



アラームのモニタ

問題を迅速に解決するために、[アラーム (Alarms)] ページ ([外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [アラーム (Alarms)]) でポリシー違反を簡単に表示できます。[アラーム (Alarms)] ページでは、アクティブなアラーム、確認済みアラーム、またはアラーム履歴を表示できます。アラームの詳細については、次を参照してください。

- [アラームの説明 \(1 ページ\)](#)
- [すべてのアラームの表示 \(18 ページ\)](#)
- [アラームの詳細の表示 \(19 ページ\)](#)
- [アラーム履歴の表示 \(23 ページ\)](#)

アラームの説明

このセクションには、アラームと説明のリストが含まれています。アラームは、ポリシー内で構成されたときにトリガーされます。ポリシーの設定方法の詳細については、次のいずれかのトピックを参照してください。

- [Crosswork Cloud Network Insightsポリシーの追加](#)
- [Crosswork Cloud Traffic Analysisポリシーの追加](#)

予期しないASプレフィックス (Unexpected AS Prefix)

このアラームは、新しいプレフィックスが以前になかった AS の予期しない変更を検出します。モニタ対象の BGP AS から発信されるプレフィックスは、ピアしきい値の対象となる組織によって登録されていない場合、違反プレフィックスです。

考えられる検出される問題

このアラームは、新しいプレフィックスが以前に観察されなかった AS の予期しない変更またはルートリークのスナリオを特定するのに役立ちます。

関連するアラームルールの設定

このアラームルールを ASN ポリシー設定に追加する場合は、次のオプションを設定する必要があります ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)] > [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [ASNポリシー (ASN Policy)] > [ルールの追加 (Add Rule)] > [予期しないASプレフィックス (Unexpected AS Prefix)])。

- [しきい値](#) (アドバタイズされたプレフィックスごと)
- [プレフィックス サブスクリプション](#)

例

[予期しないASプレフィックス (Unexpected AS Prefix)] アラームルールを使用して ASN ポリシーを作成し、モニタ対象の AS 15169 にリンクします。また、AS 15169 から発信されると予想されるすべてのプレフィックスにも登録されます。設定不備により、プレフィックス 8.8.0.0/24 が AS からリークされます。同時に、プレフィックス 9.9.0.0/24 は正しくアドバタイズされませんが、登録されません。ピアのしきい値に応じて、これらのイベントは両方ともアラームをトリガーします。その後、プレフィックス 8.8.0.0/24 を取り消すように設定を修正し、アラームをクリアするプレフィックス 9.9.0.0/24 に登録できます。

AS発信元違反 (AS Origin Violation)

このアラームは、発信元 AS を持つモニタ対象プレフィックスのアドバタイズメントが [AS発信元リスト (AS Origin List)] にない場合に検出します。これは違反アドバタイズメントであり、特にアドバタイズメントの AS パス長が正規のアドバタイズメントよりも短い場合に、プレフィックスハイジャックの試みを表す可能性があります。



- (注) 問題にすぐに対処できるように、問題 (ルート情報の漏えい、または何らかのタイプの設定不備) を起こしている可能性があるピアを知っておくと役立ちます。[マイピア (My Peers)] ルールは、特定の Crosswork Cloud サブスクリプションでこのアラームに使用できます。 [c_subscription-plan-options.xml](#) [マイピア (My Peers)] オプションは、ピアからの BGP 更新のみに従いますが、[すべてのピア (All Peers)] はピアおよびグローバルピアからの BGP 更新に従います。 [ピアの追加](#) このオプションを設定するには、 [Crosswork Cloud Network Insights](#) ポリシーの [追加](#)、

考えられる検出される問題

このアラームは、ルートリークまたはプレフィックスハイジャックの特定に役立ちます。

関連するアラームルールの設定

このアラームルールをプレフィックスポリシー設定に追加する場合は、次のオプションを設定する必要があります ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)])

> [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [プレフィックスポリシー (Prefix Policy)] > [ルール of 追加 (Add Rule)] > [AS発信元違反 (AS Origin Violation)]。

- しきい値
- 許可された発信元 ASN

例

プレフィックス 8.8.8.0/24 の [AS発信元違反 (AS Origin Violation)] アラームルールでプレフィックスポリシーを作成し、[AS発信元リスト (AS Origin List)] フィールド値が 15169 で設定されています。しかし、確認された BGP 更新が 8.8.8.0/24 および 109 の発信元 AS で受信されます。AS 109 が [AS発信元リスト (AS Origin List)] に含まれていないために、このアラームがトリガーされます。

新しいASパスのエッジ (New AS Path Edge)

このアラームは、以前に確認されていない新しい AS ピアリングを検出します。

中間者 (MITM) 攻撃では、攻撃者が自身の AS をプレフィックスの AS パスに挿入し、AS を介してプレフィックスのトラフィックを誘導します。攻撃の検出を回避するために、MITM 攻撃は通常短命で、少数のプレフィックスをターゲットとします。

一時的な AS ピアリングの別の原因として、すぐに修正されるオペレータエラーが考えられます。



- (注) AS ピアリング関係は、多くのピアによってアドバタイズされた多数のプレフィックスの AS パスに存在するか、または長期間存続しますが、正当なネットワーク設定の変更である可能性が高く、Crosswork Cloud Network Insights ではこれらのアラートは表示されません。

考えられる検出される問題

このアラームは、潜在的な MITM 攻撃またはオペレータエラーの特定に役立ちます。

例

[新しいASパスのエッジ (New AS Path Edge)] アラームルールを使用してプレフィックスポリシーを作成し、プレフィックス 8.8.0.0/24 にリンクします。アラームは、Crosswork Cloud Network Insights が、疑わしい AS ピアリング (すべてのプレフィックスのすべてのパスで以前に確認されていないピアリング、または新しいピアリング) を含む AS パスでプレフィックス 8.8.0.0/24 がアドバタイズされたことを検出したときにトリガーされます。一定の時間が経過すると、Crosswork Cloud Network Insights は、これらの AS ピアリング関係が長期間存続していると判断します。ピアリング関係が長期間存続していると判断されると、アラームはクリアされます。

ASパス長違反 (AS Path Length Violation)

設定されたプレフィックスの AS パス長が上限しきい値または下限しきい値を超えた場合に検出します。このアラームは、観察された AS パスが、AS パス長の下限しきい値を下回るか、上限しきい値を超えた場合に検出します。

BGP AS パスは、プレフィックスの遅延に影響しますが、BGP ベストパス選択 (ベストパス選択で使用される最も高い設定不可能な属性) の重要なタイプブレークステップでもあります。より短い AS パスが優先されるため、このプロパティはハイジャッカーによって悪用される可能性があります。モニタ対象プレフィックスの AS パス長に予想範囲を設定する必要があります。アドバタイズされたこの範囲外の AS パス長は、違反アドバタイズメントです。



