルダを選択します。
2. 詳細ペインで **[ユーザーの前回のログイン]** ツールを選択し、右クリックするとショートカット メニューが開きます。
3. **[すべてのタスク]** → **[ツールの起動...]** を選択すると、**[このツールの起動場所の選択]** ダイアログ ボックスが開きます。このダイアログ ボックスには、選択したツールを起動できる管理ノードが一覧表示されます。
4. ツールを起動したいノードのチェック ボックスを選択します。**[ノード]** フォルダを選択すると、フォルダ内にあるノードのグループ全体を選択できます。
5. **[起動]** をクリックします。**[ツールのステータス]** ダイアログ ボックスが開き、起動結果が表示されます。起動ツールの実行結果を保存できます。**[起動したツール]** ボックスにある 1 行または複数の行を選択してから、**[保存]** をクリックします。出力がテキスト形式で保存されます。

HPOM for UNIX 管理サーバーからツールを起動するには、以下の手順を実行します。

1. Java インターフェイスで、**[ツール]** → **[システム インフラストラクチャ]** を選択します。
2. < ツール名> ツールを右クリックし、**[カスタマイズ/起動]** を選択します。**[ツール起動 - カスタマイズ ウィザード]** ウィンドウが開きます。
3. ノード リストで、ツールを起動するノードを選択します。
4. ウィザードで **[選択の取込み]** をクリックします。ノードが [選択したノード] リストに追加されます。
5. **[次へ]** をクリックします。[ツール実行に必要な情報を追加してください] ページで、その他の情報を入力するか、各フィールドを空白のままにします。
6. **[完了]** をクリックします。ツールの出力が表示されます。

Energy Data Collector

HP Operations Agent 12.00 がインストールされているシステムでは、Energy Data Collector が、Intelligent Platform Management Interface (IPMI) ツールと共に、メトリック データを収集し、SENSOR という名前のデータソースに格納します。

注: IPMI ツールは、visual C++ 2008 がインストールされている場合にのみ機能します。

Energy Data Collector は、複数の仮想マシンがインストールされている物理マシンのエネルギー使用率を測定します。このツールは、HP Integrated Lights-Out (iLO) が物理マシンにインストールされている場合にのみ機能します。

注: HP Integrated Lights-Out (iLO) は、リモートの場所から HP サーバーを制御および監視する、

リモート サーバー管理プロセッサです。

SENSOR データソースは、Energy Data Collector ツールの配布後にのみ作成されます。SENSOR データソースは、次のメトリック クラスから構成されています。

- OEM_RESERVED
- POWER_SUPPLY
- FAN
- TEMPERATURE
- MEMORY
- CURRENT

サポートされているプラットフォーム	**Linux**
OEM_RESERVED に使用されるメトリック	SNSR_OEM_RESERVED_ID SNSR_OEM_RESERVED_NAME SNSR_OEM_RESERVED_TYPE SNSR_OEM_RESERVED_READING SNSR_OEM_RESERVED_UNITS SNSR_OEM_RESERVED_EVENTS
POWER_SUPPLY に使用されるメトリック	SNSR_POWER_SUPPLY_ID SNSR_POWER_SUPPLY_NAME SNSR_POWER_SUPPLY_TYPE SNSR_POWER_SUPPLY_READING SNSR_POWER_SUPPLY_UNITS SNSR_POWER_SUPPLY_EVENTS
FAN に使用されるメトリック	SNSR_FAN_ID SNSR_FAN_NAME SNSR_FAN_TYPE SNSR_FAN_READING SNSR_FAN_UNITS SNSR_FAN_EVENTS

TEMPERATURE に使用されるメトリック	SNSR_TEMPERATURE_ID SNSR_TEMPERATURE_NAME SNSR_TEMPERATURE_TYPE SNSR_TEMPERATURE_READING SNSR_TEMPERATURE_UNITS SNSR_TEMPERATURE_EVENTS
MEMORY に使用されるメトリック	SNSR_MEMORY_ID SNSR_MEMORY_NAME SNSR_MEMORY_TYPE SNSR_MEMORY_READING SNSR_MEMORY_UNITS SNSR_MEMORY_EVENTS
CURRENT に使用されるメトリック	SNSR_CURRENT_ID SNSR_CURRENT_NAME SNSR_CURRENT_TYPE SNSR_CURRENT_READING SNSR_CURRENT_UNITS SNSR_CURRENT_EVENTS

