paloalto TECHDOCS

NGFWのインシデントとアラート

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

January 31, 2025

Table of Contents

アラート

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	以下のいずれかです: ❑ 又は ❑ 又は

AIOps for NGFWは、デバイスの継続的な健全性を維持し、業務を中断するインシデントを回避するために、ファイアウォールのデプロイメントで検出された1つ以上の問題に基づいてアラートを生成します。これらの問題、つまりイベントは、次の3つの方法のいずれかでトリガーされます。

- 指標が大きく変わる場合
- 以前に生成されたイベントが変更された場合
- ユーザーまたはシステムがアラートの確認応答や終了などのアクションを実行する場合

アラートは、対処する必要がある特定の問題（ファイアウォール機能の低下または喪失）を示します。アラートは、複数のイベント間の相関や集約に基づいて生成することもできます。このようにイベントを1つのアラートに集約することで、トリアージ、チーム間でのアラートハンドオフの効率化、重要情報の一元化、通知の疲労軽減などを実現します。

アラートは、関連付けられているメトリックに応じて、さまざまなカテゴリに分類されます。アラート カテゴリを使用して、通知を受け取るアラートの種類を指定できます。たとえば、ハードウェア、構成制限、リソース制限、動的コンテンツ、PAN-OS&サブスクリプションなどです。

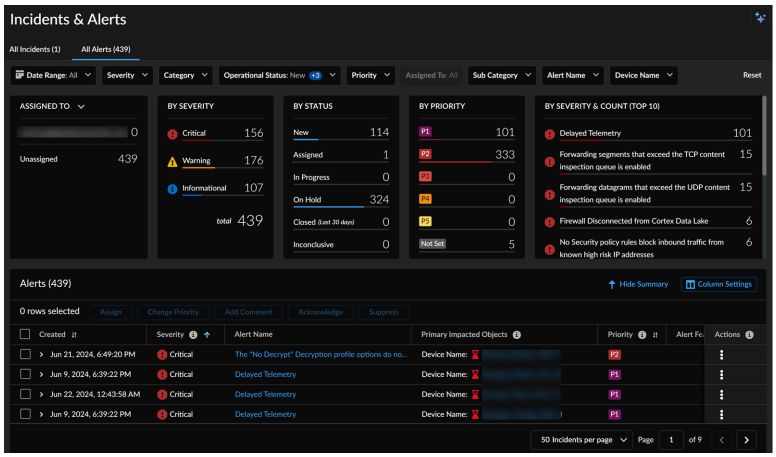
［**Incidents & Alerts (**インシデントとアラート**)]** > **[NGFW]** > **[All Alerts (**すべてのアラート**)**］から、デプロイメントに対して生成されたすべてのアラートを表示して管理できます。**[Notification Rules (**通知ルール**)]**では、イベントがアラートをトリガーしたときに通知を受けるタイミングと方法を指定する通知ルールを設定できます。

- NGFWアラートの管理
- アラートの詳細の表示
- 考えられる原因の表示
- 予測と異常検知
- Capacity Analyzerアラートの管理
- NGFW用のAIOpsのCPU使用率メトリック
- 通知ルールの作成
- ServiceNowとの統合

NGFWアラートの管理

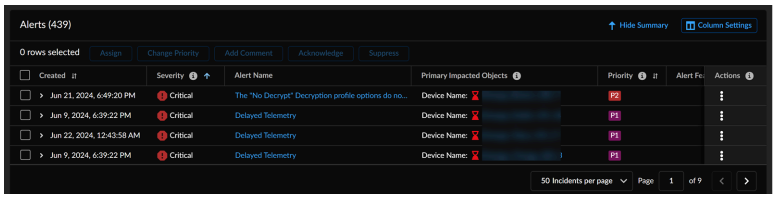
どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	以下のいずれかです: ❑ 又は ❑ 又は

[Incidents & Alerts (インシデントとアラート**)]** > **[NGFW]** > **[All Alerts (**すべてのアラート**)]**を選択すると、NGFWアラートを俯瞰できます。デバイスとデプロイメントの継続的な健全性を維持し、業務の中断を回避するために、アラート ページをご確認ください。重要な視覚的な要約とともに、アラートの詳細なリストに直接アクセスできます。**[Hide Summary (**サマリーを非表示にする**)]**では、ウィジェットを非表示にして、アラートを表形式でのみ表示することもできます。



[All Alerts (すべてのアラート**)]**の下に表示されているデータです。

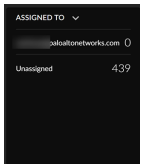
- アラート:すべてのアラートを表示します。

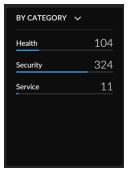


この表では、以下のタスクを実行できます。

- **[Hide Summary (**サマリーを非表示にする**)]**では、ウィジェットを非表示にして、アラートを表形式でのみ表示できます。
- アラートを展開すると、その説明と影響が表示されます。
- [Actions (アクション)]では、以下のアクションを実行できます。
  - ユーザー、お客様自身にアラートを割り当てるか、アラートの割り当てを解除します。
  - アラートの優先度を変更するか、「未設定」を選択して優先度を削除します。
  - **[}Yes (**はい**)]**を選択すると、アラートを承認したことになります 。
  - アラートをアクティブに解決する予定がない場合、抑制すると、アラートが「保留中」の動作ステータスに設定されます。
  - アラートにコメントを追加します 。
- アラートをクリックすると詳細が表示されます。
- ［**Column Settings (**カラムの設定**)**］を使用して、インシデントアラートの特定のカラムを表示または非表示にし、カラムのデフォルトの順序を並べ替えます。これらの変更は、今後のセッションでも継続されます。

- **ASSIGNED TO**（担当者）:解決のタスクを持つ個人またはエンティティ別のアラート数を表示します。上部には、現在ログインしているユーザーに割り当てられているアラートと、割り当てられていないアラートが表示されます。また、ドロップダウン リストでインシデントを選択して、カテゴリ別のアラート数を表示することもできます。