- (注) 問題にすぐに対処できるように、問題 (ルート情報の漏えい、または何らかのタイプの設定不備) を起こしている可能性があるピアを知っておくと役立ちます。[マイピア (My Peers)] ルールは、特定の Crosswork Cloud サブスクリプションでこのアラームに使用できます。 [c_subscription-plan-options.xml](#)[マイピア (My Peers)] オプションは、ピアからの BGP 更新のみに従いますが、[すべてのピア (All Peers)] はピアおよびグローバルピアからの BGP 更新に従います。 [ピアの追加](#)このオプションを設定するには、[Crosswork Cloud Network Insights](#)ポリシーの追加、

考えられる検出される問題

このアラームは、ルートルークまたはハイジャックの特定に役立ちます。また、モニタ対象プレフィックスの遅延のモニタにも役立ちます。

関連するアラームルールの設定

このアラームルールをプレフィックスポリシー設定に追加する場合は、次のオプションを設定する必要があります ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)] > [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [プレフィックスポリシー (Prefix Policy)] > [ルールの追加 (Add Rule)] > [ASパス長違反 (AS Path Length Violation)])。

- [しきい値](#)
- [許可されたASパス長の範囲 (Allowed AS path length range)]

例

[ASパス長違反 (AS Path Length Violation)] アラームルールを使用してプレフィックスポリシーを作成し、プレフィックス 8.8.0.0/24 および 9.9.0.0/24 にリンクします。プレフィックス 8.8.0.0/24 は、異なるピアリングポイントを介してユーザによってリークされることにより、AS パスが短くなり、アラームがトリガーされます。アラームは、プレフィックス 8.8.0.0/24 が正当なアドバタイズメント (許可された範囲内のパス長) によってアドバタイズされるとクリアされます。後で、プレフィックス発信元 9.9.0.0/24 からのアップストリームパスでピアリング関係が変更されると (正当または MITM 攻撃により)、より長い AS パスでアドバタイズされます。

これらのアップストリーム関係をほとんど制御できない可能性があり、設定された AS パス範囲をアラームがクリアされるように変更する必要があります。

親集約の変更 (Parent Aggregate Change)

このアラームは、予期しないスーパーネットまたはしきい値違反を検出します。

ネットワークオペレータは通常、アドバタイズされたプレフィックスの直接のスーパーネットプレフィックス (集約またはサマリー)、およびその他の集約された上位スーパーネット、およびそれらの発信元 AS を認識しています。ユーザは、Classless inter-domain routing (CIDR) プレフィックス長を指定して、予想される IPv4 および IPv4 スーパーネットのセットを少なくとも 1 つ設定する必要があります。ユーザは、許可された送信元 AS のリストから、観測された集約が発信されるように強制することもできます。



- (注) 問題にすぐに対処できるように、問題 (ルート情報の漏えい、または何らかのタイプの設定不備) を起こしている可能性があるピアを知っておくと役立ちます。[マイピア (My Peers)] ルールは、特定の Crosswork Cloud サブスクリプションでこのアラームに使用できます。[c_subscription-plan-options.xml](#)[マイピア (My Peers)] オプションは、ピアからの BGP 更新のみに従いますが、[すべてのピア (All Peers)] はピアおよびグローバルピアからの BGP 更新に従います。[ピアの追加](#)このオプションを設定するには、[Crosswork Cloud Network Insights](#)ポリシーの追加、

考えられる検出される問題

このアラームは、サマリープレフィックスの誤った取り消しやルートリークを特定するのに役立ちます。

関連するアラームルールの設定

このアラームルールをプレフィックスポリシー設定に追加する場合は、次のオプションを設定する必要があります ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)] > [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [プレフィックスポリシー (Prefix Policy)] > [ルールの追加 (Add Rule)] > [親集約の変更 (Parent Aggregate Change)])。

- [しきい値](#) (アドバタイズされた集約ごと)
- [許可された発信元ASN (Allowed Origin ASNs)] (オプション)
- [許可されるIPv4/IPv6スーパーネット (Allowed IPv4/IPv6 supernets)]

例

[親集約の変更 (Parent Aggregate Change)] アラームルールを使用してプレフィックスポリシーを作成し、プレフィックス 8.8.0.0/24 にリンクします。ポリシーは、許可された IPv4 集約プレフィックス長 [22,9] および許可された発信元 AS 3356 で設定されます。次のイベントがアラームをトリガーします。

- 予想されるスーパーネット 8.8.0.0/22 がハイジャックされます (プレフィックスは予期しない発信元 AS から発信されます)。
- 集約、プレフィックス 8.8.0.0/20 がアドバタイズされ、潜在的なリークとして識別されず。

リークまたはハイジャックが解決されるか、ユーザがアラーム設定を変更して、これらの集約アドバタイズメントが正当であることを示すと、アラームはクリアされます。

プレフィックスアドバタイズメント (Prefix Advertisement)

このアラームは、モニタ対象プレフィックスの優先 BGP パスでの予期しない変更を検出します。したがって、プレフィックスのアドバタイズされたパスの BGP 属性に対する予期しない変更をモニタし、潜在的なルートリークの広がりを確認できます。



- (注) 問題にすぐに対処できるように、問題 (ルート情報の漏えい、または何らかのタイプの設定不備) を起こしている可能性があるピアを知っておくと役立ちます。[マイピア (My Peers)] ルールは、特定の Crosswork Cloud サブスクリプションでこのアラームに使用できます。 [c_subscription-plan-options.xml](#) [マイピア (My Peers)] オプションは、ピアからの BGP 更新のみに従いますが、[すべてのピア (All Peers)] はピアおよびグローバルピアからの BGP 更新に従います。 [ピアの追加](#) このオプションを設定するには、 [Crosswork Cloud Network Insights ポリシーの追加](#)、

考えられる検出される問題

このアラームは、ルートリークまたはモニタ対象プレフィックスの優先 BGP パスの変更を特定するのに役立ちます。

関連するアラームルールの設定

このアラームルールをプレフィックスポリシー設定に追加する場合は、次のオプションを設定する必要があります ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)] > [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [プレフィックスポリシー (Prefix Policy)] > [ルールの追加 (Add Rule)] > [プレフィックスアドバタイズメント (Prefix Advertisement)])。

- [しきい値](#)

プレフィックスの取り消し (Prefix Withdrawal)

このアラームは、ピアがプレフィックスを取り消した場合に検出します。

少数の BGP ピアからのプレフィックスの取り消しは、プレフィックスに到達する複数のパスがあるため、必ずしもプレフィックスが到達不能であることを意味しません。ただし、多数のピアが地理的エリアのプレフィックスを取り消すと、プレフィックスの到達可能性が低下する

