内部 SNMP トラップの生成

内部トラップ生成について

適切に設定されている場合、Prime Infrastructure は通知宛先に SNMP トラップを送信し、Prime Infrastructure システム自体で発生する次のイベントを通知します。

- Prime Infrastructure サーバーの内部ソフトウェア プロセスのクラッシュまたは障害。
- 登録、フェールオーバー、およびフェールバックを含む高可用性（HA）状態の変更。
- CPU、メモリ、ディスクの高い使用率。
- CPU、ディスク、ファン、または電源装置（PSU）の障害。
- バックアップ障害、証明書の失効、ライセンス違反。

これらの内部 SNMP トラップに関連付けられているシビラティ（重大度）を編集できます。CPU、メモリ、およびディスクの使用率に関するしきい値限度を変更することもできます（これらの SNMP トラップはシステム ハードウェアが設定されたしきい値を超えた場合に送信されます）。

その他のイベント（CPU、ディスク、ファン、および PSU の障害、または HA 状態の変更など）の場合は、障害や HA 状態の変更が検出されるとすぐに SNMP トラップが送信されます。

SNMP トラップは次のイベントに対してカスタマイズされたしきい値とシビラティ（重大度）に基づいて生成されます。

- サーバ プロセス障害
- 高可用性操作
- CPU 使用率
- メモリ使用率

- ディスク使用率
- ディスク障害
- ファン障害
- PSU の障害
- バックアップ障害
- 証明書の失効

Prime Infrastructure は SNMPv2 通知も SNMPv3 通知も送信しません。

（注） デバイスのトラップが無効になっていても、Prime Infrastructure にはポートの使用不可を示すアラームが表示されます。

Prime Infrastructure SNMP トラップ タイプ

次の表に、Prime Infrastructure が独自の機能に対して生成する SNMP トラップを示します。リストはトラップ タイプ別になっています。表では、各トラップが生成される状況のほか、提案される操作対応を説明しています。

表 *1 : Prime Infrastructure SNMP* トラップ タイプ

トラップ タイプ	トラップ	説明
アプライアンス プロセス障害	FTP、MATLAB、TFTP	Prime Infrastructure サーバーで FTP、MATLAB、または TFTP プロセスの障害が発生した場合、サーバーは常に障害トラップを生成し、サーバーのヘルス モニター インスタンスはプロセスを自動的に再起動することを試みます。ヘルス モニターが 3 回の試行で再起動できなかった場合、HA サーバーは別の障害トラップを送信します。
アプライアンス プロセス障害	NMS	サーバーの NMS プロセスが開始するか、または障害を起こすと、Prime Infrastructure サーバーのヘルス モニター スレッドは常に、対応するトラップを生成します。 プロセスを停止または再起動するには、サーバーに CLI から接続し、管理者でログインします。次に、適宜、nms stop コマンドまたは nms start コマンドを実行します。
HA 操作	登録トリガー	Prime Infrastructure はプライマリ サーバーが HA 登録を開始すると常に、このトラップを生成します。登録が失敗するか成功するかは関係ありません。HA 登録がトリガーされると、プライマリ サーバーは操作の開始を示すトラップを生成します。
HA 操作	登録成功	HA 登録が成功すると、プライマリ サーバーは成功を示すこのトラップを生成します。

内部 SNMP トラップの生成

トラップ タイプ	トラップ	説明
HA 操作	登録失敗	HA 登録が何らかの理由で失敗した場合、障害が発生したプライマリまたはセカンダリ サーバーは、失敗を示すトラップを生成します。このトラップには、障害に関する詳細が含まれます。支援が必要な場合は、Cisco Technical Assistance Center（TAC）にお問い合わせください。
HA 操作	フェールオーバー トリガー	このトラップは Prime Infrastructure プライマリ サーバーに障害が発生した場合、自動的に生成され、フェールオーバーの一部として、セカンダリ サーバーのアクティブ化を試みます（フェールオーバーの成否やセカンダリ サーバーのアクティブ化の成否に関係なく行われます）。HA 設定（登録時の設定）に手動フェールオーバー タイプがある場合、ユーザーはフェールオーバーをトリガーする必要があります。そうでない場合、ヘルス モニターはセカンダリ サーバーへのフェールオーバーを自動的にトリガーします。 フェールオーバーがトリガーされたことを示すために 1 個のトラップが生成されます。フェールオーバーが完了する前にトラップが送信されるため、セカンダリ サーバーにはロギングされません。
HA 操作	フェールオーバー成功	トリガーされたフェールオーバー操作が成功すると、セカンダリ サーバーは成功を示すトラップを生成します。ユーザーはセカンダリ サーバーのアラーム ブラウザでトラップを表示できます。
HA 操作	フェールオーバー失敗	トリガーされたフェールオーバー操作が失敗すると、失敗を示すトラップが生成されます。ユーザーは hm-#-#.log でトラップを表示できます（「Prime Infrastructure SNMP トラップのトラブルシューティング方法 （23 ページ）」を参照）。このトラップには、障害に関する詳細が含まれます。サポートが必要な場合は、Cisco TAC にお問い合わせください。他の障害トラップの場合と同様に、障害が自動的に修復されると、アラームと「クリア」トラップが送信されます。
HA 操作	フェールバック トリガー	このトラップはセカンダリ サーバーでプライマリ サーバーへのフェールバックがトリガーされると自動的に生成されます（フェールバックの成否に関係なく行われます）。プライマリ サーバーが復元された後、ユーザーはセカンダリ サーバー ヘルス モニターの Web ページにある [フェールバック（Failback）] ボタンを使用して、セカンダリ サーバーからプライマリ サーバーへのフェールバックをトリガーする必要があります（自動のフェールバック オプションはありません）。トリガーされると、セカンダリ サーバーは操作の開始を示すトラップを生成します。
HA 操作	フェールバック成功	トリガーされたフェールバック操作が成功すると、セカンダリ サーバーは成功を示すトラップを生成します。フェールバック成功により、プライマリ サーバーは「アクティブ」状態に設定され、セカンダリ サーバーは「同期」状態に設定されます。

