アラームについて

（注） 使用可能なアラームのリストを表示するには、アラームの説明 を参照してください。

ここでは、次の内容について説明します。

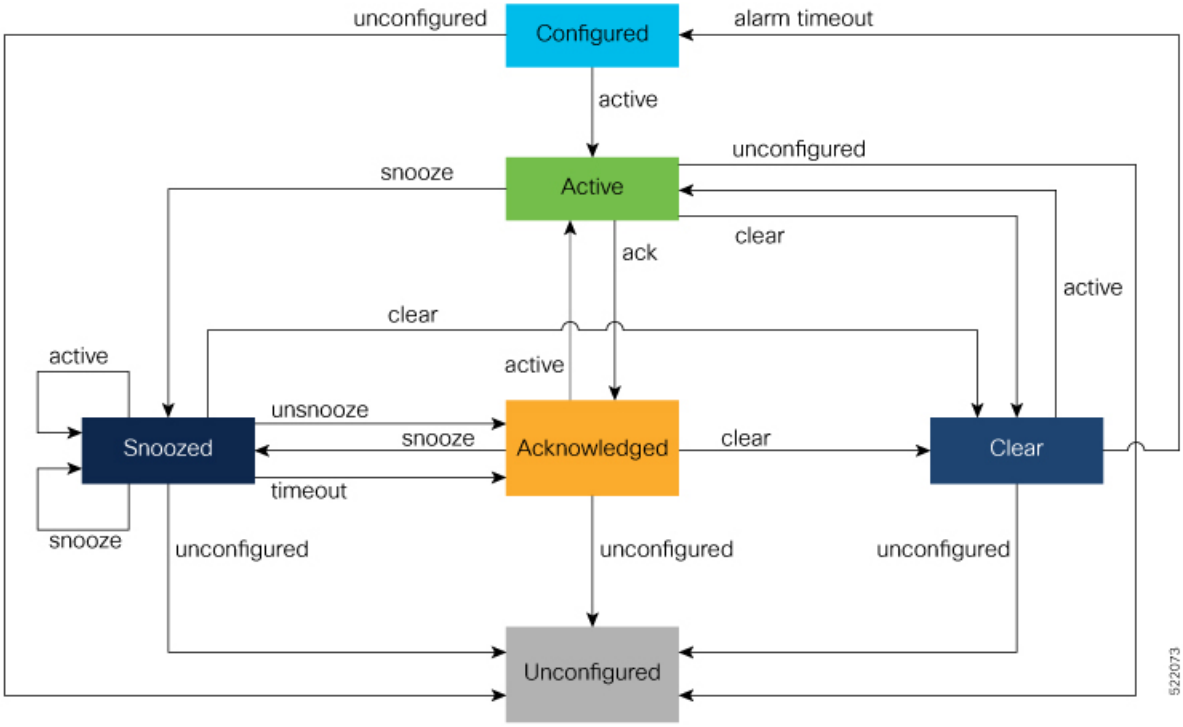
アラームライフサイクル

Crosswork Cloud Network Insights は、完全に設定されたアラームポリシーの各ルールのアラームインスタンスを作成します。完全に設定されたアラームポリシーには1つ以上のルールがあり、アラームポリシータイプに応じて、1 つ以上のプレフィックス、ASN、またはそれに関連付けられたピアがあります。

各アラームインスタンスにはライフサイクルがあり、作成後にさまざまな状態の間で遷移します。次の図は、各状態から発生する遷移を示しています。詳細については、アラームの状態 （2 ページ）を参照してください。

（注） 各アラームインスタンスは、[設定済み（Configured）] 状態でライフサイクルを開始します。

図 *1*: アラームライフサイクル



アラームの状態

アラームインスタンスは、イベントまたはユーザアクションに応じて状態間を遷移します。

次の表で、考えられるアラームの状態について説明します。

表 *1*: *Crosswork Cloud Network Insights* のアラームの状態の説明

アラーム ステータス	説明
設定済み（Configured）	アラームの初期状態。
アクティブ（Active）	アクティブイベントでアラームがトリガーされたときの状態。