可能性があります。ルータのフラップによるノイズを抑制するために、このアラームのしきい値を他のアラームよりも高く設定することをお勧めします。



- (注) 問題にすぐに対処できるように、問題（ルート情報の漏えい、または何らかのタイプの設定不備）を起こしている可能性があるピアを知っておくと役立ちます。[マイピア (My Peers)] ルールは、特定の Crosswork Cloud サブスクリプションでこのアラームに使用できます。 [c_subscription-plan-options.xml](#) [マイピア (My Peers)] オプションは、ピアからの BGP 更新のみに従いますが、[すべてのピア (All Peers)] はピアおよびグローバルピアからの BGP 更新に従います。 [ピアの追加](#) このオプションを設定するには、 [Crosswork Cloud Network Insights](#) ポリシーの [追加](#)、

考えられる検出される問題

このアラームは、プレフィックスの取り消しにつながる設定不備を特定するのに役立ちます。

関連するアラームルールの設定

このアラームルールをプレフィックスポリシー設定に追加する場合は、次のオプションを設定する必要があります ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)] > [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [プレフィックスポリシー (Prefix Policy)] > [ルールの追加 (Add Rule)] > [プレフィックスの取り消し (Prefix Withdrawal)])。

- [しきい値](#)

ROAの有効期限 (ROA Expiry)

このアラームは、Route Origin Authorization (ROA) レコードの有効期限が切れる前に警告します。ROA レコードは、リソース (アドバタイズされたプレフィックス) の所有権を主張するオペレータによって作成され、地域インターネットレジストリ (RIR) またはルーティング資産データベース (RADB) などの他のサービスによって暗号化されて配布されます。詳細については、[ripe.net](#) を参照してください。

ROA レコードの有効期限切れの何日前にアラートを送信するかを指定できます。これは、情報提供を目的とするアラームです。新しいレコードを作成するアクションを実行して、ルータによるプレフィックスの考えられるフィルタリングを回避できます。このアラームは、プレフィックスが ROA レコードでカバーされていて、現在と設定したトリガー間隔の間 (現在 + [有効期限が切れる前にトリガーする日数 (Days to Trigger Before Expiration)]) のどの時点でも、プレフィックスに有効な ROA レコードがない場合にアクティブになります。特に、期限切れのレコードと期限が切れていないレコードが混在している場合、設定された間隔内のいずれかの時点で期限が切れていないカバーしているレコードが存在する限り、アラームはアクティブになりません。

考えられる検出される問題

このアラームは、保留中の ROA カバレッジの欠如を検出します。

関連するアラームルールの設定

このアラームルールをプレフィックスポリシー設定に追加する場合は、次のオプションを設定する必要があります ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)] > [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [プレフィックスポリシー (Prefix Policy)] > [ルールの追加 (Add Rule)] > [ROAの有効期限 (ROA Expiry)])。

- ROA レコードの期限が切れる前にトリガーする日数。

例

[ROAの有効期限 (ROA Expiry)] アラームルールを使用してプレフィックスポリシーを作成し、[有効期限が切れる前にトリガーする日数 (Days to Trigger Before Expiration)] に 30 を指定して、プレフィックス 8.8.0.0/24 にリンクします。このアラームは、プレフィックス 8.8.0.0/24 が複数の ROA レコードでカバーされている場合にトリガーされ、Crosswork Cloud Network Insights はこれらすべてのレコードがすでに期限切れになっているか、または 30 日未満で期限切れになることを検出します。アラームをクリアするには、トリガー時間間隔をカバーする 8.8.0.0/24 に対して少なくとも 1 つの ROA レコードを作成する必要があります。

ROA障害 (ROA Failure)

このアラームは、モニタ対象プレフィックスの **ROA 有効性状態** が無効かどうかを示します。発信元 AS がプレフィックスをカバーする ROA レコードにない、モニタ対象プレフィックスのアドバタイズメントは、違反アドバタイズメントです。アラームは、プレフィックスの観測されたすべての送信元 ASN を含む ROA レコードの追加、またはすべてのレコードの期限切れのいずれかによりクリアされます。具体的には、このアラームは、ROA レコードがない (存在しない、またはすべてが期限切れになっている) 場合はアクティブになりません。

ROA の詳細については、[ripe.net](https://www.ripe.net) を参照してください。

考えられる検出される問題

このアラームは、プレフィックスハイジャックの試行を特定するのに役立ちます。

関連するアラームルールの設定

このアラームルールをプレフィックスポリシー設定に追加する場合は、次のオプションを設定する必要があります ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)] > [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [プレフィックスポリシー (Prefix Policy)] > [ルールの追加 (Add Rule)] > [ROA障害 (ROA Failure)])。

- [しきい値](#)

ROAが見つからない (ROA Not Found)

プレフィックスは、それをカバーする複数の ROA レコードを持つことができます。このアラームは、モニタ対象のプレフィックスに ROA レコードがない (存在しない、または期限切れに

なっている) 場合にトリガーされます。これにより、RTR プロトコルを実装するルータによってプレフィックスがドロップされることを回避できます。

ROA の詳細については、ripe.net を参照してください。

考えられる検出される問題

これは、モニタ対象のプレフィックスに ROA レコードがないことをユーザに警告する情報アラームです。

DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal)

IANA によって割り当てられ、OpenDNS と Google によって提供されるサーバーを含むパブリック DNS ルートサーバーは、通常のルータ操作がパブリック インターネットルーティングに参加するために必要です。このアラームは、DNS サーバアドレスが属する一連のプレフィックス (ネットブロック) をモニタします。セット内のいずれかのプレフィックスが取り消されると、ユーザに警告します。



- (注) このアラームは [プレフィックスの取り消し (Prefix Withdrawal)] アラームとは異なります。これらのプレフィックスは、ユーザがサブスクリプションで消費するプレフィックスの合計量に追加されず、アラームルールにリンクされたピアからの取り消しだからです。

考えられる検出される問題

このアラームは、既知のルート DNS サーバプレフィックスがモニタ対象ピアのルーティングテーブルから削除されたかどうかを検出します。このアラームは、DNS ルートサーバーの撤回につながるインターネットルータの不良構成を特定するのに役立ちます。

関連するアラームルールの設定

このアラームルールをピアポリシー設定に追加する場合は、次のオプションを設定する必要があります ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)] > [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [ピアポリシー (Peer Policy)] > [ルールの追加 (Add Rule)] > [DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal)])。

