



CHAPTER 7

アラームのモニタリング

アラームは、1 つ以上の関連イベントに対する Prime AM の応答です。イベントの重大度（非常に重大、重大、重大でない、または警告）が十分に高いと考えられる場合、Prime AM はその状態が存在しなくなるまでアラームを発生させます。

イベントとは

イベントとは、ネットワーク内やその周辺である状態が発生すること、およびこれを検出することです。イベントは、特定の時点で発生する別個の問題です。イベントの例には次のものがあります。

- ポート ステータスの変更
- デバイス リセット
- デバイスに管理ステーションが到達できなくなります。

また、イベントは次のいずれかの症状です。

- ネットワーク内のエラー、障害、または例外状況である障害の症状。たとえば、デバイスが到達不能になると、到達不能イベントがトリガーされます。
- 障害除去の症状。たとえば、デバイスの状態が到達不能から到達可能に変更されると、到達可能イベントがトリガーされます。

1 つ以上のイベントによって、異常ステートまたはアラームが生成されることがあります。アラームは削除できますが、イベントは残ります。[Event Browser] を使用して、イベントのリストを表示できます。

[Operate] > [Alarms & Events] を選択し、[Events] をクリックして [Events Browser] ページにアクセスします。

イベントの作成

Prime AM は、イベント カタログを維持し、イベントをいつどのように作成するかと、アラームをイベントと関連付けるかどうかを決定します。複数のイベントを同じアラームに関連付けることができます。

Prime AM は、次の方法でイベントを検出します。

- 通知イベント（たとえば、Syslog やトラップ）を受信して、分析します。
- デバイスを自動的にポーリングして変更を検出します（たとえば、到達不能なデバイス）。
- Prime AM サーバで重大な変更が行われたとき（たとえば、サーバのリポート）にイベントを受信します。

■ アラームとは

- アラームのステータスが変更されると（たとえば、ユーザがアラームを認知するかクリアすると）、イベントを受信します。

着信イベント通知（トラップおよび Syslog）は、イベント データと事前定義パターンを照合して識別されます。トラップまたは Syslog は、一致するパターンがあり、正しく識別できる場合は Prime AM でサポートされると見なされます。イベント データが事前定義済みのパターンと一致しない場合は、イベントはサポートされないと見なされ、ドロップされます。

障害は、Prime AM でポーリング、トラップ、または Syslog メッセージを使用して検出されます。Prime AM は、すべての障害の状況を維持し、重複するイベントまたはアラームが Prime AM データベースに維持されないようにします。

次の表に、Prime AM がイベントを作成する時間の例を示します。

時間	イベント	Prime AM の動作
10:00AM PDT 2011/12/01	デバイス A が到達不能になった。	デバイス A で新しい到達不能イベントを作成します。
10:30AM PDT 2011/12/01	デバイス A が引き続き到達不能になる。	イベント ステータスに変更はありません。
10:45AM PDT 2011/12/01	デバイス A が到達可能になった。	デバイス A で新しい到達可能イベントを作成します。
11:00AM PDT 2011/12/01	デバイス A は到達可能なまま。	イベント ステータスに変更はありません。
12:00AM PDT 2011/12/01	デバイス A が到達不能になった。	デバイス A で新しい到達不能イベントを作成します。

アラームとは

アラームは、1 つ以上の関連イベントへの Prime AM の応答です。イベントの重大度（非常に重大、重大、重大でない、または警告）が十分に高いと考えられる場合、Prime AM はその状態が存在しなくなるまでアラームを発生させます。

1 つまたは複数のイベントで、発生するアラームが 1 つの場合もあります。アラームは、次の順序で作成されます。

- ネットワークで障害が発生すると、通知がトリガーされます。
- 通知に基づいてイベントが作成されます。
- このイベントに対応するアクティブなアラームがないかどうかを確認した後で、アラームが作成されます。

アラームは、次の 2 つのタイプのイベントに関連付けられます。

- アクティブ イベント：クリアされていないイベント。アラームは、ネットワークで障害が解決されるまでこの状態のままです。
- 履歴イベント：クリアされたイベント。ネットワークで障害が解決されたときに、イベントのステータスが履歴イベントに変わります。

アラームのクリア後は、アラームのライフ サイクルの終了を示します。クリアされたアラームは、プリセット期間内に同じ障害が再発生した場合に復活されることがあります。プリセット期間は、Prime AM で 5 分に設定されます。