アラーム ステータス	説明
承認済み（Acknowledged）	この状態では、アラームが認識され、承認されたことをユーザに示します。[アクティブ（Active）] または [スヌーズ（Snoozed）] 状態のアラームは、[承認済み（Acknowledged）] としてマークできます。 （注） • [承認済み（Acknowledged）] 状態のアラームは、アクティブなアラームのリストに表示されません。 • 別のアクティブなアラートがある場合、[承認済み（Acknowledged）] 状態のアラームは [アクティブ（Active）] 状態に戻ります。
クリア（Clear）	アラームはアクティブではありません。[クリア（Clear）] 状態はエフェメラル状態です。アラームインスタンスは、30 秒の保留時間後に [設定済み（Configured）] 状態に遷移します。
スヌーズ（Snoozed）	[アクティブ（Active）] または [承認済み（Acknowledged）] 状態のアラームは、指定された期間、ユーザが [スヌーズ（Snoozed）] 状態としてマークできます。この期間中、アラームはアクティブアラームリストに表示されます。ただし、アラーム条件がクリアされると、通知エンドポイント（設定されている場合）に通知が送信されます。
未設定（Unconfigured）	アラームは [未設定（Unconfigured）] 状態に遷移し、ユーザがアラームポリシーまたはアラームインスタンスに対応するルールを削除すると、最終的に削除されます。[未設定（Unconfigured）] 状態はエフェメラル状態であり、アラームインスタンスは 30 秒の保留時間後に削除されます。

（注）
- アラームインスタンスは、アラーム検出レイヤから受信したイベントに応じてのみ、[アクティブ（Active）] または [クリア（Clear）] 状態に遷移できます。

アラーム通知

ポリシールールに違反すると、アラーム通知が 1 つ以上のエンドポイントに送信されるように設定できます（通知エンドポイントの設定を参照）。通知には、アラーム状態とアラームイベントデータに関する情報が含まれます。

次のいずれかのアラーム状態が変化すると、通知が送信されます。

- アクティブからクリアへ
- 設定済みからアクティブへ

- 承認済みからクリアへ
- スヌーズからクリアへ

アラームが再びアクティブになり、すでに次のいずれかの状態になっている場合、通知は生成されません。

- Active
- スヌーズ（Snoozed）
- 承認済み（Acknowledged）

関連リンク

- 通知エンドポイントについて

アラームタイプ

アラームは、次の 3 つのタイプに分類されます。

タイプ	説明
ASN	自律システム番号（ASN）タイプのアラームは、設定されたBGP自律システム（AS）の状態をモニタします。これらのアラームは通常、ASNからの予期しないプレフィックスを検出し、予期される条件に違反した場合に警告するために使用されます。たとえば、アラームがアクティブになるのは、以前に確認されておらず、設定済みの ASN から発信されてはならない新しいプレフィックスを Crosswork Cloud Network Insights が検出した場合です。
ピア（PEER）	ピアタイプのアラームは、設定されたピアとそのルーティング情報ベース（RIB）の状態をモニタします。これらのアラームは、ピアモニタリングを設定した場合に使用されます。たとえば、アラームがアクティブになるのは、設定されたパラメータの範囲外の RIB で多数のプレフィックスを Crosswork Cloud Network Insights が検出した場合です。
プレフィックス（PREFIX）	プレフィックスタイプのアラームは、プレフィックスの送信元 ASN や AS パス属性の長さなど、設定されたプレフィックスの状態とそのBGP属性の数をモニタします。これは最も一般的なアラームタイプであり、監視されているプレフィックスの不明なイベントを検出するように設計されています。プレフィックスタイプのアラームのセットは、設定されたプレフィックスのROAステータス（VALID、INVALID、またはABOUT-TO-EXPIRE）もモニタします。

アラームのしきい値

アラームのしきい値は、アラームの感度を制御するために使用されます。一部のアラームが少数の観測された変更によってトリガーされることが多く、「誤アラーム」と見なされる場合は、アラームのしきい値を構成することを検討してください。