内部 SNMP トラップの生成

トラップ タイプ	トラップ	説明
HA 操作	フェールバック失敗	トリガーされたフェールバック操作が失敗すると、失敗を示すトラップが生成されます。障害はどちらのサーバーでも発生する可能性があるので、障害が発生したサーバーがトラップを生成します。ユーザーは hm-#-#.log およびノースバウンド管理サーバーでトラップを表示できます。 フェールバック失敗は自動ロールバックをトリガーし、セカンダリ サーバーは前のアクティブ状態に戻ることを試みます。この操作に失敗すると、セカンダリ サーバーはロールバック失敗を示す追加のトラップを生成します。この障害トラップには障害に関する詳細が含まれます。サポートが必要な場合は、Cisco TAC にお問い合わせください。他の障害トラップの場合と同様に、障害が自動的に修復されると、アラームと「クリア」トラップが送信されます。
ハードウェア トラップ	CPU 使用率	トラップは CPU 使用率がプリセットされた使用率のしきい値を超える場合にのみ送信されます。これらのトラップを表示するには、トラップを生成したサーバーのジョブとアクティブ セッションを確認します。
ハードウェア トラップ	ディスク使用率	トラップはディスク使用率が設定されたディスク使用率のしきい値限度を超える場合にのみ送信されます。対応するには、/opt および /localdisk パーティションの下のディスク領域を解放してみます。Cisco TAC の指導なしで /opt/CSCOlumos の下のフォルダを削除しないでください。
ハードウェア トラップ	メモリ使用率	トラップはメモリ使用率が設定されたメモリ使用率のしきい値限度を超える場合にのみ SNMP トラップ レシーバに送信されます。
ハードウェア トラップ	ディスク障害	トラップはディスク障害が検出された場合に SNMP トラップ レシーバに送信されます。修正措置については、ローカル システム管理者にお問い合わせください。他の障害トラップの場合と同様に、障害が自動的に修復されると、アラームと「クリア」トラップが送信されます。
ハードウェア トラップ	ファン障害	トラップはファン障害が検出された場合に SNMP トラップ レシーバに送信されます。トラップまたはアラーム メッセージに不良または欠落したファンが表示されます。修正措置については、ローカル システム管理者にお問い合わせください。他の障害トラップの場合と同様に、障害が自動的に修復されると、アラームと「クリア」トラップが送信されます。
ハードウェア トラップ	PSU の障害	トラップは PSU 障害が検出された場合に SNMP トラップ レシーバに送信されます。トラップまたはアラーム メッセージに問題のある電源が表示されます。修正措置については、ローカル システム管理者にお問い合わせください。他の障害トラップの場合と同様に、障害が自動的に修復されると、アラームと「クリア」トラップが送信されます。

内部 SNMP トラップの生成

トラップ タイプ	トラップ	説明
しきい値トラップ	バックアップ障害	Prime Infrastructure サーバー バックアップの毎日のバックグラウンド タスクで障害が検出されると、トラップが SNMP トラップ レシーバに送信されます。バックグラウンドタスクは毎日実行され、スケジュール設定された時刻にサーバーのバックアップが取得されます。ディスク領域の不足によりバックアップに失敗すると、そのイベントが処理されます。バックアップが正常に実行されると、アラームはクリアされます。
しきい値トラップ	バックアップしきい値	Prime Infrastructure でスケジュール設定された毎日のバックアップが、しきい値日数の間取得されなかった場合、ユーザーに通知されます。デフォルトのしきい値は 7 日です。バックアップが 7 日間取得されなかった場合、ユーザーはこのイベントによって通知されます。
しきい値トラップ	証明書有効期日	証明書が有効期日間近になると、トラップが SNMP トラップ レシーバに送信されます。証明書の有効期日の 15 日前になると Critical トラップが送信され、証明書の有効期日の 60 日前になると Major トラップが送信されます。
システム トラップ	ライフサイクル	ライフサイクル ライセンスは、デバイスの管理に使用されます。ライセンス使用率が所定のしきい値パーセンテージを超えると、アラームが生成されます。デフォルトでは、使用率が 80 % を超えると、トラップが送信されます。ただし、これはカスタマイズ可能です。
システム トラップ	保証	保証ライセンスは、NetFlow を Prime Infrastructure に送り込むデバイスの表示に使用されます。ライセンス使用率が所定のしきい値パーセンテージを超えると、アラームが生成されます。デフォルトでは、使用率が 80 % を超えると、トラップが送信されます。ただし、これはカスタマイズ可能です。
システム トラップ	コレクタ	コレクタ ライセンスは、Prime Infrastructure に送り込まれた NetFlow の量の表示に使用されます。ライセンス使用率が所定のしきい値パーセンテージを超えると、アラームが生成されます。デフォルトでは、使用率が 80 % を超えると、トラップが送信されます。ただし、これはカスタマイズ可能です。
システム トラップ	ライフサイクル ライセンス	ライセンスの有効期日がしきい値限度を下回ると、トラップが送信されます。デフォルトでは、トラップが送信される限度は 30 日です。ただし、この限度は 1 ～ 99 日の間でカスタマイズできます。このイベントは、評価ライセンスを使用する場合のみ考慮されます。
システム トラップ	保証ライセンス	ライセンスの有効期日がしきい値限度を下回ると、トラップが送信されます。デフォルトでは、トラップが送信される限度は 30 日です。ただし、この限度は 1 ～ 99 日の間でカスタマイズできます。このイベントは、評価ライセンスを使用する場合のみ考慮されます。
システム トラップ	コレクタ ライセンス	ライセンスの有効期日がしきい値限度を下回ると、トラップが送信されます。デフォルトでは、トラップが送信される限度は 30 日です。ただし、この限度は 1 ～ 99 日の間でカスタマイズできます。このイベントは、評価ライセンスを使用する場合のみ考慮されます。