イベントとアラームの関連付け

Prime AM は、イベントとアラームのカタログを維持します。カタログには、Prime AM によって管理されるイベントのリスト、およびイベントとアラーム間の関係が含まれています。さまざまなタイプのイベントを同じアラームタイプに結び付けることができます。

通知の受信時には、次のことが行われます。

1. Prime AM は、着信通知をイベントとアラーム カタログと突き合わせて比較します。
2. Prime AM は、イベントを出す必要があるかどうかを決定します。
3. イベントを出す場合、Prime AM は、イベントが新しいアラームをトリガーするか、既存のアラームに関連付けるかを決定します。

トリガーされる新しいイベントのタイプが同じで、同じソースで発生する場合、新しいイベントは既存のアラームに関連付けられます。

たとえば、アクティブなインターフェイス エラー アラームです。同じインターフェイスで発生するインターフェイス エラー イベントは、すべて同じアラームに関連付けられます。

アラームのステータス

次に、アラームでサポートされるステータスを示します。

- [New] : イベントが新しいアラームをトリガーしたか、イベントが既存のアラームに関連付けられる場合。
- [Acknowledged] : ユーザがアラームを認知すると、ステータスは [New] から [Acknowledged] に変更されます。
- [Cleared] : アラームのステータスには次のものがあります。
 - [Auto-clear from the device] : 障害がデバイスで解決され、同じデバイスでイベントがトリガーされます。たとえば、デバイス到達可能イベントは、デバイス到達不能イベントをクリアします。次に、これによって、デバイス到達不能アラームがクリアされます。
 - [Manual-clear from Prime AM users] : ネットワークで障害を解決せずに、アクティブ アラームを手動でクリアできます。クリア イベントがトリガーされ、このイベントによってアラームがクリアされます。

障害が引き続きネットワークに存在する場合は、イベント通知（トラップまたは Syslog）に基づいて、その後に新しいイベントとアラームが作成されます。

イベントとアラームの重大度

各イベントには重大度が割り当てられています。イベントは、次の重大度カテゴリに大きく分類され、Prime AM ではそれぞれに色が関連付けられています。

- フラグ付き : 障害を示します。クリティカル（赤）、メジャー（オレンジ）、マイナー（黄色）、または警告（空色）。
- 情報 : 情報（青）。一部の情報イベントは、フラグ付きイベントをクリアします。

たとえば、「リンク停止」イベントには、クリティカルの重大度が割り当てられる可能性があるのに対して、対応する「リンク起動」イベントは情報の重大度になります。

イベントの順序では、重大度が最も高いイベントが、アラームの重大度を決定します。

アラームの検出

表 7-1 に、アラームを検出できる場所を示します。

表 7-1 アラームを検出する場所

GUI の場所	説明
[Operate] > [Alarms & Events]	重大度、ステータス、ソース、タイムスタンプなどの詳細とともにすべてのアラームを表示する新しいページが表示されます。このページでは、アラームのステータスを変更し、電子メール通知の割り当て、注釈追加、削除、および指定を行えます。
カーソルを [Alarm Summary] に置く	Prime AM により現在検出されている非常に重大なアラーム、重大なアラーム、および重大でないアラームを示す表が表示されます。
Alarm Browser	[Operate] > [Alarms & Events] を選択した場合と同じ情報を示すウィンドウが開きます（ただし、新しいページは表示されません）。
デバイスの 360° のビュー	[Alarms] タブをクリックしてデバイスのアラームとそのステータスおよびカテゴリを表示するか、[Alarm Browser] アイコンをクリックして Alarm Browser を起動します。
[Operate] > [Monitoring Dashboard] > [Incidents]	アラームの要約情報、最もアラームが多い上位サイト、問題がある上位アラーム タイプ、上位イベント、および上位インターフェイスを含むダッシュレットが表示されます。

しきい値の定義

モニタリング テンプレートを使用してしきい値を定義します。指定のしきい値に達すると、Prime AM からアラームが出力されます。

しきい値を定義するには、次の手順を実行します。

-
- ステップ 1 [Design] > [Monitoring Templates] を選択します。
 - ステップ 2 [Features] で [Threshold] を選択します。
 - ステップ 3 基本のテンプレート フィールドを入力します。
 - ステップ 4 [Feature Category] で、次のメトリックのいずれかを選択します。
 - [Device Health] : CPU 使用率、メモリ プール使用率、および環境温度のしきい値を変更できます。
 - [Interface Health] : 破棄される発信パケットの数に対するしきい値を変更できます。
 - ステップ 5 [Metric Parameters] で、変更するしきい値設定を選択し、[Edit Threshold Setting] をクリックします。
 - ステップ 6 新しい値を入力し、しきい値のアラーム重大度を選択します。
 - ステップ 7 [Done] をクリックします。
 - ステップ 8 [Save as New Template] をクリックします。
 - ステップ 9 [My Templates] フォルダで、作成したテンプレートに移動して選択します。
 - ステップ 10 [Go to Deployment] をクリックします。
 - ステップ 11 作成したテンプレートを選択して、[Deploy] をクリックします。
-