サポートされているプラットフォーム	**Windows**
OEM_RESERVED に使用されるメトリック	SNSR_OEM_RESERVED_ID SNSR_OEM_RESERVED_NAME SNSR_OEM_RESERVED_TYPE SNSR_OEM_RESERVED_READING SNSR_OEM_RESERVED_UNITS SNSR_OEM_RESERVED_EVENTS

POWER_SUPPLY に使用されるメトリック	SNSR_POWER_SUPPLY_ID SNSR_POWER_SUPPLY_NAME SNSR_POWER_SUPPLY_TYPE SNSR_POWER_SUPPLY_READING SNSR_POWER_SUPPLY_UNITS SNSR_POWER_SUPPLY_EVENTS
POWER_UNIT に使用されるメトリック	SNSR_POWER_UNIT_ID SNSR_POWER_UNIT_NAME SNSR_POWER_UNIT_TYPE SNSR_POWER_UNIT_READING SNSR_POWER_UNIT_UNITS SNSR_POWER_UNIT_EVENTS
FAN に使用されるメトリック	SNSR_FAN_ID SNSR_FAN_NAME SNSR_FAN_TYPE SNSR_FAN_READING SNSR_FAN_UNITS SNSR_FAN_EVENTS
TEMPERATURE に使用されるメトリック	SNSR_TEMPERATURE_ID SNSR_TEMPERATURE_NAME SNSR_TEMPERATURE_TYPE SNSR_TEMPERATURE_READING SNSR_TEMPERATURE_UNITS SNSR_TEMPERATURE_EVENTS
MEMORY に使用されるメトリック	SNSR_MEMORY_ID SNSR_MEMORY_NAME SNSR_MEMORY_TYPE SNSR_MEMORY_READING SNSR_MEMORY_UNITS SNSR_MEMORY_EVENTS

CURRENT に使用されるメトリック	SNSR_CURRENT_ID SNSR_CURRENT_NAME SNSR_CURRENT_TYPE SNSR_CURRENT_READING SNSR_CURRENT_UNITS SNSR_CURRENT_EVENTS

Windows または Linux ノードでの Energy Data Collector の起動

以下の手順を実行します。

1. コンソール ツリーで、**[ツール]** -> **[システム インフラストラクチャ]** フォルダを選択します。
2. ツール グループを選択します。

   Windows の場合:

   [Energy Data Collector] -> **[Windows]**

   Linux の場合:

   [Energy Data Collector] -> **[Linux]**
3. **[収集の開始/停止]** をダブルクリックします。[このツールの起動場所の選択] ウィンドウが開きます。
4. ツールを起動するノードを選択し、**[起動]** をクリックします。[パラメータの編集] ウィンドウが開きます。
5. データ収集を開始するには、[パラメータ] フィールドに、「**開始**」と入力し、**[起動]** をクリックします。

注: データ収集を停止するには、**[パラメータ]** フィールドに、「**停止**」と入力し、**[起動]** をクリックします。

第6章: Systems Infrastructure SPI のレポートとグラフ

SI SPI と HP Reporter を統合することにより、管理ノードから収集したメトリック データに基づいてレポートを生成できます。レポートから、システム リソースの全体像を把握できます。また、グラフを作成して、収集されたメトリック データを分析することもできます。SI SPI で収集したデータからレポートとグラフを作成して表示するには、HP Reporter と HP Performance Manager を HPOM と併用します。

Systems Infrastructure SPI のレポート

レポートから、システム リソースの全体像を把握できます。SI SPI と HP Reporter を統合することにより、管理ノードから収集したメトリック データに基づいてレポートを生成できます。

SI SPI のレポートには、HPOM for Windows コンソールからアクセスできます。SI SPI 向けに HP Reporter パッケージをインストールする手順については、『HP Operations Smart Plug-ins for Infrastructure インストール ガイド』を参照してください。

HPOM for Windows から SI SPI のレポートを表示するには、コンソール ツリーで **[レポート]** → **[Systems Infrastructure]** を選択して展開します。必要なレポートを選択して右クリックし、**[レポートの表示]** を選択すると、レポートが表示されます。