- 重大度と数**(**トップ**10):**重大度別に分類されたアラートを、各カテゴリのアラート数とともに表示します。重大アラートの優先順位は、最初に警告アラート、次に情報アラートの順になります。

- ステータスごと**:**アラートの総数をステータス別に表示します。
  - [New (新規)]は未割り当てのインシデントを示します。
  - [Assigned (割り当て済み)]は、ユーザーに割り当てられているインシデントを示します。
  - [In Progress (進行中)]は、インシデントの処理中であることを示します。
  - [On Hold (保留)]は、アラートまたはインシデントを積極的に解決する予定がないことを示します。
  - [Closed (クローズ済み)]は、過去30日間にクローズされたアラートを示します。
  - [Inconclusive (不確定)]は、これらのアラートに対する解決策がないことを示しています。

- 重要度別**:**[Critical (重大)]、[Warning (警告)]、および[Informational (情報)]に分類されたアラートの総数が表示されます。

- 優先順位ごと**:**アラートを優先度に従って表示します。P1が最も重大です。

アラートの詳細の表示

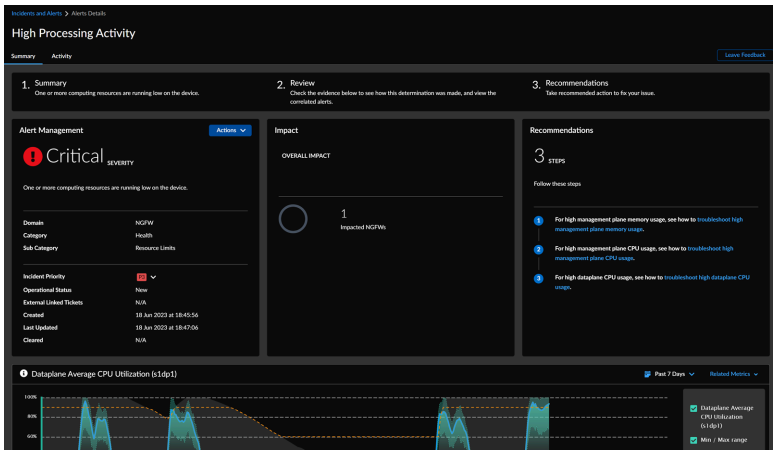
どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	以下のいずれかです: ❑ 又は ❑ 又は

[All Alerts (すべてのアラート)]からアラートを選択すると、アラートの詳細が記載されたページが開きます。**[Summary (概要)]**タブには、以下の詳細が表示されます。

1. アラートの概要と詳細。アラートの優先度を変更したり、ユーザーに割り当てることができます。
2. アラートによって引き起こされた影響、つまり影響を受けたNGFWの数。
3. 問題を修正するための改善推奨事項とリソース。

貢献イベントのチャートも確認できます。

[Activity (アクティビティ)]タブには、アラートに対して記録されたアクティビティが表示されます。



考えられる原因の表示

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	❑ または

高度なAI機能を使用して、NGFW用のAIOpsはアラートの考えられる原因を表示し、根本的な問題を修正するための推奨事項を提供します。この機能は、中断を軽減し、サイバーセキュリティ ソリューションの効果を最大化することで、最適なネットワーク パフォーマンスを保証します。

次に、考えられる原因解析をサポートするアラートを示します。

- 高い処理活動
- トラフィック レイテンシの増加 - パケット バッファ
- トラフィック遅延の増加 - オンチップのパケット記述子
- 許可された脅威
- トラフィック レイテンシ - パケット記述子 (オンチップ)
- リソースの不利な使用
- 非同期ピア - 設定
- 潜在的な資格情報の盗難の悪用
- プッシュのコミットに失敗しました

考えられる原因の解析は、Strata Logging Serviceログを使用し、アラートまたはインシデントの作成につながった考えられる原因に追加のメタデータを提供するように拡張されています。この機能拡張により、アラートの原因となりうるポリシー、アプリケーション、送信元ゾーン、URL、送信元IP、リージョンを特定できます。

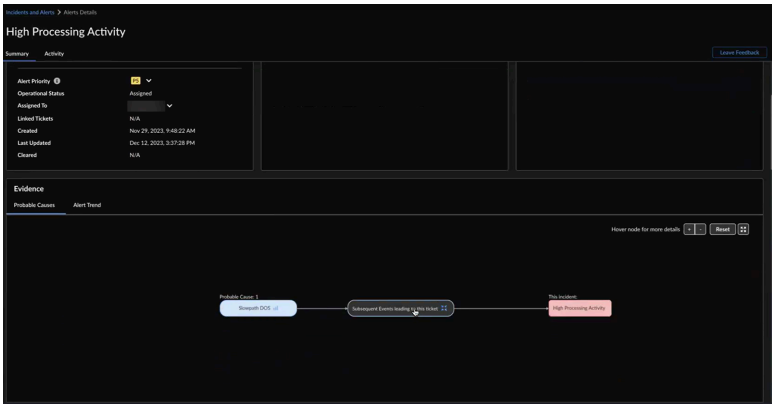
以下のシナリオの考えられる原因を表示できます。

- 高い処理活動(高い処理活動アラート):データプレーンのCPU使用率が高い場合、ファイアウォールの不安定さ、ファイアウォールのハングやスタック状態、パケットの損失やレイテンシの問題など、さまざまな問題につながる可能性があります。業務に悪影響を及ぼす可能性があります。データプレーンのCPU使用率が60%以上で、使用率が大幅に急上昇している場合、NGFW用のAIOpsは高い処理活動のアラートで考えられる原因を表示します。しかし、データプレーンのCPU使用率が変動なく長期間高水準で推移していると、原因が曖昧で容易に判断できないため、考えられる原因が表示されません。たとえば、データプレーンのCPU使用率が長期間一貫して70%である場合、NGFW用のAIOpsでは考えられる原因が表示されません。
- 単一または複数の貪欲セッションの検出と修復(高い処理活動アラート):ファイアウォールに対する貪欲なセッション攻撃とは、攻撃者が多数の接続を急速に作成し、ファイアウォールの内部リソースを悪用して、リソースの枯渇やサービス拒否（DoS）インシデントを引き起