- 監視対象の DNS ルートサーバー

例

[DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal)] アラームルールを使用してピアポリシーを作成し、ピア RTR1 にリンクします。プレフィックス 198.41.0.0/24 (A ルートサーバ) および 2001:7fd::/48 (K ルートサーバ) に対するアラートを受け取ることを選択します。アラームは、これらのプレフィックスのいずれかが RTR1 によって取り消されるとアクティブになり、両方がアドバタイズされるとクリアされます。

サブプレフィックスアドバタイズメント (SubPrefix Advertisement)

ハイジャッカーは、ルータが新しいサブプレフィックスをインストールすることで、モニタ対象プレフィックスによってカバーされる IP スペースの一部のトラフィックをリダイレクトできます。これは、ルータが具体的ではないルートよりも具体的なルートを優先するためです。ハイジャッカーは、既存のサブプレフィックスの新しいルートをインストールすることもできます。これらのハイジャックの試行を検出するために、サブプレフィックスの許可された発信元 ASN のリストを設定できます。このアラームの場合、違反アドバタイズメントは、アドバタイズされたサブプレフィックスとそのピアのしきい値のいずれかが違反している場合です。

考えられる検出される問題

このアラームは、ルートリークまたはモニタ対象プレフィックスのサブプレフィックスのハイジャックを特定するのに役立ちます。

関連するアラームルールの設定

このアラームルールをプレフィックスポリシー設定に追加する場合は、次のオプションを設定する必要があります ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)] > [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [プレフィックスポリシー (Prefix Policy)] > [ルールの追加 (Add Rule)] > [サブプレフィックスアドバタイズメント (SubPrefix Advertisement)])。

- [プレフィックスサブスクリプション](#)
- アドバタイズされたサブプレフィックスごとのしきい値 (Peers to Resolve および Peers to Trigger) [アラームのしきい値](#)
- 許可された発信元 ASN



(注) 発信元 ASN リストを無視するには、[発信元ASNリストを使用 (Use Origin ASNs)] オプションを [いいえ (No)] に切り替えます。発信元 ASN リストが無視されると、すべての ASN に対してアラームがトリガーされます。

- IPv4/IPv6 の最大長：設定された IPv4/IPv6 の最大長よりも長いサブプレフィックスマスクを無視するオプションを使用できます。IPv4 の最大長は 8 より大きく、IPv6 の最大長は 16 より大きい必要があります。

例

[サブプレフィックスアドバタイズメント (Subprefix Advertisement)] アラームルールを使用してプレフィックスポリシーを作成し、プレフィックス 8.8.0.0/24 にリンクします。次のサブプレフィックスアドバタイズメントが発生し、アラームがトリガーされます。

- 予期しないサブプレフィックス 8.8.0.5/30 がアドバタイズされます。この場合、このプレフィックスは新しい管理組織に割り当てられ、新しい発信元 AS から初めてアドバタイズされます。このアラームをクリアするには、サブプレフィックス 8.8.0.5/30 を登録するように Crosswork Cloud Network Insights を設定するか、または新しい発信元 AS を許可された発信元 ASN のリストに追加します。
- 予期しないサブプレフィックス 8.8.0.4/30 がアドバタイズされます。これは、ルートリークまたはハイジャックのいずれかを示している可能性があります。このアラームをクリアするには、8.8.0.4/30 を取り消す必要があります。

アップストリームASの変更 (Upstream AS Change)

BGP オペレータは、アウトバウンドポリシー（たとえば、どのアップストリーム AS がプレフィックスを伝播できるか）によってピアリング関係を制御できます。このアラームは、プレフィックスを伝播しない既存のピアへのルートリークを検出します。ユーザは、許可されたアップストリーム ASN のリストを設定する必要があります。リストにないアップストリーム AS パスに 1 ホップが残っている ASN を持つモニタ対象プレフィックスのアドバタイズメントは、違反アドバタイズメントです。



- (注) 問題にすぐに対処できるように、問題（ルート情報の漏えい、または何らかのタイプの設定不備）を起こしている可能性があるピアを知っておくと役立ちます。[マイピア (My Peers)] ルールは、特定の Crosswork Cloud サブスクリプションでこのアラームに使用できます。[c_subscription-plan-options.xml](#)[マイピア (My Peers)] オプションは、ピアからの BGP 更新のみに従いますが、[すべてのピア (All Peers)] はピアおよびグローバルピアからの BGP 更新に従います。[ピアの追加](#)このオプションを設定するには、[Crosswork Cloud Network Insights](#) ポリシーの追加、

考えられる検出される問題

このアラームは、モニタ対象プレフィックスのルートリークを特定するのに役立ちます。

関連するアラームルールの設定

このアラームルールをプレフィックスポリシー設定に追加する場合は、次のオプションを設定する必要があります ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)] > [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [プレフィックスポリシー (Prefix Policy)] > [ルールの追加 (Add Rule)] > [アップストリームASの変更 (Upstream AS Change)])。

- [しきい値](#)
- [許可されるアップストリームASN (Allowed upstream ASNs)]

例

[アップストリームASの変更 (Upstream AS Change)] アラームルールで許可されたアップストリームASN[293,1221]を使用してプレフィックスポリシーを作成し、プレフィックス8.8.0.0/24にリンクします。プレフィックス8.8.0.0/24は、ASパス[2711,1299,3356]を持つピアによってアドバタイズされます。AS1299は許可されたアップストリームASNではないため、しきい値が適用されて、アラームがトリガーされます。違反しているASパスを持つルートが取り消されるか、許可されたアップストリームASNのリストにAS1229が追加されると、アラームはクリアされます。

有効なASパス違反 (Valid AS Path Violation)

このアラームは、プレフィックスアドバタイズメントASパスが指定されたASNパターンと一致しない場合に検出します。

Crosswork Network Insightsは、設定された**有効なASパスパターン**を、アドバタイズされたプレフィックスのASパスと比較します。ASNパターンは、スペースで区切ったAS番号を順に並べた予測されるシーケンスであり、107 3462 109のように発信元ASで終わります。演算子を使用して複雑なパターンを表現できます。パターンが一致しない場合は、Crosswork Network Insightsはアラームをトリガーしてアクティブにします。



- (注) 問題にすぐに対処できるように、問題(ルート情報の漏えい、または何らかのタイプの設定不備)を起こしている可能性があるピアを知っておくと役立ちます。[マイピア (My Peers)]ルールは、特定のCrosswork Cloudサブスクリプションでこのアラームに使用できます。[c_subscription-plan-options.xml](#)[マイピア (My Peers)]オプションは、ピアからのBGP更新のみに従いますが、[すべてのピア (All Peers)]はピアおよびグローバルピアからのBGP更新に従います。[ピアの追加](#)このオプションを設定するには、[Crosswork Cloud Network Insightsポリシーの追加](#)、

パターンの例: [0-]* 806 * 200

- 有効なASパス: 1900 1731 806 100 200
- 違反ASパス: 1900 1731 807 100 200
- 違反ASパス: 1900 1731 806 150 100 200