アラーム ステータスの変更

単一のアラームとその関連イベントを表示し、アラーム ステータスを変更するには、次の手順を実行します。

- ステップ 1** [Operate] > [Alarms & Events] を選択します。
- ステップ 2** 詳細を表示するアラームの横にある展開アイコンをクリックします。
- ステップ 3** [Change Status] > [Acknowledge] または [Clear] を選択します。

アラームのリストから、[Acknowledged] アラームと [Cleared] アラームが削除されます。アラームを認知済みまたは削除済みとしてマークした場合は、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。

デフォルトでは、認知済みアラームと削除済みアラームは検索対象になりません。このデフォルト値を変更するには、[Administration] > [System] > [Alarms and Events] を選択し、[Hide Acknowledged Alarms or Hide Cleared Alarms] 設定を無効にします。

[Cleared] アラームは、Prime AM データベースに維持されますが、削除の状態になります。この原因となる状況がなくなった場合は、アラームを削除します。

アラームを認知する場合

状況によっては、特定のアラームを [Alarms List] から削除した方がよい場合があります。たとえば、特定のデバイスから干渉アラームを継続的に受信している場合は、[Alarm Summary] ページまたは任意のアラーム リストで、そのデバイスがアクティブなアラームとしてカウントされないようにすることができます。そのためには、[Alarms] リストでデバイスのアラームを探し、該当するチェックボックスをオンにして、[Select a command] ドロップダウン リストから [Acknowledge] を選択します。

これで、そのデバイスが同じインターフェイスで新しい違反を生成しても、Prime AM によって新しいアラームが生成されず、[Alarm Summary] ページにも新しいアラームが表示されません。ただし、別のインターフェイスで干渉違反が発生すると、新しいアラームが生成されます。

デフォルトでは、認知済みアラームは、[Alarm Summary] ページまたは任意のアラーム リスト ページに表示されません。また、アラームを認知済みとしてマークした場合、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。デフォルトでは、認知済みアラームは検索対象となりません。このデフォルト値を変更するには、[Administration] > [System] > [Alarms and Events] ページに移動し、[Hide Acknowledged Alarms] 設定を無効にします。

アラームを認知する場合は、この機能が無効でない限り、問題の再発により別のアラームが生成されないことを通知する次の警告が表示されます。



(注)

アラームを認知する場合は、この機能が無効でない限り、問題の再発により別のアラームが生成されないことを通知する警告が表示されます。[Administration] > [User Preferences] ページを使用して、この警告メッセージを無効にします。

また、以前の認知済みアラームをすべて検索して、過去 7 日間に認知されたアラームを表示することもできます。Prime AM は、経過日数が 7 日間を超えた解除済みアラートを自動的に削除するため、結果に表示できるのは過去 7 日間のアクティビティだけです。既存のアラームが削除されるまで、Prime AM がすでにアラームを生成しているすべての管理対象エンティティに新しいアラームを生成できません。

アラーム表示オプションの設定

いつアラームを削除するかや、どのアラーム重大度を表示するかなどのアラーム オプションおよびイベント オプションと、アラーム電子メールオプションを変更するには、次の手順を実行します。

-
- ステップ 1 [Administration] > [System] > [Alarms and Events] を選択します。
 - ステップ 2 アラームに対して必要な設定を変更します。
 - ステップ 3 [Save] をクリックします。
-

アラーム重大度の設定

新しく生成されたアラームに対して重大度を設定するには、次の手順を実行します。

-
- ステップ 1 [Administration] > [System] を選択します。
 - ステップ 2 左側のサイドバー メニューから、[Severity Configuration] を選択します。
 - ステップ 3 変更する重大度のアラーム条件のチェックボックスをオンにします。
 - ステップ 4 [Configure Security Level] ドロップダウン リストから、次のいずれかの重大度を選択します。
 - Critical
 - Major
 - Minor
 - Warning
 - Informational
 - Reset to Default
 - ステップ 5 [Go] をクリックします。
 - ステップ 6 [OK] をクリックして、変更を確認します。
-