こすことを指します。NGFW用のAIOpsは、これらの問題を検出し、考えられる原因を表示することができます。

- 接続損失セッション枯渇（高い処理活動アラート）:ファイアウォールは、トラフィックを受信すると、そのトラフィックのセッションを確立して状態を追跡し、必要なセキュリティ検査を実行します。各セッションは、メモリやCPUサイクルなどのシステム リソースを消費します。ファイアウォールが同時セッションの最大容量に達すると、セッションの枯渇につながります。この問題は、大量のトラフィック、セキュリティポリシーの設定ミス、不適切なセッション タイムアウト設定など、いくつかの原因で発生する可能性があります。NGFW用AIOpsは、高度なAI機能を活用して、ネットワーク デバイスのセッション枯渇の問題を事前に検出します。これにより、リソースの割り当ての最適化、ネットワーク パフォーマンスの向上、接続の問題の軽減を実現し、中断のないサービスの可用性を確保できます。
- 単一アプリケーションによる高いパケット バッファ使用率(トラフィック遅延の増加:パケット バッファ):NGFW用AIOpsは、1つのアプリケーションがパケット バッファを独占しているためにパケット バッファ使用率が高くなる原因として考えられるものを検出します。NGFW用AIOpsは、高度なAI機能を活用して、最適でないリソース割り当てをタイムリーに警告し、パフォーマンスの低下を防ぐことで、最適なネットワーク パフォーマンスを実現します。
- 単一アプリケーションによるパケット記述子の高いオンチップ使用率(トラフィック遅延の増加: オンチップのパケット記述子):NGFW用AIOpsは、オンチップ パケット記述子の使用率が高くなる原因として考えられるものを検出します。これにより、1つのアプリケーションがオンチップ パケット記述子を独占することによって発生するネットワークの輻輳を事前に特定して解決できます。
- 低速パス**DoS**攻撃の検出と修復の提案(高い処理活動アラート):NGFW用AIOpsは、AIを活用したテクノロジーで低速パスDoS攻撃を検出し、ネットワーク セキュリティと中断のないサービスの可用性を確保します。高いデータプレーン処理アクティビティのアラート、高いポリシー拒否アクティビティの根本原因解析、および因果関係分析に基づく改善提案を実行します。
- 高**URL**キャッシュ検索アクティビティの検出と修復(高い処理活動アラート):NGFW用AIOpsは、URLキャッシュの高い検索アクティビティを検出して対処し、処理効率を最適化し、システムの安定性を維持します。この機能は、URLキャッシュ検索アクティビティとDP CPU使用率を関連付け、高CPU使用率を特定し、飽和状態に近いシナリオを防ぐための改善提案を提供します。
- 高コンテンツ処理アクティビティの検出と修復(高い処理活動アラート):NGFW用AIOps機能は、高いコンテンツ処理アクティビティを検出します。この機能は、さまざまなコンテンツ処理段階とデータプレーンのCPU使用率の相関関係を分析し、CPU使用率の高い状態や飽和状態に近い状態のインスタンスを特定して、システムの安定性を向上させるための実行可能な改善案を提供します。
- 証明書が長すぎる**RCA**レポート(コミットプッシュ失敗アラート):NGFW用AIOpsはコミット失敗を検出し、特に証明書の長さがバッファ サイズを超えている場合に発生する可能性のあるコミット失敗の原因を概説します。

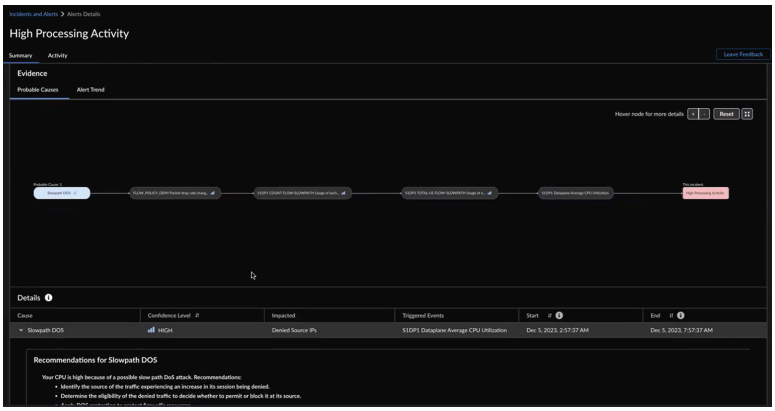
STEP 1 | **[Incidents & Alerts (インシデントとアラート)] > [Alerts (アラート)]**からアラートを選択すると、アラートに関する詳細が記載されたページが開きます。



フローチャートでは、次のように表されます。

- 高処理アクティビティ アラートをトリガーしたイベント
- トリガーされたイベントの考えられる原因

また、ノードにカーソルを合わせると、考えられる原因、信頼度、トリガーされたイベント、影響の期間などの詳細が表示されます。イベント ノードが3つ以上ある場合は、イベントをクリックして展開し、詳細を表示できます。



NGFW用AIOpsでは、同じ情報が表形式でも表示されます。表内の考えられる原因の上にカーソルを置くと、フロー チャート内のノードとパスが強調表示されます。また、フローチャート内の考えられる原因をクリックすると、その詳細を表形式で表示できます。

［**Confidence Level (信頼度)**］は、NGFWの特定のAIOpsが、高い処理活動のアラートの原因をどの程度特定しているかを示します。考えられる原因は信頼度の降順に並べたものです。「高い信頼度」で原因を確認することから始められます。