HP Reporter を HPOM 管理サーバーにインストールした場合、管理サーバーでレポートを直接表示できます。

HPOM 管理サーバーに接続されている別のシステムに HP Reporter をインストールした場合、HP Reporter システムでレポートを表示できます。HP Reporter と HPOM を統合する方法の詳細は、『HP Reporter Installation and Special Configuration Guide』を参照してください。以下に、レポートの例を示します。

図 3: Systems Infrastructure SPI のレポートの例

Unused Logins

for Group Systems Infrastructure

This report was prepared: 8/11/2009, 3:00:53 AM

This report shows the login information for all the managed nodes.

aspint7-sol.ov.test

Login Name	Dates in Database	Last Login Date	Day Since Login (DD:HH:MM:SS)
root	08/09/2009 - 07/29/2009	8/4/2009 11:59:32PM	2:13:30:28

Never Logged in User List

halt
netdump
news
opc_op
shutdown
sync
vi-user

btovm555.ov.test

Login Name	Dates in Database	Last Login Date	Day Since Login (DD:HH:MM:SS)
vi-admin	08/08/2009 - 07/29/2009	8/5/2009 11:59:05PM	0:19:05:55

Never Logged in User List

halt
netdump
news
opc_op
shutdown
sync
vi-user

SI SPI には、以下のレポートが用意されています。

レポート/レポートのタイトル	目的
System Last Login	特定のログインが管理ノード上で最後に使用された日時が表示されます。また、これまでに一度もログインしていないユーザーが一覧表示されます。データは、日付および時刻順にソートされます。このレポートでは、使用されていないユーザー アカウントや古くて無効になったユーザー アカウントを特定できます。
System Failed Login	管理ノード上で発生したログインの失敗がすべて一覧表示されます。このレポートでは、管理ノードにログインを繰り返し試行する不正ユーザーがいないかどうかを把握できます。
System Availability	システムに関する可用性情報が表示されます。このレポートでは、勤務時間外、週末、祭日を除くデータベース内の日付範囲について、システム稼働時間の比率やダウンタイムの長さに関する情報を把握できます。
Top CPU Process	CPU 使用率が高いシステムが表示されます。このレポートのデータに基づいて、レポート期間中に大量の CPU サイクルを消費しているシステムを分析できます。
Top Memory Process	メモリ使用量が多いシステムが表示されます。このレポートのデータに基づいて、レポート期間中に大量のメモリ容量を消費しているシステムを分析できます。

Systems Infrastructure SPI のグラフ

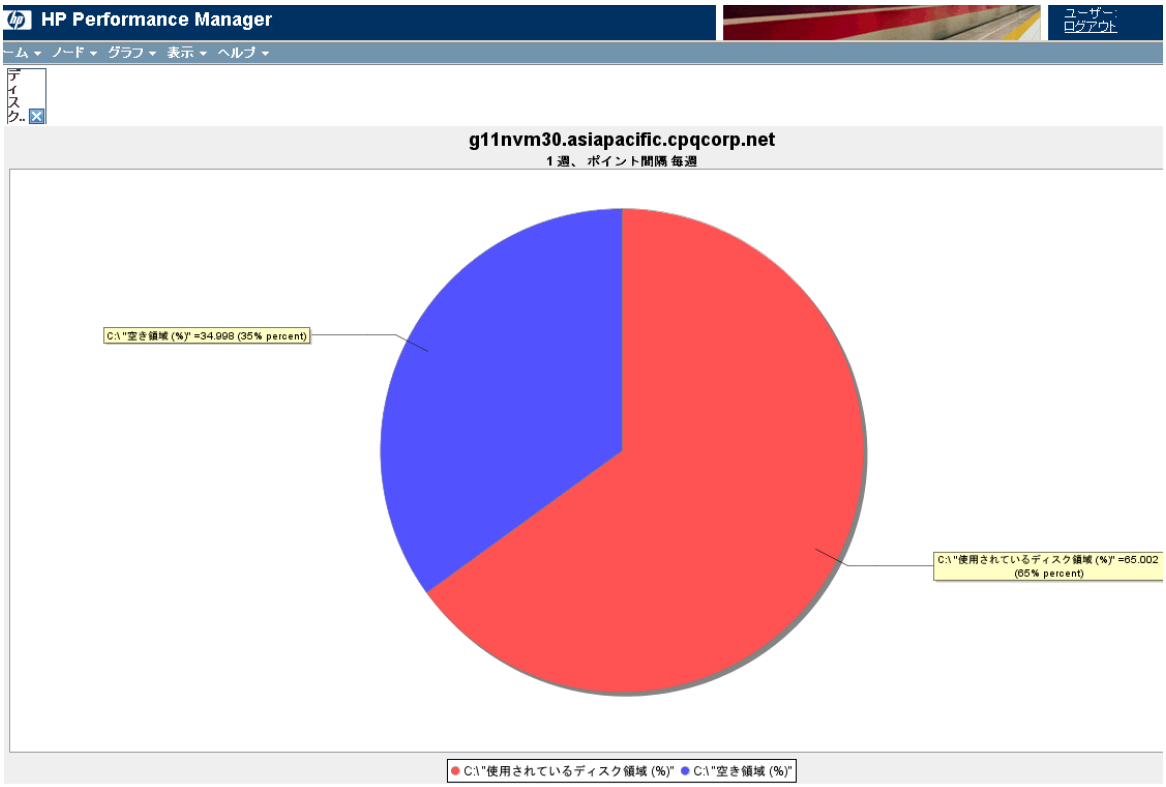
HP Performance Manager では、管理ノードで収集されたほぼリアルタイムのデータを元にグラフが生成されます。HP Performance Manager を HPOM 管理サーバーにインストールしている場合、HPOM コンソールからこれらのグラフにアクセスできます。