考えられる検出される問題

このアラームは、潜在的なMITM攻撃または遅延の低下を示す予期しないBGP ASパスの変更を検出します。

関連するアラームルールの設定

このアラームルールをプレフィックスポリシー設定に追加する場合は、次のオプションを設定する必要があります ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)]

> [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [プレフィックスポリシー (Prefix Policy)] > [ルールの追加 (Add Rule)] > [有効なASパス違反 (Valid AS Path Violation)])。

- しきい値

ピアの停止 (Peer Down)

このアラームは、Crosswork Cloud Network Insights とモニタ対象ピアとの間のピアリングセッションの状態をモニタします。Crosswork Cloud Network Insights とモニタ対象ピアとの間のピアリングセッションが、予測されていた確立状態でない場合に、問題が発生する可能性があります。ピアリングセッションが確立状態になると、アラームはクリアされます。

考えられる検出される問題

このアラームは、モニタ対象ピアでの BGP プロセスの問題、またはピアリングに影響を与えるハードウェアやソフトウェアの問題を特定するのに役立ちます。

アドバタイズされたプレフィックスの数 (Advertised Prefix Count)

このアラームは、モニタ対象ピアの RIB のサイズをモニタします。Crosswork Cloud Network Insights は、すべてのモニタ対象ピアに関連する統計情報 (各ピアが Crosswork Cloud Network Insights にアドバタイズするプレフィックスの数を含む) を定期的に収集します。モニタ対象ピアから Crosswork Cloud Network Insights にアドバタイズされると予想されるプレフィックスの数に対して、少なくとも1つの IPv4/IPv6 アドレスファミリー範囲を設定する必要があります。アドバタイズされたプレフィックスの数が予想される最小数を下回った場合は、モニタ対象ピアと Crosswork Cloud Network Insights またはその他のピアとの間のピアリングセッションに問題があることを示しています。また、ピアに適用されている、モニタ対象ピアに設定されたインバウンドポリシーの制限が Crosswork Cloud Network Insights よりも厳しい場合や、Crosswork Cloud Network Insights ピアに適用されているアウトバウンドポリシーの制限が厳しい場合にも発生します。逆に、アドバタイズされたプレフィックスの数が予想される最大数を超過している場合は、制限の緩いポリシーが設定されているか、またはプレフィックスアドバタイズメントでピアに大きな負担をかける悪意のある試みを示している可能性があります。

考えられる検出される問題

このアラームは、ピアリングの問題 (ソフトウェア、ハードウェア、または設定不備の問題による) またはピアでの DoS 攻撃を特定するのに役立ちます。

関連するアラームルールの設定

このアラームルールを ASN ポリシー設定に追加する場合は、次のオプションを設定する必要があります ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)] > [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [ピアポリシー (Peer Policy)] > [ルールの追加 (Add Rule)] > [アドバタイズされたプレフィックスの数 (Advertised Prefix Count)])。

- 予期されるプレフィックスの数の範囲 (IPv4/IPv6 アドレスファミリーごと)

例

ピア RTR1 にリンクされている、[アドバタイズされたプレフィックスの数 (Advertised Prefix Count)] アラームルールで、予期される IPv4 プレフィックス範囲 [1000, 800000] を使用して、ピアポリシーを作成します。RTR1 から Crosswork Cloud Network Insights にアドバタイズされた IPv4 プレフィックスの数がこの範囲外で、以前に記録されたものと異なる場合、アラームはデータ収集イベントごとにアクティブになります。

禁止されたIPプレフィックス (Prohibited IP Prefix)

このアラームは、監視対象ピアの Routing Information Base (RIB) にインストールされているパブリック IP ルーティングスペースに禁止されたプレフィックスがあるか、または監視対象ピアがそれを転送している場合に検出します。

Bogon は、予約されているか、地域インターネットレジストリ (RIR) に割り当てられていないため、パブリックではない IP アドレスブロックです。[フルBogon (Full bogons)] には、RIR に割り当てられているが、RIR によって特定のネットワークに割り当てられていないアドレスブロックも含まれます。禁止されたプレフィックスのアドバタイズメントをルータでフィルタリングすることをお勧めします。ユーザーは、このアラームを使用して、Bogon アドバタイズメントについてのみアラートを受け取るように選択できます。

考えられる検出される問題

このアラームは、ルータに対する DoS 攻撃の特定に役立ちます。

関連するアラームルールの設定

このアラームルールをピアポリシー設定に追加する場合は、[Bogon (Bogons)] または [フル Bogon (Full bogons)] を選択します ([外部ルーティング分析 (External Routing Analysis)] > [設定 (Configure)] > [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [ピアポリシー (Peer Policy)] > [ルールの追加 (Add Rule)] > [禁止されたIPプレフィックス (Prohibited IP Prefix)])。

例

[禁止されたIPプレフィックス (Prohibited IP Prefix)] アラームルールでオプション [Bogons] を使用してピアポリシーを作成し、ピア RTR1 にリンクします。RTR1 が 10.0.0.0/24 (RFC1918 による BOGON) を Crosswork Cloud Network Insights にアドバタイズすると、アラームはアクティブになりますが、2001:221::/32 (フル Bogons) がアドバタイズされるとアクティブになりません。

ゲートウェイ接続

Crosswork Data Gateway が Crosswork Cloud Traffic Analysis 用にインストールされると、Crosswork Data Gateway と Crosswork Cloud の間の接続をモニターするポリシーが自動的に作成されます。Crosswork Data Gateway が Crosswork Cloud への接続を失った場合 (レポート間隔内で Crosswork

Cloudとの通信に失敗した場合)、アラームが生成され、Crosswork Cloud Traffic Analysis[アラーム (Alarms)]ページに表示されます (🔍>[モニター (Monitor)]>[アラーム (Alarms)])。ゲートウェイ接続の詳細を表示したり、アラーム重大度レベル、モニター対象ゲートウェイのリスト、または通知エンドポイントを更新したりするには、次の手順を実行します。

ステップ 1 🔍 > [構成 (Configure)] > [ポリシー (Policies)] の順に選択します。

[ゲートウェイ接続 (Gateway Connectivity)] で、アクティブなアラームの数、モニター対象のゲートウェイの数、および最新のアクティブなアラームを持つゲートウェイを表示できます。

ステップ 2 [ゲートウェイ接続 (Gateway Connectivity)] で、[詳細 (Details)] をクリックします。

ステップ 3 デフォルトでは、[概要 (Overview)] タブに現在のゲートウェイ接続ポリシーの設定が表示されます。

ステップ 4 アラームの詳細を表示するには、[アラーム (Alarms)] タブをクリックします。このページから、[ゲートウェイ接続の喪失 (Lost Gateway Connection)] アラームをクリックして特定のアラームの詳細を確認したり、[アクティブ (Active)]、[確認 (Acknowledge)]、または [履歴 (History)] のタブ間を移動したりできます。