汎用 SNMP トラップの形式

次に、Prime Infrastructure の SNMP トラップ通知のシンタックスを示します。

Component：コンポーネント名、**Server**：Primary、Secondary、または Standalone、**Type**：Process、Sync、Activity など、**Service**：サービス名、**When**：Prime Infrastructure ライフサイクルでのフェーズ、**State**：サーバーの HA および HM の状態、**Result**：Warning、Failure、Success、Information、Exception、**MSG**：通知される SNMP トラップに関する自由形式のメッセージ

表 A-2 に、汎用トラップ形式の各属性について可能な値を示しています。

表 *2*：汎用 *SNMP* トラップ形式の属性値

属性	値
コンポーネント	Health Monitor または High Availability
サーバ	このトラップの送信元サーバ（Primary、Secondary、または Standalone）
タイプ	このトラップの原因となったアクションのタイプ（Process、Sync、Activity など）
サービス	この問題を報告した Prime Infrastructure サービス。取り得る値には、Registration、Failover、Failback、NMS、NCS、Health Monitor、All、Prime Infrastructure、Database、Disk Space などがあります。
日時（When）	このトラップが発生した Prime Infrastructure サーバーのライフサイクルにおける時点（Startup、Shutdown など）
状態（State）	サーバの状態（Standalone、Failover、Failback、Registration など）
結果	この SNMP トラップがレポートされている条件
MSG	各 SNMP トラップに固有の詳細を提供する自由形式のテキスト

ノースバウンド SNMP トラップとアラームのマッピング

次の表に、ノースバウンド トラップが Prime Infrastructure のイベントとアラームにマッピングされる仕組みに関する説明を示します。次の表の「イベント」列の項目は、「Prime Infrastructure Supported Events」ドキュメントの [イベント（Events）] タブの列名であり、追加情報が含まれています。たとえば、この表の MIB 変数「cWNotificationSubCategory」では、「*Supported Events*」ドキュメントの [イベント/アラーム条件（Event/Alarm Condition）] 列を調べ、転送されたイベントまたはアラームで報告または解決されている問題のタイプを調べます。

内部 SNMP トラップの生成

表 *3:* ノースバウンド *SNMP* トラップとアラームのマッピング

MIB 変数名	関連付けられているアラームのフィールド	GUI 名	イベント	詳細
cWNotificationIndex	なし。各トラップに対して一意に生成されます。	なし	なし	各ノースバウンド トラップが送信されると増加する（折り返して 1 に戻る）インデックス値。
cWNotificationTimestamp	alarmCreationTime	アラーム検出日時（Alarm Found At）	なし	関連付けられているアラームが作成された時刻。
cWNotificationUpdatedTimestamp	lastModifiedTimestamp	[タイムスタンプ（Timestamp）]（列）、[アラーム最終更新日時（Alarm Last Updated At）]	なし	関連付けられているアラームが最後に更新された時刻。
cWNotificationKey	applicationSpecificAlarmID	なし	なし	アラーム条件を一意に識別する（不明瞭な）文字列。これは基本的にアラームの「識別子」です。同じ cWNotificationKey で 2 つのノースバウンドトラップ（最初のトラップはシビラティ（重大度）がクリアされていない、2 番目のトラップはシビラティ（重大度）がクリアされている）を受信した場合は、最初のトラップで報告された問題が 2 番目のトラップでクリアされていると判断できます。

内部 SNMP トラップの生成

MIB 変数名	関連付けられているアラームのフィールド	GUI 名	イベント	詳細
cWNotificationCategory	category	カテゴリ（Category）	デフォルトカテゴリ	関連付けられているアラームのカテゴリ。実際の値は数値であり、「*Prime Infrastructure Supported Events*」ドキュメントに含まれている実際のカテゴリ名にマップできます。マッピングはMIBで使用可能です。
cWNotificationSubCategory	eventType	条件	イベント/アラーム条件	報告または解決されている問題のタイプを示します。
cWNotificationManagedObjectAddressType	なし	なし	なし	IPv4 を示します。
cWNotificationManagedObjectAddress	reportingEntityAddress	なし	なし	問題を報告するデバイスのアドレス。トラップの実際の送信元アドレスではない可能性があります。1 つのアドレスを管理アドレスとして使用して Prime Infrastructure にデバイスを追加したが、別のアドレスからトラップを送信した場合、この値はデバイスが追加されたときのアドレスになります。
cWNotificationSourceDisplayName	displayName	障害の原因（Failure Source）	なし	影響を受けたリソースの名前の表現。

内部 SNMP トラップの生成

MIB 変数名	関連付けられているアラームのフィールド	GUI 名	イベント	詳細
cWNotificationDescription	description (ciscoLwappIpsType, ciscoLwappIpsDescId, ciscoLwappIpsDescriptionParams)	メッセージ（Message）	Prime Infrastructure メッセージ	発生した問題または解決を示すメッセージ。これは通常、アラームの説明から取得されますが、WIPS アラームの場合は、他のフィールドから取得されます（左側の「関連付けられているアラームのフィールド」列を参照）。