SI SPI には、設定済みのグラフがいくつか用意されています。これらのグラフは、HPOM コンソール ツリーの [Graphs] フォルダにあります。この [Graphs] フォルダにアクセスできるのは、HPOM 管理サーバーに HP Performance Manager をインストールした場合のみです。以下に、グラフの例を示します。

HPOM for Windows でグラフにアクセスするには、**[Graphs]** → **[Infrastructure Performance]** を選択します。

HPOM for UNIX/Linux/Solaris で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] 項で、**[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。

図 4: Systems Infrastructure SPI のグラフの例



Systems Infrastructure SPI には、以下のグラフが用意されています。

グラフ	グラフの設定
ディスク	• ディスク使用率 • ディスクの概要 • ディスクのスループット • ディスク領域 • ディスク容量 (円グラフ) • ディスクの詳細
グローバル パフォーマンス	• 全体の履歴 • グローバル実行キューのベースライン • 全体の詳細 • 複数のグローバル予測

CPU	• CPU の概要 • CPU 使用率の概要 • 個々の CPU • CPU の比較 • CPU ゲージ • CPU の詳細 • 全体的な CPU の予測 • 季節を考慮した CPU の予測
ネットワーク	• ネットワークの概要 • 個々のネットワーク • ネットワーク インターフェイスの詳細
メモリ	• メモリの概要 • 物理メモリ使用率
設定	• 構成の概要 • システム構成
トランザクション	• トランザクションの正常性 • トランザクションの履歴 • トランザクションの詳細 • トランザクションの応答予測
ファイル システム	ファイル システムの詳細
アプリケーション	• アプリケーション CPU ゲージ • アプリケーション CPU 予測 • アプリケーションの履歴 • アプリケーションの詳細
プロセス	プロセスの詳細

第7章: トラブルシューティング

この章では、SI SPI 問題のトラブルシューティングに役立つ情報、および問題の発生を回避するのに役立つ情報を提供します。

問題	ハードウェア監視ポリシーがアラートを送信しない。
解決策	以下の手順を実行します。 • snmpd サービスが停止している場合は、開始します。 `# /etc/init.d/snmpd start` • opctrapi がポート番号 162 で設定されていることを確認します。

問題	HPOM コンソールに警告/エラー メッセージが表示される。
	`An error occurred in the processing of the policy 'SI-DiskCapacityMonitor'. ('SI-DiskCapacityMonitor' ポリシーの実行中にエラーが発生しました。)Please check the following errors and take corrective actions. (以下のエラーを確認して適切なアクションを取ってください。)(OpC30-797)`
	`Initialization of collection source "DoNotRename" failed. (コレクション ソース "DoNotRename" の初期化に失敗しました。) (OpC30-724)`
	`Cannot find object 'FILESYSTEM' in Coda object list. (Coda オブジェクト リスト内で 'FILESYSTEM' オブジェクトが見つかりません。)(OpC30-761)`
	`Searching for 'data source: SCOPE' in the DataSourceList failed. (DataSourceList での 'data source: SCOPE' の検索に失敗しました。)(OpC30-766)`