ステップ 5 アラームの重大度やモニター対象ゲートウェイのリストを変更したり、エンドポイント通知の設定をしたりするには、[編集 (Edit)] をクリックします。

- [トリガー (Triggers)] > [ゲートウェイルール (Gateway Rules)] > [重大度 (Severity)] ドロップダウンメニューで、重大度を選択します。
- [データ (Data)] で、[変更 (Modify)] をクリックして、モニターまたは無視するゲートウェイを更新します。
- [アクション (Actions)] で、既存のエンドポイント通知を変更、もしくはさらに追加できます。設定できるエンドポイント通知のタイプの詳細については、[通知エンドポイントについて](#) を参照してください。
- [保存 (Save)] をクリックします。

デバイスの接続性

デバイスが Crosswork Data Gateway にリンクされて Crosswork Cloud Traffic Analysis に追加されると、Crosswork Data Gateway とそのデバイス間の接続をモニターするためのポリシーが自動的に作成されます。Crosswork Data Gateway がデバイスとの接続を失うと、アラームが生成され、Crosswork Cloud Traffic Analysis [アラーム (Alarms)] ページに表示されます (🔍>[モニター (Monitor)]>[アラーム (Alarms)])。

デバイス接続の詳細を表示したり、重大度レベル、モニター対象デバイスのリスト、または通知エンドポイントを更新したりするには、次の手順を実行します。


ステップ 1 🔍 > [構成 (Configure)] > [ポリシー (Policies)] の順に選択します。

[デバイス接続 (Device Connectivity)] で、アクティブなアラームの数、モニタ対象のデバイスの数、および最新のアクティブなアラームを持つデバイスを表示できます。

- ステップ 2** [デバイス接続 (Device Connectivity)] で、[詳細 (Details)] をクリックします。
- ステップ 3** デフォルトでは、[概要 (Overview)] タブに現在のデバイス接続のポリシー設定が表示されます。
- ステップ 4** アラームの詳細を表示するには、[アラーム (Alarms)] タブをクリックします。このページから、[デバイス接続の喪失 (Lost Device Connection)] アラームをクリックして特定のアラームの詳細を確認したり、[アクティブ (Active)]、[確認 (Acknowledge)]、または[履歴 (History)] のタブ間を移動したりできます。
- ステップ 5** アラームの重大度やモニター対象デバイスのリストを変更したり、エンドポイント通知の設定をしたりするには、[編集 (Edit)] をクリックします。
- [トリガー (Triggers)] > [デバイスルール (Device Rules)] > [重大度 (Severity)] ドロップダウンメニューで、重大度を選択します。
 - [データ (Data)] で、[変更 (Modify)] をクリックして、モニターまたは無視するデバイスを更新します。
 - [アクション (Actions)] で、既存のエンドポイント通知を変更、もしくはさらに追加できます。設定できるエンドポイント通知のタイプの詳細については、[通知エンドポイントについて](#) を参照してください。
 - [保存 (Save)] をクリックします。


インターフェイス TX の使用率

このアラームは、送信トラフィック情報をモニターし、インターフェイスの TX 使用率が指定した範囲外の場合にトリガーされます。このアラームを設定するには、次の手順を実行します。

- ステップ 1** メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。
- ステップ 2** [ポリシーを追加 (Add Policy)] をクリックします。
- ステップ 3** [名前 (Name)] フィールドでポリシー名を入力します。
- ステップ 4** [トリガー (Triggers)] で、[ルールの追加 (Add Rules)] をクリックします。
- ステップ 5** [インターフェイス TX の使用率 (Interface TX Utilization)] をクリックします。
- ステップ 6** [Next] をクリックします。
- ステップ 7** デフォルトでは、ルールが有効になっています。ルールをまだ使用しない場合は、スイッチを [無効 (DISABLED)] に切り替えます。
- ステップ 8** このアラームをトリガーする使用率の範囲を示すには、スライダを使用します。使用率が赤色と ALARM テキストで示される範囲内にある場合、Crosswork Cloud から通知が届きます。
- ステップ 9** [重大度 (Severity)] ドロップダウンリストで、このアラームに定義する重大度を選択します。
- ステップ 10** その他の必要なインターフェイスおよびエンドポイント通知の設定を行い、[保存 (Save)] をクリックします。


インターフェイス RX の使用率

このアラームは、受信トラフィック情報をモニターし、インターフェイスの RX 使用率が指定した範囲外になった場合にトリガーされます。このアラームを設定するには、次の手順を実行します。

- ステップ 1 メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。
- ステップ 2 [ポリシーを追加 (Add Policy)] をクリックします。
- ステップ 3 [名前 (Name)] フィールドでポリシー名を入力します。
- ステップ 4 [トリガー (Triggers)] で、[ルールの追加 (Add Rules)] をクリックします。
- ステップ 5 [インターフェイス RX の使用率 (Interface RX Utilization)] をクリックします。
- ステップ 6 [Next] をクリックします。
- ステップ 7 デフォルトでは、ルールが有効になっています。ルールをまだ使用しない場合は、スイッチを [無効 (DISABLED)] に切り替えます。
- ステップ 8 このアラームをトリガーする使用率の範囲を示すには、スライダを使用します。使用率が赤色と ALARM テキストで示される範囲内にある場合、Crosswork Cloud から通知が届きます。
- ステップ 9 [重大度 (Severity)] ドロップダウンリストで、このアラームに定義する重大度を選択します。
- ステップ 10 その他の必要なインターフェイスおよびエンドポイント通知の設定を行い、[保存 (Save)] をクリックします。

プレフィックス使用率

このアラームは、プレフィックスのキャパシティをモニターするもので、モニター対象インターフェイスのプレフィックスの1つが合計キャパシティのうち最大となるパーセンテージを超えた場合にトリガーされます。このアラームを設定するには、次の手順を実行します。

- ステップ 1 メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。
- ステップ 2 [ポリシーを追加 (Add Policy)] をクリックします。
- ステップ 3 [名前 (Name)] フィールドでポリシー名を入力します。
- ステップ 4 [トリガー (Triggers)] で、[ルールの追加 (Add Rules)] をクリックします。
- ステップ 5 [プレフィックス使用率 (Prefix Utilization)] をクリックします。
- ステップ 6 [Next] をクリックします。
- ステップ 7 デフォルトでは、ルールが有効になっています。ルールをまだ使用しない場合は、スイッチを [無効 (DISABLED)] に切り替えます。
- ステップ 8 このアラームをトリガーする使用率の範囲を示すには、スライダを使用します。使用率が赤色と ALARM テキストで示される範囲内にある場合、Crosswork Cloud から通知が届きます。
- ステップ 9 [重大度 (Severity)] ドロップダウンリストで、このアラームに定義する重大度を選択します。