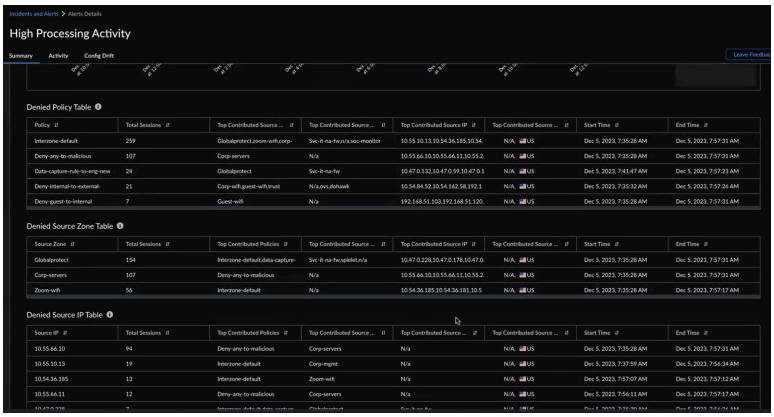
STEP 2 | 表内の考えられる原因を展開して、アラートをトリガーするために調査するグラフと影響を受けたメトリックを表示します。

STEP 3 | グラフ ツールを使用してグラフを調べます。

因果関係期間により、アラートの原因とトリガー イベントの因果関係を時系列で可視化できます。

グラフで影響の前後6時間、24時間、48時間を表示できます。

考えられる原因の解析は、SLSログを使用し、アラートまたはインシデントの作成につながった考えられる原因に追加のメタデータを提供するように拡張されています。この機能拡張により、アラートの原因となりうるポリシー、アプリケーション、送信元ゾーン、URL、送信元IP、リージョンを特定できます。たとえば、データプレーンのCPU使用率が高くなると、高い処理活動アラートがトリガーされます。この場合、考えられる原因解析を利用して、アラートの主な要因を特定し、推奨される改善策に従うことができます。



予測と異常検知

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	以下のいずれかです: ❑ 又は ❑ 又は

通常、AIOps for NGFWはデプロイメント内のメトリックに固定ルールを適用することで問題を検出します。たとえば、管理プレーンのCPU使用率が85%を超えた場合、メトリックは「Critical(極めて重大)」状態になります。

しかし、固定ルールでは見逃してしまうようなイベントを警告するために、AIOps for NGFWは機械学習を使用してデプロイメントを把握し、利用動向に合わせた追加のアラートやインシデントを提供することができます。

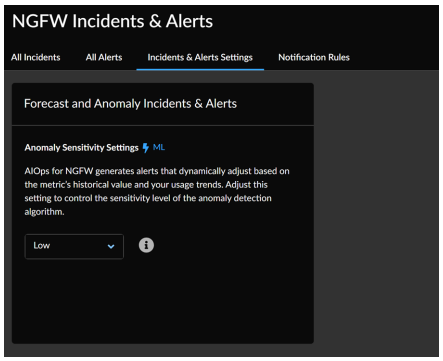
- 予測ベースのアラートは、デバイス メトリックがどのように変化するかを予測し、それに応じてアラートを発することで、問題を予測するのに役立ちます。
- 異常ベースのアラートは、デバイス メトリックのベースライン動作を確立し、そのメトリックが指定した異常感度設定を超えるとアラートを出します。

予測と異常検知のメリットは以下のとおりです。

- プロアクティブな管理:管理者は、潜在的な問題を予測し、早期に異常を特定することで、問題を予防するためのプロアクティブな対策を講じ、ダウンタイムを削減し、ネットワーク全体のパフォーマンスを向上させることができます。
- 強化されたセキュリティ:異常なパターンや行動を検出することで、セキュリティの脅威や脆弱性を特定でき、タイムリーな介入と軽減が可能になります。
- 最適化されたリソース:予測は、リソース計画と割り当ての改善に役立ち、ネットワーク インフラが将来の要求に適切に対応できるようになります。

[Incidents & Alerts (インシデントとアラート**)]** > **[Incident & Alert Settings (**インシデントとアラート設定**)]** > **[Forecast and Anomaly Incidents & Alerts (**予測、異常インシデント、アラート**)]**に移動します。

AIOps for NGFWは、メトリックの履歴値と利用傾向に基づいて動的に調整するアラートとインシデントを生成します。正規性バンドからの乖離は、潜在的な問題を示す場合があります。この設定を調整して、異常検知アルゴリズムの感度レベルを制御できます。



Capacity Analyzerアラートの管理

どこで使用できますか?	何が必要ですか?
•	☐ または

Capacity Analyzerは、機械学習モデルを使用して、リソース消費が最大容量に近づくことを予測し、アラートを発します。Capacity Analyzerのアラートは、潜在的な容量ボトルネックを特定するために前もって生成されます。