モニタ対象のAS、ピア、またはプレフィックスに関連する一連の条件に対する違反をCrosswork Cloud Network Insights が検出すると、アラームがトリガーされます（アクティブ）。すべての条件に違反しなくなると、アラームはクリアされます。データは多くの BGP ピアから収集されるため、Crosswork Cloud Network Insights はプレフィックスまたはAS の状態の複数のビューにアクセスできます。これらのビューは常に同じであるとは限りません。また、少数のピア（ルータのフラップによって発生するピアなど）で頻繁に状態が変化すると、大量のアラームノイズが発生する可能性があります。しきい値は、ノイズ減衰メカニズムとして機能できます。

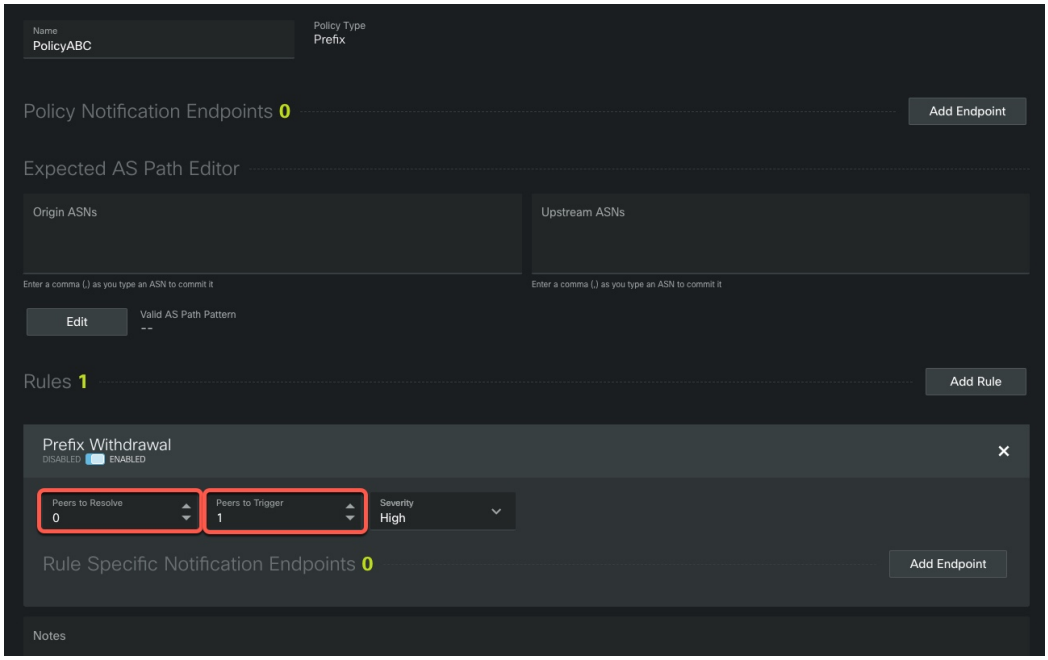
アラームノイズを減衰させるために、特定のアラームルールに対して次のピアカウントしきい値を設定できます。

[トリガーするピア（Peers to Trigger）]：アラームがアクティブになる条件違反を報告するために必要な違反ピアの最小数。例：[トリガーするピア（Peers to Trigger）] しきい値が [プレフィックスの取り消し（Prefix Withdrawal）] アラームに対して 1 に設定されています。外部ルーティング分析がアクティブなプレフィックスの取り消しアラームを発行する前に、プレフィックスが取り消されたことを報告するピアの数が 1 を超える必要があります。

[解決するピア（Peers to Resolve）]：アラームがアクティブ化された後も、アクティブのままになります。アラームは、違反ピア数が [解決するピア（Peers to Resolve）] のしきい値以下になるまで、すべての新しい条件違反で再度トリガーされます（たとえば、これは違反アドバタイズメントの取り消しまたは [解決するピア（Peers to Resolve）] のしきい値の増加によって発生する可能性があります）。その後でアラームは [クリア（Clear）] 状態になります。

（注） [解決するピア（Peers to Resolve）] のしきい値は、[トリガーするピア（Peers to Trigger）] のしきい値よりも小さくする必要があります。

図 *2 :* 例：*[*想定される*AS*パス（*Expected AS Path*）*]*アラームルールのしきい値オプション



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。