内部 SNMP トラップの生成

MIB 変数名	関連付けられているアラームのフィールド	GUI 名	イベント	詳細
cWNotificationSeverity	severity	シビラティ（重大度）（Severity）	デフォルトのシビラティ（重大度）	

内部 SNMP トラップの生成

MIB 変数名	関連付けられているアラームのフィールド	GUI 名	イベント	詳細
				アラームのシビラティ（重大度）。これは、CISCO-TC MIB で定義されているアラームのシビラティ（重大度）を数値で表したものです。値は、[クリア済み（1）（cleared(1)）]、[不確定（2）（indeterminate(2)）]、[クリティカル（3）（critical(3)）]、[メジャー（4）（major(4),）]、[マイナー（5）（minor(5)）]、[警告（6）（warning(6)）]、[情報（7）（info(7)）] です。イベントタイプのシビラティ（重大度）は必要に応じて変更できるため、シビラティ（重大度）が変更されている場合は、「*Prime Infrastructure Supported Events*」のシビラティ（重大度）と一致しないことがあります。シビラティ（重大度）は、ノースバウンドトラップを介して通知されるアラームの変更を制御することによって変更できます（つまり、[クリティカル（CRITICAL）] アラームのみがノースバウンドトラップになるように指定し、不要なアラームのシビラティ（重大度）を [クリティカル

内部 SNMP トラップの生成

MIB 変数名	関連付けられているアラームのフィールド	GUI 名	イベント	詳細
				（CRITICAL）] から [メジャー（MAJOR）] に変更することができます）。
cWNotificationSpecialAttributes	すべてのアラーム フィールド	特定のアラーム フィールドに基づいて異なる	特定のアラーム フィールドに基づいて異なる	アラーム自体の内容（フィールドと値）が含まれます。
cWNotificationType	なし	なし	なし	トラップがアラームの作成/更新に基づいているか、またはイベントの作成に基づいているかを示します。一部のイベント（シビラティ（重大度）が [情報（Informational）] である場合）ではアラームが生成されないため、そのような情報イベントについては、ノースバウンドトラップを取得することができます。
cWNotificationVirtualDomains	なし	なし	なし	MIBから：「このオブジェクトは、cWNotificationTypeで表されるネットワーク条件の送信元が論理的に割り当てられる 1 つ以上の仮想ドメインの名前（カンマで区切られている）を表します」。たとえば、「root, California, San Jose」は、ネットワーク条件の送信元が論理的に複数の仮想ドメインに割り当てられていることを示します。

Prime Infrastructure SNMP トラップのリファレンス

次の表に、Prime Infrastructure で生成される SNMP トラップ通知の各クラスの詳細を示します。WCS ノースバウンド通知 MIB のマッピング済み OID は 1.3.6.1.4.1.9.9.712.1.1.2.1.12 です。この OID は、Prime Infrastructure のソフトウェア関連とハードウェア関連のトラップによって参照されます。ノースバウンド MIB のトラップ OID は、常に 1.3.6.1.4.1.9.9.712.0.1 です。詳細については、CISCO-WIRELESS-NOTIFICATION-MIB の一覧と関連項目の「ノースバウンド SNMP トラップにアラーム マッピング」を参照してください。

表 *4* : アプライアンス プロセス障害

目的	特定の Prime Infrastructure サーバー サービスが停止していること、およびヘルス モニターがそのサービスの再起動を試みていることをユーザーに通知します。
送信される条件	トラップは、ヘルス モニターがプロセスを再起動しようとするときに送信されます。
OID	1.3.6.1.4.1.9.9.712.1.1.2.1.12
例	Component: Health Monitor, Server: Primary, Type: Process, Service: NCS, When: Startup, State: Stand Alone, Result: Warning, MSG: FTP service is down and an attempt will be made to automatically restart the service
MSG コンテンツ	PI **servername**：serviceName のサービスが停止しています。このサービスを自動的に再起動することを試みます。
値のタイプ、範囲、および制約	MSG 属性中の **servername** パラメータは、Prime Infrastructure サーバーのホスト名の値を取得します。このパラメータは、NMS Server、FTP、TFTP、または MATLAB のいずれかの値を取ることができます。

表 *5* : *Failback*

目的	セカンダリ サーバーからプライマリ サーバーへのフェールバックが開始されたことをユーザーに通知します。
送信される条件	このトラップは、セカンダリ サーバーからプライマリ サーバーへのフェールバックが開始されると送信されます。フェールバック操作が失敗するか成功するかは関係ありません。
OID	1.3.6.1.4.1.9.9.712.1.1.2.1.12
例	Component: High Availability, Server: Secondary, Type: Process, Service: Database, When: Failback, State: Primary Failback, Result: Failure, MSG: Error in Failback: Failed to recover the primary database using Duplicate DB.

内部 SNMP トラップの生成

表 *6*: フェールオーバー

目的	セカンダリ サーバーが起動したときにユーザーに通知します。
送信される条件	プライマリ サーバーが停止し、フェールオーバーの一部として、セカンダリ サーバーがアクティブになると、トラップが生成されます。フェールオーバー操作が失敗するか成功するかは関係ありません。
OID	1.3.6.1.4.1.9.9.712.1.1.2.1.12
例	Component: High Availability, Server: Secondary, Type: Process, Service: Failover, When: Failover, State: Secondary Synching, Result: Success, MSG: Completed failover from primaryAddressInfo to secondaryAddressInfo.
MSG コンテンツ	MSG 属性中の primaryAddressInfo および secondaryAddressInfo は、サーバーの IP アドレスまたはホスト名を取得します。