ステップ 10 その他の必要なインターフェイスおよびエンドポイント通知の設定を行い、[保存 (Save)] をクリックします。

すべてのアラームの表示

アクティブなアラームは、ポリシーのいずれかの条件が満たされると生成されます。[アラーム (Alarms)] ページで発生する可能性のあるアラームの説明を表示するには、[アラームの説明 \(1 ページ\)](#) を参照してください。アラームの詳細を表示するには、[アラームの詳細の表示 \(19 ページ\)](#) を参照してください。

ステップ 1 メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [アラーム (Alarms)] の順にクリックします。

ステップ 2 [アラーム (Alarms)] ページの上部にある次のいずれかのタブをクリックします。

- [アクティブ (Active)] : すべてのアクティブなアラームのリストが表示され、優先順位でソートされます。
- [確認済み (Acknowledged)] : 優先順位でソートされたすべての確認済みアラームのリストが表示されます。
- [履歴 (History)] : [タイムフレーム (Timeframe)] ドロップダウンリストから時間範囲を指定できる履歴アラームが表示されます。詳細については、[アラーム履歴の表示 \(23 ページ\)](#) を参照してください。

次の表で、アラームフィールドについて説明します。

表 1: アラームのフィールドに関する説明

カラム	説明
アラームの詳細 (Alarm Details)	違反してアラームをトリガーしたルール。詳細については、 アラームの詳細の表示 (19 ページ) を参照してください。
トリガー (Trigger)	アラームが発生したプレフィックスまたは ASN。プレフィックスまたは ASN の詳細については、このリンクをクリックしてください。
ポリシー (Policy)	アラームをトリガーしたポリシーの名前。このリンクをクリックすると、ポリシーに関する詳細が表示されます。
# ピア (# Peers)	アラームをレポートしたピアの数。
シビラティ (重大度) (Severity)	設定されたアラームのシビラティ (重大度) レベル。
アクティブ化 (Activated)	アラームの発生時刻。

カラム	説明
注記 (Notes)	ユーザが入力したアラームに関するメモ。アイコンをクリックしてメモを表示します。

- ステップ 3** 昇順または降順で列をソートできます。いずれかの列の見出しにカーソルを合わせ、表示される下矢印をクリックして、ソート順を変更するか、フィルタリングするテキストを入力します。
- ステップ 4** 一時的にアラームのアラートを停止するには、アラームの横にあるボックスをクリックしてから、[スヌーズ (Snooze)] をクリックします。
- ステップ 5** アラームをスヌーズする時間範囲を選択し、[スヌーズ (Snooze)] をクリックします。Crosswork Cloud Network Insights では、選択した期間、このアラームの通知は送信されません。
- ステップ 6** アラームを確認済みの状態にするには、アラームの横にあるボックスをクリックしてから、[確認 (Acknowledge)] をクリックします。

アラームの詳細の表示

特定のアラームに関する詳細情報を表示できます。

- ステップ 1** メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [アラーム (Alarms)] の順にクリックします。
- ステップ 2** 詳細を表示する特定のアラームをクリックします。[アラーム詳細 (Alarm Details)] ページが表示されます。
- ステップ 3** 右上隅にあるボタンを使用して、このアラームに関連する次の操作のいずれかを実行できます。
- [プレフィックス/ASNをポリシーから削除 (Remove Prefix/ASN from Policy)] をクリックして、ポリシーからアラームをトリガーしたプレフィックスまたは ASN とルールを削除します。
 - [スヌーズ (Snooze)] をクリックして一時的にアラームのアラートを停止し、アラームをスヌーズする時間範囲を選択してから、[スヌーズ (Snooze)] をクリックします。Crosswork Cloud Network Insights は、選択した期間、このアラームの通知は送信しません。

アラームをスヌーズすると、アラームは [アクティブ (Active)] アラームページから [確認済みアラーム (Acknowledged Alarm)] ページに移動します。[アラーム (Alarms)] > [履歴 (History)] タブでは、アラームの状態が [スヌーズ済み (Snoozed)] に設定されており、その状態のままになる時間が示されています。スヌーズしたアラームをキャンセルするには、[アラームの詳細 (Alarm details)] ページに戻り、[未確認 (Unacknowledge)] をクリックします。

- [確認 (Acknowledge)] をクリックして、アラームを確認済みの状態にします。これは、アラームが認識され、確認されることを意味します。

アラームを確認すると、アラームは [アクティブ (Active)] アラームページから [確認済み (Acknowledged)] ページに移動します。

ステップ 4 アラームに関する追加情報を表示するには、次のいずれかのタブをクリックします。

(注) 以下に説明するすべてのタブが、すべてのアラームタイプに表示されるわけではありません。指定したアラームタイプに関連するタブのみを使用できます。

- [概要 (Overview)]: このページはデフォルトで表示されます。アラームが発生したポリシーに含まれるアラームおよびルールに関する詳細が含まれています。詳細については、[アラームの概要の詳細 \(20 ページ\)](#) を参照してください。
- [関連するBGP更新 (Relevant BGP Updates)]: このアラームをトリガーしたピアによってレポートされたBGP更新に関する詳細が含まれています。詳細については、[アラームに関連するBGP更新の詳細 \(22 ページ\)](#) を参照してください。
- [プレフィックス (Prefixes)]: アラームのプレフィックス情報が含まれます。[アラームプレフィックスの詳細 \(21 ページ\)](#) を参照してください。
- [履歴 (History)]: アラームに関する履歴の詳細が含まれています。詳細については、[アラーム履歴の表示 \(23 ページ\)](#) を参照してください。

アラームの概要の詳細

アラームの概要の詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)]>[モニター (Monitor)]>[アラーム (Alarms)]の順にクリックし、詳細を表示する特定のアラームをクリックしてから、[概要 (Overview)]タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、アラームの概要の詳細が表示されます。

表 2: アラームの概要のフィールドに関する説明

フィールド	説明
重大度	設定されたアラームのシビラティ (重大度) レベル。
アクティブ化 (Activated)	アラームの発生時刻。
非アクティブ化 (Deactivated)	アラームが以前に非アクティブ化された日時。
最後のユーザアクション (Last User Action)	ユーザがこのアラームに対して実行した直近のアクション。
想定される結果 (Expected)	Crosswork Cloud Network Insights がアラームをレポートすることを想定する値。
観察 (Observed)	Crosswork Cloud Network Insights によって観察された実際の値。
違反ピア	違反を観察したピア。