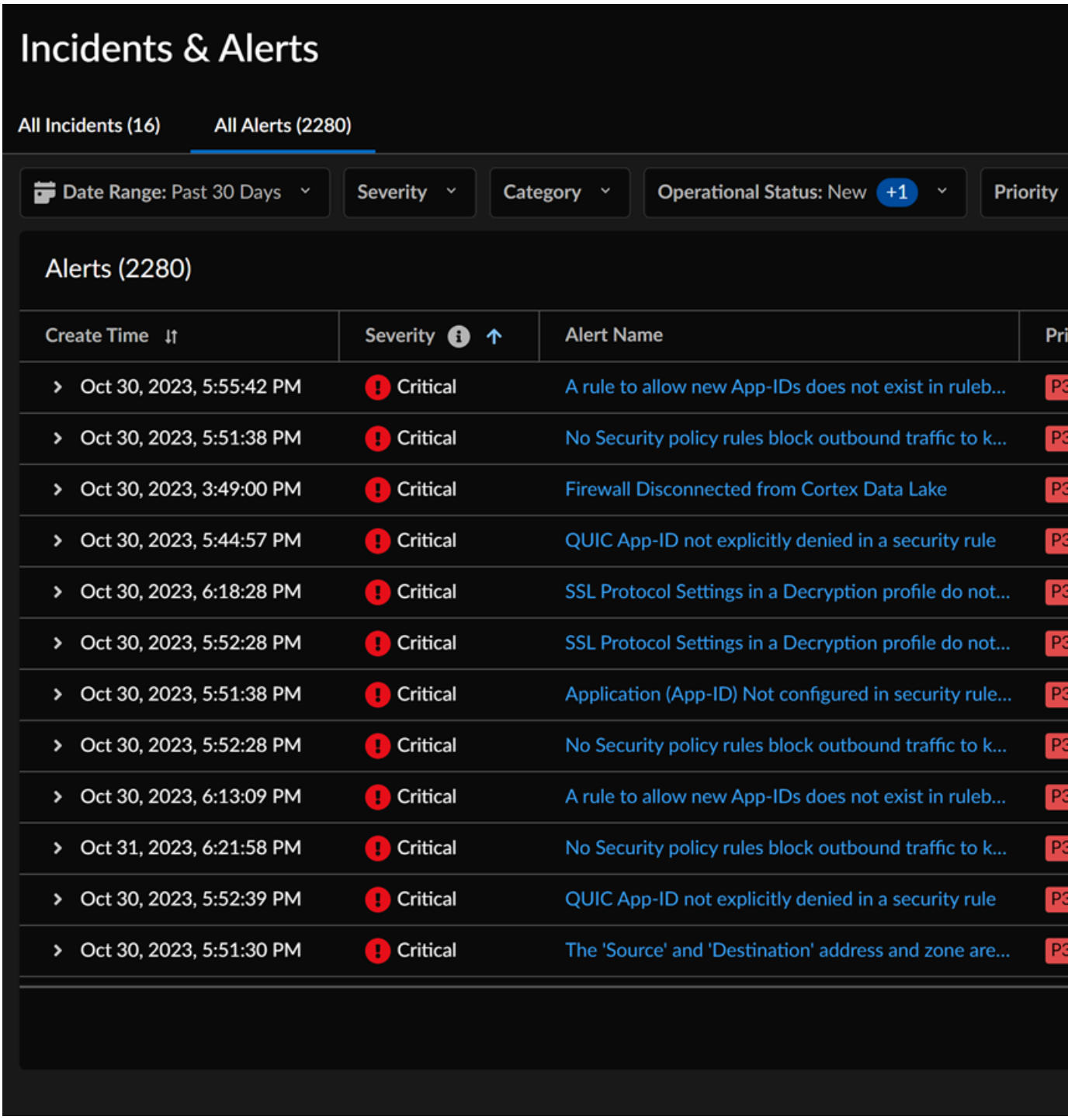
Capacity Analyzerアラートの通知をトリガーする 通知ルールを作成する こともできます。

STEP 1 | **[Incidents & Alerts (インシデントとアラート)]>「NGFW」>[All Alerts (すべてのアラート)]** に移動し、**[List View (リスト表示)]**をクリックします。

STEP 2 | **[Alert Name (アラート名)]**の下で、**approaching max alerts**を検索します。

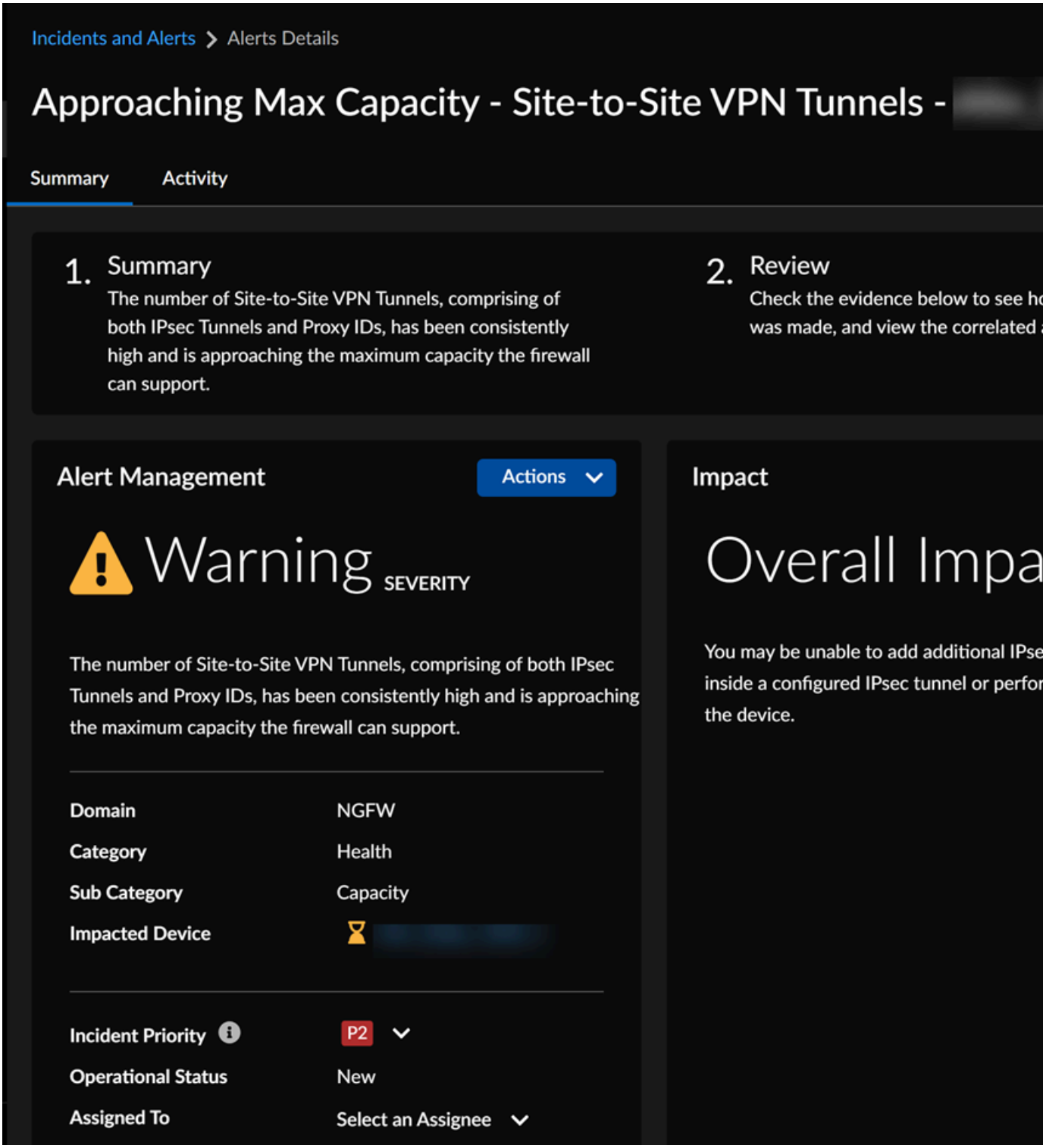
Capacity Analyzer機能に対して発生するアラートの名前は以下のとおりです。