表 *7*: *CPU* 使用率

目的	CPU 使用率が設定されたしきい値限度を超えたことをユーザーに通知します。
送信される条件	CPU 使用率が設定されたしきい値を超えた後、トラップは次のポーリング サイクルで生成されます。システム ポーラー ジョブは 5 分ごとに実行されます。トラップはしきい値限度が [Prime Infrastructure イベント設定（Prime Infrastructure Event Configuration）] Web ページで変更されたときにも生成されます。
OID	.1.3.6.1.4.1.9.9.712.0.1.
例	CPU Utilization is at 85% and has violated threshold limit of 80%.
値のタイプ、範囲、および制約	すべてのパーセンテージの範囲は 1 ～ 99 です。しきい値限度を指定する場合はパーセント文字（「%」）を入力しないでください。
ワイヤ形式	[OctetString] applicationSpecificAlarmID=Appliance_CPU, lastModifiedTimestamp=12 Jun 2014 11:12:32 UTC, alarmCreationTime=12 Jun 2014 11:12:32 UTC, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=8178170, severity=4, eventType=APPLIANCE_CPU_VIOLATED_THRESHOLD, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=CPU, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: primary, Type: Hardware, Message: CPU Utilization is at 3% and has violated threshold limit of 1%, isAcknowledged=false, displayName=NMS:192.168.115.141
制限事項と警告	次のポーリング サイクルの前に問題が解決される場合、トラップは生成されません。

内部 SNMP トラップの生成

表 *8*：ディスク使用率

目的	ディスク使用率が設定されたしきい値限度を超えたことをユーザーに通知します。
送信される条件	ディスク使用率が設定されたしきい値を超えた後、トラップは次のポーリング サイクルで生成されます。システム ポーラー ジョブは 5 分ごとに実行されます。トラップはしきい値限度が [Prime Infrastructure イベント設定（Prime Infrastructure Event Configuration）] Web ページで変更されたときにも生成されます。
OID	.1.3.6.1.4.1.9.9.712.0.1
例	PI opt disk volume utilization is at 85% and has violated threshold limit of 0%. PI opt disk volume is within the recommended disk usage range, less than 80% used. PI local disk volume utilization is at 85% and has violated threshold limit of 80%. PI local disk volume is within the recommended disk usage range, less than 80% used.
値のタイプ、範囲、および制約	すべてのパーセンテージの範囲は 1 ～ 99 です。しきい値限度を指定する場合はパーセント文字（「%」）を入力しないでください。
ワイヤ形式	[OctetString] applicationSpecificAlarmID=LocaldiskDiskSpace, reportingEntityAddress=10.77.240.246,lastModifiedTimestamp=Sun Mar 23 08:44:06 UTC 2014, alarmCreationTime=2014-03-14 13:29:31.069, eventCount=1, mayBeAutoCleared=false, instanceId=483484, severity=1, eventType=NCS_LOW_DISK_SPACE, authEntityId=93093, previousSeverity=MAJOR, category=System(17), transientNameValue={}, source=10.77.240.246, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=PI localdisk volume is within the recommended disk usage range, less than 70% used., isAcknowledged=false, authEntityClass=983576643, displayName=NCS 10.77.240.246
制限事項と警告	次のポーリング サイクルの前に問題が解決される場合、トラップは生成されません。

表 *9*：メモリ使用率

目的	メモリ使用率が設定されたしきい値限度を超えたことをユーザーに通知します。
送信される条件	メモリ使用率が設定されたしきい値を超えた後、トラップは次のポーリング サイクルで生成されます。システム ポーラー ジョブは 5 分ごとに実行されます。トラップはしきい値限度が [Prime Infrastructure イベント設定（Prime Infrastructure Event Configuration）] Web ページで変更されたときにも生成されます。
OID	.1.3.6.1.4.1.9.9.712.0.1.
例	Memory Utilization is at 85% and has violated threshold limit of 80%.
値のタイプ、範囲、および制約	すべてのパーセンテージの範囲は 1 ～ 99 です。しきい値限度を指定する場合はパーセント文字（「%」）を入力しないでください。

内部 SNMP トラップの生成

ワイヤ形式	[OctetString] applicationSpecificAlarmID=Appliance_MEMORY, lastModifiedTimestamp=12 Jun 2014 11:12:32 UTC, alarmCreationTime=12 Jun 2014 11:12:32 UTC, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=8178171, severity=4, eventType=APPLIANCE_MEM_VIOLATED_THRESHOLD, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=MEMORY, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: primary, Type: Hardware, Message: MEMORY Utilization is at 38% and has violated threshold limit of 1%, isAcknowledged=false, displayName=NMS:192.168.115.141
制限事項と警告	次のポーリング サイクルの前に問題が解決される場合、トラップは生成されません。

表 *10* : ディスク障害

目的	ドライブが欠落しているか不良であることをユーザーに通知します。
送信される条件	ディスク ドライブの問題が検出されると、トラップは次のポーリング サイクルで生成されます。システム ポーラー ジョブは 5 分ごとに実行されます。
OID	.1.3.6.1.4.1.9.9.712.0.1
例	Component: Appliance, Server: Standalone, Type: Hardware, Message: A problem was detected in the RAID device. A rebuild is in progress. Device at enclosure 252 slot ZERO is bad or missing. Drive0 is missing or bad.
制限事項と警告	次のポーリング サイクルの前に問題が解決される場合、トラップは生成されません。システムの再起動時にドライブが取り外されていると、トラップが生成されます。