フィールド	説明
地理的マップ (Geographical map)	アラームが発生した場所。
注記 (Notes)	アラームに関するメモを入力します。

アラーム検索グラスの詳細

アラームの検索グラスの詳細を表示するには、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [アラーム (Alarms)] の順にクリックし、詳細を表示するアラームの [表示 (View)] をクリックしてから、[検索グラス (Looking Glass)] タブをクリックします。



(注) このタブは、使用可能で、指定したアラームタイプに関連する場合にのみ表示されます。

Crosswork Cloud Network Insights では、次の表に示すように、アラームの検索グラスの詳細が表示されます。

表 3: アラーム検索グラスのフィールドに関する説明

フィールド	説明
ピア AS (Peer AS)	ピア AS。
ピア (Peer)	ピアを識別するために使用されるが、その ID は非公開のままに維持するピア識別子。
AS パス (AS Path)	AS ルーティングパス。
コミュニティ (Communities)	コミュニティのパス属性 (該当する場合)。
最終変更日 (Last Modified)	プレフィックスが最後に変更された日時。

アラームプレフィックスの詳細

アラームのプレフィックスの詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニター (Monitor)] > [アラーム (Alarms)] の順にクリックし、詳細を表示する特定のアラームをクリックしてから、[プレフィックス (Prefixes)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、アラームのプレフィックスの詳細が表示されます。

表 4: アラームプレフィックスのフィールドに関する説明

フィールド	説明
違反 (Violating)	予期しないプレフィックスを表示するには、[違反 (Violating)] をクリックします。
登録 (Subscribed)	[登録 (Subscribed)] をクリックすると、自分が登録しているプレフィックスのみが表示されます。
すべて (All)	[すべて (All)] をクリックすると、すべての違反プレフィックスおよび登録済みプレフィックスが表示されます。
プレフィックス (Prefix)	違反が発生したプレフィックス。
レポートピア (Reporting Peers)	違反をレポートしたピアの数。
登録 (Subscribed)	プレフィックスに登録されているかどうかを示します。

アラームに関連する BGP 更新の詳細

アラームに関連する BGP 更新の詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニター (Monitor)] > [アラーム (Alarms)] の順にクリックし、詳細を表示する特定のアラームをクリックしてから、[関連する BGP 更新 (Relevant BGP Updates)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、アラームに関連する BGP 更新の詳細が表示されます。

表 5: アラーム関連の BGP 更新のフィールドに関する説明

フィールド	説明
非表示 (Not displayed)	更新が 6 ヶ月より古い違反ピアが表示されない場合は、メモが表示されます。
ピア (Peer)	BGP 更新を受信したピア。
ピア AS (Peer AS)	BGP 更新を受信したピア AS。
プレフィックス (Prefix)	BGP 更新を受信したプレフィックス。
AS パス (AS Path)	AS ルーティングパス。
コミュニティ (Communities)	コミュニティのパス属性 (該当する場合)。
更新のタイプ (Update Type)	BGP 更新のタイプ。
最終更新日 (Last Updated)	前回の BGP 更新の日時。

アラームサブプレフィックスの詳細

アラームのサブプレフィックスの詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニター (Monitor)] > [アラーム (Alarms)] の順にクリックし、詳細を表示する特定のアラームをクリックしてから、[サブプレフィックス (Subprefixes)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、アラームのサブプレフィックスの詳細が表示されます。

表 6: アラームサブプレフィックスのフィールドに関する説明



フィールド	説明
プレフィックス (Prefix)	サブプレフィックスがアドバタイズされたプレフィックス。
登録 (Subscribed)	プレフィックスに登録されているかどうかを示します。
ピア AS (Peer AS)	サブプレフィックス アドバタイズメントのピア AS。
ピア (Peer)	サブプレフィックス アドバタイズメントのピア。
AS パス (AS Path)	AS ルーティングパス。
コミュニティ (Communities)	コミュニティのパス属性 (該当する場合)。
最終変更日 (Last Modified)	最後に行った変更の日時。

アラーム履歴の表示



[アラーム履歴 (Alarm history)] ページには、時間範囲を指定できる履歴アラームが表示されます。デフォルトでは、アラームは最新の [イベント (EVENTAt)] の日付でソートされます。アラームの履歴には、そのライフサイクル中に発生したすべての状態遷移が含まれます。アラーム履歴レコードは変更されません。

ステップ 1 このページには次のようにしてアクセスできます。

• Crosswork Cloud Network Insights の場合 :


-  > [モニター (Monitor)] > [アラーム (Alarms)] から、詳細を表示する特定のアラームをクリックし、[履歴 (History)] タブをクリックします。
-  > [設定 (Configure)] > [ポリシー (Policies)] <ポリシー名> > [アラーム (Alarms)] タブ > [履歴 (History)] タブをクリックします。

- Crosswork Cloud Traffic Analysis の場合 :

-  > [モニター (Monitor)] > [アラーム (Alarms)] から、詳細を表示する特定のアラームをクリックし、[履歴 (History)] タブをクリックします。
-  > [設定 (Configure)] > [ポリシー (Policies)] <ポリシー名> > [アラーム (Alarms)] タブ > [履歴 (History)] タブをクリックします。

ステップ 2 [タイムフレーム (Timeframe)] ドロップダウンリストから、目的の期間を選択します。ウィンドウが更新され、選択した時間範囲のアラート情報が表示されます。

ステップ 3 [フィルタの追加 (Add Filter)] テキストを表示する任意の列をフィルタリングできます。[フィルタの追加 (Add Filter)] をクリックし、フィルタリングするテキストを入力します。

ステップ 4 [タイムフレーム (Timeframe)] ドロップダウンリストで、次のタスクのいずれかをクリック  して実行します。

- [列のカスタマイズ (Customize Columns)] : デフォルトでは、使用可能なすべての列が表示されるわけではありません。列を追加、削除、または並べ替えるには、このオプションを選択します。
- [CSVのエクスポート (Export CSV)] : 現在ロードされているすべての行をエクスポートするには、このオプションを選択します。

(注) ロードされた行は、現在表示されている行であり、合計の全体の一部にすぎない可能性があります。下にスクロールすると、さらに多くの行をロードできます。
- [テーブル設定の保存 (Save Table Settings)] : カスタマイズしたテーブル設定を保存するには、このオプションを選択します。これには、列幅のサイズ変更、列の追加または削除、および適用されたフィルタが含まれます。最初にテーブル設定を保存した後、[テーブル設定の削除 (Remove Table Settings)] または [テーブル設定の更新 (Update Table Settings)] を選択できます。

(注) トリガー値の上にマウスを合わせると、Whois 情報が表示されます (使用可能な場合)。

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。