最大容量に近づいています - <*Metric-Name*>。



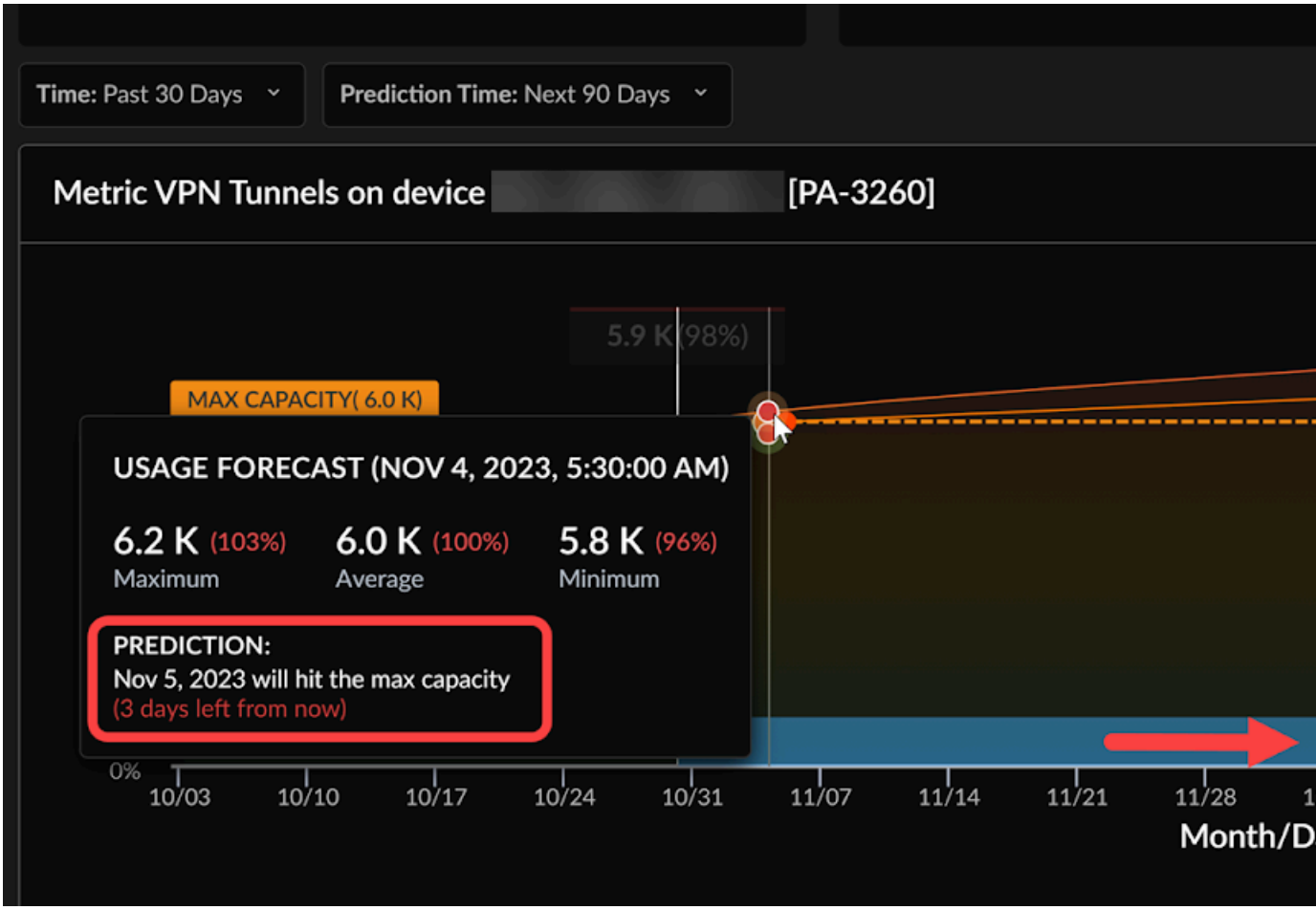
STEP 3 | アラートの1つを選択すると、以下の内容を含む詳細が表示されます。