表 *11* : ファン障害

目的	ファンに障害が発生したときにユーザーに通知します。
送信される条件	ファンに障害が発生すると、トラップは次のポーリング サイクルで生成されます。システム ポーラー ジョブは 5 分ごとに実行されます。
OID	.1.3.6.1.4.1.9.9.712.0.1
例	Fan is either bad or missing.
ワイヤ形式	[OctetString] applicationSpecificAlarmID=Appliance_Fan1, lastModifiedTimestamp=Sun Apr 13 15:24:11 IST 2014, alarmCreationTime=Sun Apr 13 15:24:11 IST 2014, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=2875873, severity=4, eventType=APPLIANCE_FAN_BAD_OR_MISSING, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=Fan1, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Fan is either bad or missing, isAcknowledged=false, displayName=NMS: 10.77.240.246
制限事項と警告	問題が次のポーリング サイクルの前に解決するか、またはシステムの再起動時にファンが取り外された場合、トラップは生成されません。

内部 SNMP トラップの生成

表 *12 : PSU* の障害

目的	電源装置が取り外されていることをユーザーに通知します。
送信される条件	電源が取り外されると、トラップは次のポーリング サイクルで生成されます。システム ポーラー ジョブは 5 分ごとに実行されます。
OID	.1.3.6.1.4.1.9.9.712.0.1
例	Component: Appliance, Server: Standalone, Type: Hardware, Message: Power supply: PSx is either bad or missing.
ワイヤ形式	[OctetString] applicationSpecificAlarmID=Appliance_PS1, lastModifiedTimestamp=19 Aug 2015 01:41:26 UTC, alarmCreationTime=19 Aug 2015 01:41:26 UTC, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=1424089, severity=4, eventType=APPLIANCE_POWER_SUPPLY_BAD_OR_MISSING, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=x.x.x.x, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: Standalone, Type: Hardware, Message: Power supply: PSx is either bad or missing, isAcknowledged=false, displayName=NMS:x.x.x.x
制限事項と警告	PSU が取り外されている場合、Prime Infrastructure で電源アラームが発生し、トラップが送信されます。システムのシャットダウン時に PSU が取り外されている場合、Prime Infrastructure は再起動までアクティブにならず、アラームは生成されません。

表 *13 :* サービス エンジン停止の識別

目的	ISE が到達不能な場合に、ユーザーに通知します。
送信される条件	ISE が停止または到達不能の場合、トラップがポーリングによって生成されます。 （注） これはシステムで生成されたトラップです。そのため、対応する OID はありません。
例	Identity services engine **ISEIPAddress** is unreachable.

表 *14 :* ライセンス違反

目的	Prime Infrastructure が実際に管理しているデバイスの数が管理のライセンス付与数を超えるとユーザーに通知します。
送信される条件	Prime Infrastructure インベントリに余分なデバイスを追加したジョブの完了後の翌日午前2時10分 （注） これはシステムで生成されたトラップです。そのため、対応する OID はありません。
例	Number of managed devices **N** is greater than licensed devices **N**. Please purchase and install a license that will cover the number of managed devices, or remove unused devices from the system.

表 *15 : Prime Infrastructure* にバックアップ用の十分なディスク容量がありません

目的	Prime Infrastructure がバックアップを実行するために、指定のディレクトリに十分な容量を確保できない場合にユーザーに通知します。
送信される条件	Prime Infrastructure がサーバー バックアップ ジョブを実行し、指定されたバックアップ リポジトリ（つまり「defaultrepo」）が 100 % フルである場合は毎回。トラップはジョブが完了した後に生成されます。 （注） これはシステムで生成されたトラップです。そのため、対応する OID はありません。
例	Prime Infrastructure with address **localIPAddress** does not have sufficient disk space in directory **directoryName** for backup. Space needed: **Needed** GB, space available **Free** GB.

表 *16 : Prime Infrastructure* の電子メールの失敗

目的	電子メール通知の送信試行に失敗したことをユーザーに通知します。
送信される条件	このトラップは、Prime Infrastructure が無効なユーザーに電子メール通知を送信しようとした場合、または、Prime Infrastructure で電子メール サーバーを指定せずに電子メール通知が有効になっている場合に、ポーリングによって生成されます。 （注） これはシステムで生成されたトラップです。そのため、対応する OID はありません。
例	Prime Infrastructure with address **localIPAddress** failed to send email. This may be due to possible SMTP misconfiguration or network issues.

表 *17 :* ノースバウンド *OSS* サーバーが到達不能です

目的	ノースバウンド通知サーバーが到達不能であることをユーザーに通知します。
送信される条件	このトラップは、宛先のノースバウンド通知サーバーが到達不能の場合にポーリングによって生成されます。
OID	.1.3.6.1.4.1.9.9.712.0.1
例	Northbound notification server **OSSIPAddress** is unreachable. NCS alarms will not be processed for this server until it is reachable.

Prime Infrastructure トラップの設定

以下のセクションでは、Prime Infrastructure トラップ通知を設定および使用する方法について説明します。

関連トピック

通知の設定 （19 ページ）
トラップの送信に使用するポート （20 ページ）

通知の設定

Prime Infrastructure にノースバウンド SNMP トラップ通知を送信させるには、[Prime Infrastructure イベント通知（Prime Infrastructure Event Notification）] ページと [通知宛先（Notification Destiantion）]ページの両方で正しい設定を行う必要があります。設定が完了すると、トラップは、次の SNMP イベントのしきい値とシビラティ（重大度）に関連付けられた値に基づいて生成されます。

- アプライアンス プロセス障害
- HA 操作
- CPU、ディスク、およびメモリの使用率
- ディスク、ファン、および PSU の障害
- バックアップ障害、証明書有効期日、ライセンス違反

各イベントに関連付けられるしきい値とシビラティ（重大度）を編集し、関連イベントのトラップ生成を有効または無効に設定できます。

ステップ 1 ルート ドメイン権限を持つユーザー ID を使用して Prime Infrastructure にログインします。

ステップ 2 [管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [アラームおよびイベント（Alarms and Events）] > [システム イベント設定（System Event configuration）] の順に選択します。