原因	HP Performance Agent がインストールされていないノードに SI-DiskCapacityMonitor ポリシーを配布すると、このエラーが発生します。SI-DiskCapacityMonitor ポリシーは、SCOPE が提供するメトリックを使用し、正常に動作するためには HP Performance Agent が必要です。
解決策	管理ノードに HP Performance Agent をインストールします。これにより、ポリシーは正常に機能します。

問題	HPOM for UNIX の管理者用 GUI で変更した高度な監視ポリシーを管理ノードに配布した後、実行できない。
原因	HPOM for UNIX ポリシー エディタのユーザー インターフェイス モードで高度な監視ポリシーを編集すると、Perl コード モジュールで構文エラーが発生します。そのため、ポリシーを実行できません。以下のようなエラーが表示されます。 `An error occurred in the processing of the policy 'SI-LinuxSshdProcessMonitor'. ('SI-LinuxSshdProcessMonitor' ポリシーの実行中にエラーが発生しました。)Please check the following errors and take`

	corrective actions. (以下のエラーを確認して適切なアクションを取ってください。) (OpC30-797) Error during evaluation of threshold level "Processes - Fill Instance list" (しきい値レベル "Processes - Fill Instance list" の評価中にエラーが発生しました) (OpC30-728) Execution of instance filter script failed. (インスタンス フィルタ スクリプトの実行に失敗しました。)(OpC30-714) Perl Script execution failed: syntax error at PerlScript line 11, near "1 (Perl スクリプトの実行に失敗しました。Perl スクリプトの 11 行目、"1 の近くに構文エラーがあります) #BEGIN_PROCESSES_LIST #ProcName=/usr/sbin/sshd #Params= #Params= #MonMode=>= #ProcNum=1 #END_PROCESSES_LIST @ProcNames" Missing right curly or square bracket at PerlScript line 17, within string (Perl スクリプトの 17 行目の文字列に右中括弧または右角括弧がありません) syntax error at PerlScript line 17, at EOF. (Perl スクリプトの 17 行目、EOF に構文エラーがあります。) (OpC30-750) 未編集の高度な監視ポリシー ([Measurement Threshold] タイプ) を HPOM for UNIX から配布して使用できます。
解決策	Measurement Threshold ポリシーの設定を編集するため、HPOM for UNIX の管理者用 GUI の「編集 (Raw モード)」機能を使用してポリシーの内容を変更します。そのためには、ポリシー データ ファイルの構文を理解している必要があります。

問題	HPOM for UNIX (バージョン 9.00) オペレータ コンソールから SI SPI グラフを表示するコマンドをオペレータが実行すると、エラーが発生する。
解決策	HPOM サーバーで次のコマンドを実行してください。 /opt/OV/contrib/OpC/OVPM/install_OVPM.sh <OMU サーバー名>:8081

問題	英語以外の名前を使用すると、検出手順とデータ収集でエラーが発生する。

原因	英語版以外の HP Operations Manager では、SI SPI をインストールすることはできますが、名前に英語以外の言語を使用するとエラーが発生します。このエラーは、HP Operations Agent のストア コレクション Perl API が英語以外の名前を認識できないことが原因で発生します。
解決策	クラスターやリソース グループの名前には英語を使用してください。

問題	システム検出でノードが自動追加されるときに、アラート メッセージが表示される。
原因	クラスター環境や仮想化環境でノードを自動追加する際、システム検出ポリシーによって、通常の重要度でアラート メッセージが生成されます。ポリシーの自動追加機能によってノード バンクにノードを追加する処理には時間がかかるので、アラート メッセージが受諾されるまでに若干の時間がかかります。
解決策	次に示す XPL 設定パラメータのデフォルト値を変更して、自動追加機能を無効にします。 • AutoAdd_ClusterNode: デフォルト値は「True」です。「False」に変更します。 • AutoAdd_Cluster_RG_IP: デフォルト値は「True」です。「False」に変更します。 • AutoAdd_HypervisorNode: デフォルト値は「True」です。「False」に変更します。 • AutoAdd_Guests: デフォルト値は「False」です。「True」に変更します。