- アラートの概要と詳細。
- アラートによって発生した影響。
- 問題を解決するための推奨処置。

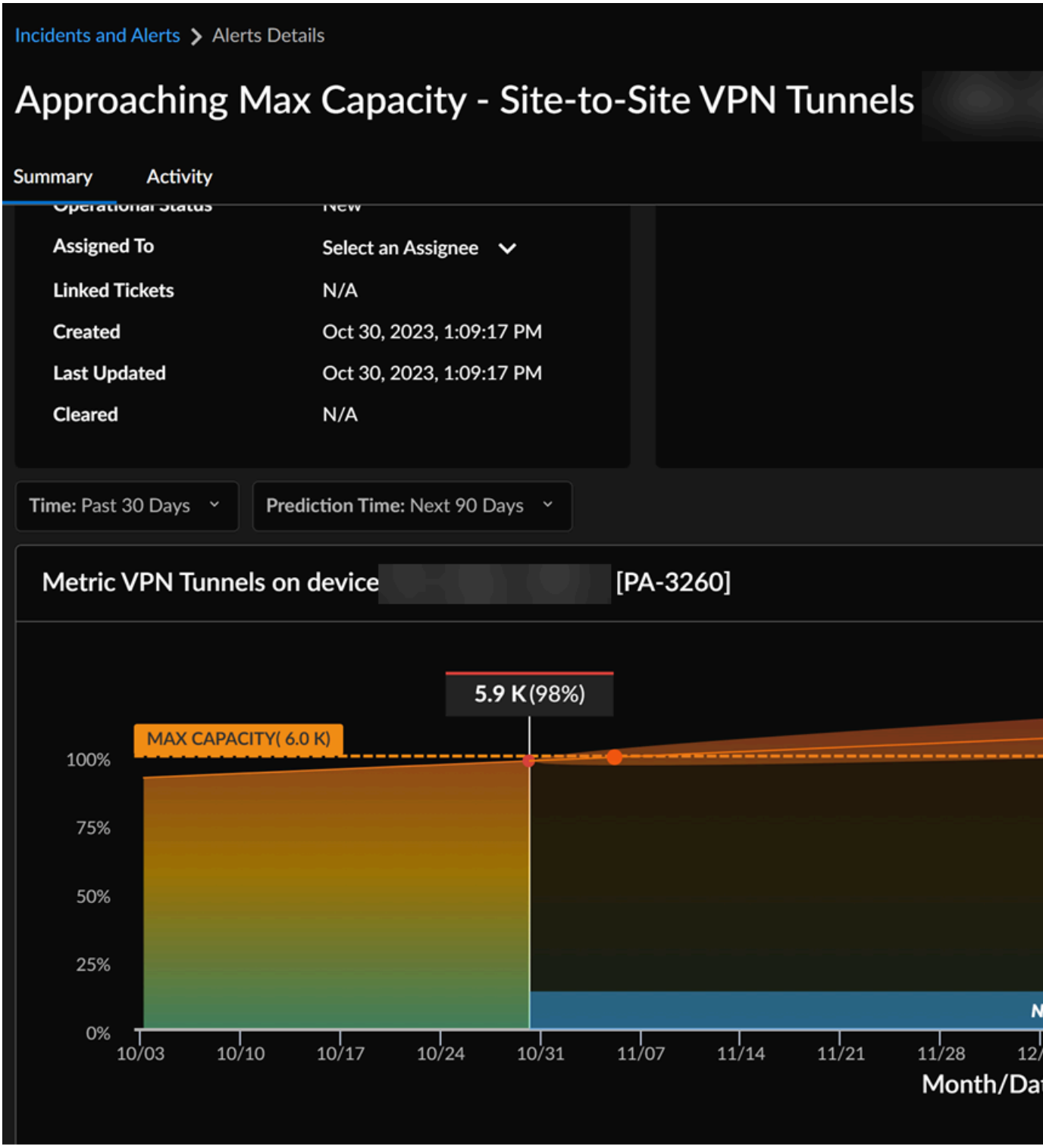


アラートの詳細では、メトリックの傾向を示すグラフも表示できます。Strata Cloud Managerは、メトリックが最大容量に達する日付を予測します。グラフの上にカーソルを置くと、任意の時点のメトリック容量を確認できます。今後30日間または90日間の**[Prediction Time (**予想時刻**)]**を選択できます。

この例では、デバイスのVPNトンネル メトリックが**2023**年**11**月**5**日に最大容量に達することがわかります。



STEP 4 | **[Alerts (アラート)]** ページから、 **Capacity Analyzer**ページに移動して、Capacity Analyzerヒートマップを表示できます。



Capacity Analyzer ヒートマップを活用して容量アラートを確認する方法については、「メトリック容量の分析」を参照してください。

NGFW用のAIOpsのCPU使用率メトリック

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	以下のいずれかです: ❑ 又は ❑ 又は

CPU使用率は、以下のメトリックを使用してNGFW用のAIOpsで追跡されます。

- **mp_system_resources.mp_cpu**:合計CPU使用率を示します。
- **mp_system_resources_daemon.cpu_usage_sum**:管理プレーンCPU(MP-CPU)で実行されている管理プレーン タスクによるCPU使用率を示します。このメトリックは、SNMPのCPU使用率に相当します。
- **mp_system_resources_daemon.pan_task_cpu_usage**:データ プレーンのような操作を実行するMP-CPUで実行されているPANタスクによるCPU使用率を示します。このデータは、SNMPおよび**mp_system_resources_daemon.pan_task_cpu_usage**メトリックの一部ではありません。

合計CPU使用率は次のように計算されます。

mp_system_resources.mp_cpu = mp_system_resources_daemon.cpu_usage_sum + mp_system_resources_daemon.pan_task_cpu_usage

通知ルールの作成

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	以下のいずれかです: ❑ 又は ❑ 又は

Strata Cloud Managerを既存の運用に統合するには、プロアクティブなアラートのセットアップが必要です。これにより、深刻な複雑さにエスカレートする前に、潜在的な問題を検出し、管理できます。これらのアラートは、一般的に使用されるP1やP2など、運用チームのケース管理プロトコルに合わせて調整できます。

たとえば、最も重大な問題を示す重要なアラートが瞬時にセキュリティチームにエスカレーションされ、すぐに対処できるアラートシステムをセットアップするとします。一方、緊急度は低いものの、それでも重要な警告アラートは、毎日確認できるようにアレンジできます。このような配置により、円滑な業務運営を維持しながら、効率的なインシデント管理を実現します。

チームに基づいてアラートをルーティングする方法もあります。特定のカテゴリのアラート、さらには特定のアラートを、そのアラートを処理するのに最適な設備を備えたさまざまなチームにルーティングできます。通知をトリガーするアラート、通知の受信方法、受信頻度など、通知の環境設定を定義し、通知ルールを作成できます。

通知ルールの作成方法を紹介する動画です。

STEP 1 | **[Incidents & Alerts (インシデントとアラート)]** > **[Incident & Alert Settings (インシデントとアラートの設定)]** > **[Notification Rules (通知ルール)]** > **[+ Add Notification Rule (通知ルールを追加)]**を選択します。