ステップ 3 設定する各 SNMP イベントに対して、次の手順を実行します。

a) そのイベントの行をクリックします。

b) 必要に応じて、[イベントのシビラティ（重大度）（Event Severity）] レベルを [重大（Critical）]、[メジャー（Major）]、または [マイナー（Minor）] に設定します。

c) CPU、ディスク、メモリ使用率、ライクサイクル、アシュアランス、およびコレクタのトラップについては、[しきい値（Threshold）] にパーセンテージ（1 ～ 99）を入力します。これらのイベントは、使用率がしきい値限度を超えたときに、関連の SNMP トラップを送信します。しきい値設定が NA と表示されるイベントのしきい値は設定できません。これらのイベントは、関連付けられた障害が検出されるたびにトラップを送信します。

d) バックアップしきい値、証明書の失効（重大）、ライフサイクル ライセンス、アシュアランス ライセンス、およびコレクタ ライセンスのトラップについては、[しきい値（Threshold）] に日数（x-y の形式。x は最小日数値、y は最大日数値）を入力します。

e) [イベント ステータス（Event Status）] を [有効（Enabled）] または [無効（Disabled）] に設定します。[有効（Enabled）] に設定すると、このイベントに対応するトラップが生成されます。

f) CPU、ディスク、メモリの使用率について、[アラームの反復の作成とクリア（Create and Clear Alarm Iteration）] の値を入力します。デフォルト値は 2 です。反復値を設定した後の最初のポーリングの所要時間は、入力された反復値（分単位）の 2 倍です。その後のポーリングはいずれも 20 分しかかかりません。

デフォルトのポーリング時間は 20 分です。

ステップ 4 完了したら、[保存（Save）] をクリックして変更を保存します。

関連トピック

アラーム通知先の設定

トラップの送信に使用するポート

Prime Infrastructure はトラップを通知宛先のポート 162 に送信します。このポートは現時点ではカスタマイズできません。ノースバウンド管理システムは、[通知宛先（Notification destination）] Web ページで自分自身を登録する必要があります（アラーム通知先の設定 を参照）。

電子メール サーバー設定の構成

Prime Infrastructure で電子メール通知の送信を可能にするには、システム管理者はプライマリ SMTP 電子メール サーバーを（また、できればセカンダリ電子メール サーバーも）設定する必要があります。

ステップ 1 管理者権限のユーザー ID を使用して Prime Infrastructure にログインします。

ステップ 2 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [メールおよび通知（Mail and Notification）] > [メール サーバー設定（Mail Server Configuration）]** の順に選択します。

ステップ 3 [プライマリ SMTPサーバー（Primary SMTP Server）] で、Prime Infrastructure で使用する電子メール サーバーに合わせて、[ホスト名/IP（Hostname/IP）]、[ユーザー名（User Name）]、[パスワード（Password）]、[ポート（Port）]、および [パスワードの確認（Confirm Password）] フィールドに入力します。物理サーバーの IP アドレスを入力します。仮想 IP アドレスを [Hostname/IP] フィールドに入力することはできません。また、IP アドレスをロード バランサの後に配置することはできません。

ステップ 4 [接続セキュリティ（Connection Security）] ドロップダウンリストからいずれかのオプションを選択します。使用可能なオプションは、[プレーンテキスト（Plain Text）]、[STARTTLS]、および [SSL/TLS] です。

（注） 対応するポート番号を [ポート（Port）] テキストボックスに入力する必要があります。

ステップ 5 （オプション）[セカンダリ SMTP サーバー（Secondary SMTP Server）] で同じ各フィールドに入力します。

ステップ 6 [送信者および受信者（Sender and Receivers）] で、Prime Infrastructure サーバーの正当なメール アドレスを入力します。

ステップ 7 （任意）[件名（Subject）] テキスト ボックスに件名を入力します。

ステップ 8 完了したら、[保存（Save）] をクリックします。

関連トピック

SNMP トラップのイベントとアラームの表示 （21 ページ）
SNMP トラップのイベントとアラームのフィルタ処理 （21 ページ）

SNMP トラップのアラームの消去 （23 ページ）
Prime Infrastructure SNMP トラップのトラブルシューティング方法 （23 ページ）
通知の設定 （19 ページ）
トラップの送信に使用するポート （20 ページ）

SNMP トラップのイベントとアラームの表示

Prime Infrastructure の内部 SNMP トラップのすべてのイベントとアラームは[システム（System）] カテゴリに分類されます。これらは Prime Infrastructure の [アラームおよびイベント（Alarms and Events）] ダッシュボードで表示できます。

ステップ 1 Prime Infrastructure にログインします。

ステップ 2 **[モニター（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** を選択します。

SNMP トラップのイベントとアラームのフィルタ処理

Prime Infrastructure のフィルタ機能を使用して、アラームの表示をシステム カテゴリだけに絞り込んだり、条件と演算子の組み合わせを使用して、明確に限定したアラームのリストに焦点を合わせたりすることができます。以下のセクションで、この方法について説明します。

関連トピック

クイック フィルタを使用した SNMP トラップ用のフィルタ処理 （21 ページ）
高度なフィルタを使用する SNMP トラップのフィルタ処理 （22 ページ）

クイック フィルタを使用した SNMP トラップ用のフィルタ処理

Prime Infrastructure のクイック フィルタを使用すると、特定のテーブル列にフィルタを適用することで、テーブル内のデータにすばやく焦点を合わせることができます。