問題	HPOM コンソールに警告/エラー メッセージが表示される。 Check the following errors and take corrective actions. (以下のエラーを確認して適切なアクションを取ってください。)(OpC30-797) Error during evaluation of threshold level "CPU Spikes level Critical" (しきい値レベル "CPU Spikes level Critical" の評価中にエラーが発生しました) (OpC30-728) Execution of threshold script failed. (しきい値スクリプトの実行に失敗しました。)(OpC30-712) Perl Script execution failed:Can't locate OvTrace.pm in @INC (@INC contains:/usr/lpp/OV\lbin\eaagt\perl /usr/lpp/OV/lbin/eaagt/perl /var/opt/OV/bin/instrumentation /usr/lpp/OV/nonOV/perl/a/lib/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl .) at PerlScript line 136. (Perl スクリプトの実行に失敗しました。Perl スクリプトの 136 行目の @INC (@INC には以下が含まれています。/usr/lpp/OV\lbin\eaagt\perl /usr/lpp/OV/lbin/eaagt/perl /var/opt/OV/bin/instrumentation /usr/lpp/OV/nonOV/perl/a/lib/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl) 内に OvTrace.pm が見つかりません。) BEGIN failed--compilation aborted (in cleanup) Can't locate OvTrace.pm in @INC (@INC contains:/usr/lpp/OV\lbin\eaagt\perl /usr/lpp/OV/lbin/eaagt/perl /var/opt/OV/bin/instrumentation /usr/lpp/OV/nonOV/perl/a/lib/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl .) at PerlScript line 136. (BEGIN が失敗しました。コンパイルは中断しました (クリーンアップ) Perl スクリプトの 136 行目の @INC (@INC には以下が含まれています。/usr/lpp/OV\lbin\eaagt\perl /usr/lpp/OV/lbin/eaagt/perl /var/opt/OV/bin/instrumentation /usr/lpp/OV/nonOV/perl/a/lib/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8/aix-thread-multi /usr/lpp/OV/nonOV/perl/a/lib/site_perl/5.8.8 /usr/lpp/OV/nonOV/perl/a/lib/site_perl) 内に OvTrace.pm が見つかりません。) BEGIN failed--compilation aborted at PerlScript line 136. (BEGIN が失敗しました。コンパイルは Perl スクリプトの 136 行目で中断しました。) (OpC30-750)
原因	インストルメンテーションがノードに正しく配布されないと、任意のポリシーと *.pm ファイルでこのエラーが発生します。
解決策	インストルメンテーションをノードに強制的に配布します。

問題	StoreCollection によって、SI-MSWindowsFailedLoginsCollector ポリシーの coda_SetUTF8: coda_set_fcn_mismatch_data_type (80004005) エラーが発生する。
解決策	Windows ノード上で以下のコマンドを実行して、CODA ファイルを再利用します。 1. `ovc -stop coda` 2. `rm -rf /var/opt/OV/datafiles/coda*` 3. `ovc -start coda`

問題	Windows ノードでは、新しいバージョンの設定ファイル ポリシー SI-RealTImeAlerts ポリシーを配布後も、アラートが前のバージョンのポリシーに送信されます。
原因	SI-RealTImeAlerts ポリシーを適切に配布しなければ、前のバージョンの padv プロセスが抹消されず、実行し続けます。このため、アラートが前のバージョンのポリシーに送信されます。

解決策	次のコマンドを実行して、プロセス ID を取得します。
	`ps-ef|grep padv`
	次のコマンドを実行して、前のバージョンの padv プロセスを抹消します。
	`kill <プロセス ID>`

ドキュメントのフィードバックを送信

本ドキュメントについてのご意見、ご感想については、電子メールでドキュメント制作チームまでご連絡ください。このシステムで電子メールクライアントが設定されていれば、このリンクをクリックすることで、以下の情報が件名に記入された電子メールウィンドウが開きます。

Feedback on ユーザー ガイド (Operations Smart Plug-in for Systems Infrastructure 12.00)

本文にご意見、ご感想を記入の上、[送信] をクリックしてください。

電子メールクライアントが利用できない場合は、上記の情報をコピーして Web メールクライアントの新規メッセージに貼り付け、 docfeedback@hp.com 宛にお送りください。

お客様からのご意見、ご感想をお待ちしています。