ステップ 1 Prime Infrastructure にログインします。

ステップ 2 **[モニター（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** を選択します。

ステップ 3 [表示（Show）] ドロップダウン リストで、[クイック フィルタ（Quick Filter）] を選択します。Prime Infrastructure はテーブル ヘッダー フィールドのリストを表示し、[シビラティ（重大度）（Severity）]、[メッセージ（Message）]、および [カテゴリ（Category）] などのクイック フィルタを実行できます。

ステップ 4 [カテゴリ（Category）] フィールドに、「System」と入力します。Prime Infrastructure にはシステム アラームだけが表示されます。

ステップ 5 クイックフィルタをクリアするには、[表示（Show）]ボックスの横に表示される漏斗アイコンをクリックします。

高度なフィルタを使用する SNMP トラップのフィルタ処理

Prime Infrastructure の高度なフィルタを使用すると、複数のタイプのデータと論理演算子を組み合わせたフィルタ（「次を含まない（Does not contain）」、「等しくない（Does not equal）」、「次で終わる（Ends with）」など）を適用して、テーブル内のデータを絞り込むことができます。たとえば、カテゴリに基づいてアラーム テーブルをフィルタにかけ、さらにシビラティ（重大度）でフィルタリングすることで、データを減らすことができます（次の手順を参照）。高度なフィルタを保存して、後で再利用することもできます。

ステップ 1 Prime Infrastructure にログインします。

ステップ 2 [モニター（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択します。

ステップ 3 [表示（Show）] ドロップダウン リストで、[高度なフィルタ（Advanced Filter）] を選択します。Prime Infrastructure はフィルタ内の最初のルールの条件を示すテーブル ヘッダーを表示します。

ステップ 4 次のように、最初のルールを完成させます。

a) 最初のフィールドで、ドロップダウン リストから [Category] を選択します。
b) 2 番目のフィールドで、ドロップダウン リストから [Contains] を選択します。
c) ルールの 3 番目のフィールドに、[System] を入力します。
d) [実行（Go）] をクリックします。Prime Infrastructure にはシステム アラームだけが表示されます。

ステップ 5 プラス記号のアイコンをクリックして別のルールを追加し、次のように、2番目のルールを完成させます。

a) 最初のフィールドで、ドロップダウンリストから[シビラティ（重大度）（Severity）]を選択します。
b) 2 番目のフィールドで、ドロップダウン リストから [equals (=)] を選択します。
c) ルールの 3 番目のフィールドで、ドロップダウン リストから [メジャー（Major）] を選択します。
d) [実行（Go）]をクリックします。Prime Infrastructure はシビラティ（重大度）がメジャーのシステム アラームのみを表示します。

必要に応じてこの手順を繰り返します。

ステップ 6 高度なフィルタを保存するには、[Save] アイコンをクリックし、フィルタの名前を入力します。

ステップ 7 高度なフィルタをクリアするには、[フィルタのクリア（Clear Filter）] をクリックします。

詳細については、SNMP トラップのアラームの消去 （23 ページ）を参照してください。

関連トピック

Prime Infrastructure SNMP トラップのトラブルシューティング方法 （23 ページ）
通知の設定 （19 ページ）
トラップの送信に使用するポート （20 ページ）
SNMP トラップのイベントとアラームの表示 （21 ページ）

SNMP トラップのイベントとアラームのフィルタ処理 （21 ページ）

SNMP トラップのアラームの消去

アラーム リストに含まれるアラームは、ステータスを [認知済み（Acknowledged）] から [クリア済み（Cleared）] に変更することで削除できます。これらのアラームに対して電子メールは生成されません。

ステップ 1 Prime Infrastructure にログインします。

ステップ 2 **[モニター（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** を選択します。

ステップ 3 アラームを選択し、**[ステータスの変更（Change Status）] > [確認（Acknowledge）]** または **[ステータスの変更（Change Status）] > [クリア（Clear）]** を選択します。

Prime Infrastructure SNMP トラップのトラブルシューティング方法

Prime Infrastructure の内部トラップおよび関連する通知で問題が生じた場合は、次の点を確認してください。

ステップ 1 Prime Infrastructure サーバーから通知宛先に ping を実行し、Prime Infrastructure と管理アプリケーションの間の接続を確認します。

ステップ 2 ファイアウォールの ACL 設定がポート 162 をブロックしていないかを確認し、必要に応じてそのポートの通信を開きます。

ステップ 3 管理者権限を持つユーザー ID を使用して Prime Infrastructure にログインします。**[管理（Administration）] > [設定（Settings）] > [ロギング（Logging）]** を選択し、ログ ファイルをダウンロードします。次に、これらのログ ファイルに記録されたアクティビティを、管理アプリケーションで参照しているアクティビティと比較します。

- ncs_nb.log：これは、Prime Infrastructure が送信したすべてのノースバウンド SNMP トラップ メッセージのログです。受信していないメッセージの有無をチェックします。
- ncs-#-#.log：これは、最近のその他の Prime Infrastructure アクティビティのログです。受信していないハードウェア トラップ メッセージの有無をチェックします。
- hm-#-#.log：これはヘルス モニター アクティビティのすべてのログです。未受信のハイ アベイラビリティ状態の変更およびアプリケーション プロセス障害に関する、最近のメッセージをチェックします。

内部 SNMP トラップの生成

これらのログに表示されるメッセージは、管理アプリケーションに表示されるアクティビティと一致する必要があります。大きな違いがある場合は、Cisco Technical Assistance Center（TAC）でサポートケースを開き、疑わしいログ ファイルをケースに添付してください。

関連トピック

Prime Infrastructure SNMP トラップ タイプ （2 ページ）
Prime Infrastructure SNMP トラップのリファレンス （13 ページ）
Prime Infrastructure トラップの設定 （18 ページ）

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。