STEP 2 | `[Name (名前)]`と`[Description (説明)]`を入力します。

STEP 3 | **[Add New Condition (新しい条件を追加)]**をクリックして、通知をトリガーする`[Rule Conditions (規則条件)]`を指定します。

たとえば、ハードウェアアラートの通知を作成するには、**[subCategory (サブカテゴリ)]**、**[Equals (イコール)]**、**[Hardware (ハードウェア)]**を選択します。

STEP 4 | 通知の[Notification Type and Recipients (通知タイプと受信者)]を選択します。

1. **[Email (電子メール)]**を選択する場合は、電子メール通知を受け取るユーザーのグループである電子メールグループを選択するか、または**[Create a New Email Group (新しい電子メールグループの作成)]**を選択します。
   1. 新しい電子メールグループを作成する場合は、「電子メールグループ名」を入力し、グループに追加する電子メールアドレスの入力を開始します。各メールアドレスの入力が終わったらリターンキーを押します。
   2. **Next**（次へ）を選択します。
   3. これらの通知を送信する頻度を選択します。
   - 直ちに
   - グループ化して4時間ごとに送信
   - グループ化して1日1回送信
2. **ServiceNow**を選択する場合は、ServiceNow URL、クライアント認証情報、ServiceNow認証情報、ServiceNow APIバージョンを入力します。
   1. 接続をテストして、連動が機能していることを確認します。
   2. **Next**（次へ）を選択します。

STEP 5 | ルールを保存します。

ServiceNowとの統合

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	❑ または

AIOps for NGFW通知ルールでServiceNowとの連携を設定する場合、以下のものが必要です。

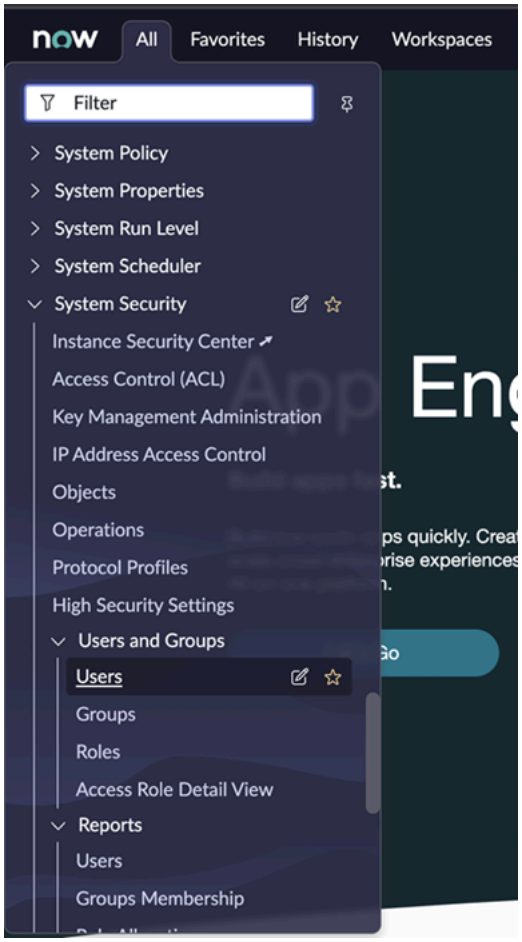
- ServiceNowインスタンス（管理アクセスあり）
- ServiceNowのユーザー名とパスワードとWebアクセス、インシデントの作成や各種テーブルへのクエリを行う特定のロール
- AIOpsがServiceNowインスタンスにアクセスすることを承認するために、アプリケーションレジストリの下に作成されたクライアントIDとパスワード
- ServiceNowインスタンスのURL

ServiceNowインスタンスには、アラートを送信するAIOpsのインシデントテーブルと、これらのアラートを特定の担当者に上げることができるように、**[Assignees (割当先)]**を持つ**[Assignment Groups (割当グループ)]**も設定する必要があります。

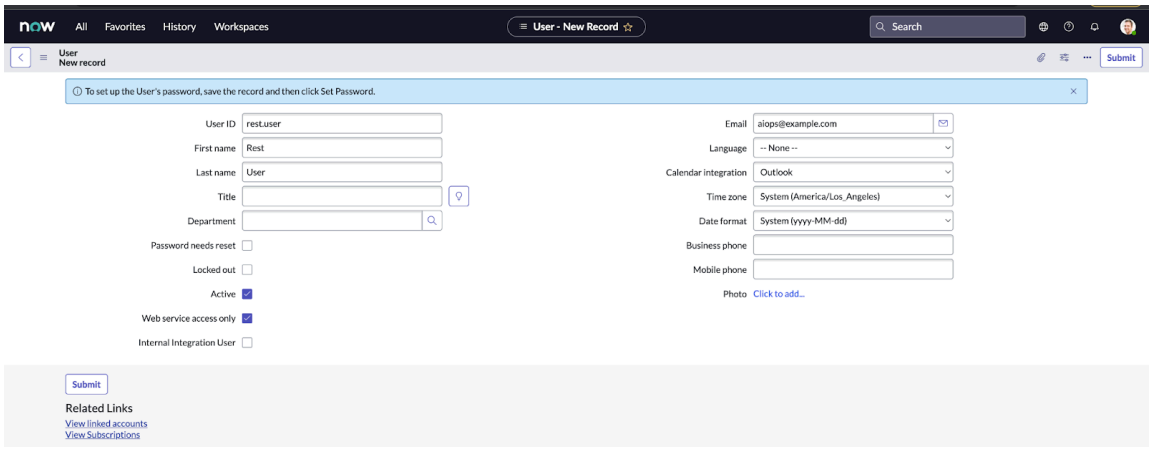
STEP 1 | ServiceNowの残りのユーザーの作成。

統合に必要な各種テーブル（インシデント、割当グループ、割当先）を読み書きする特定のロールを持つ新しいServiceNowユーザーを作成します。

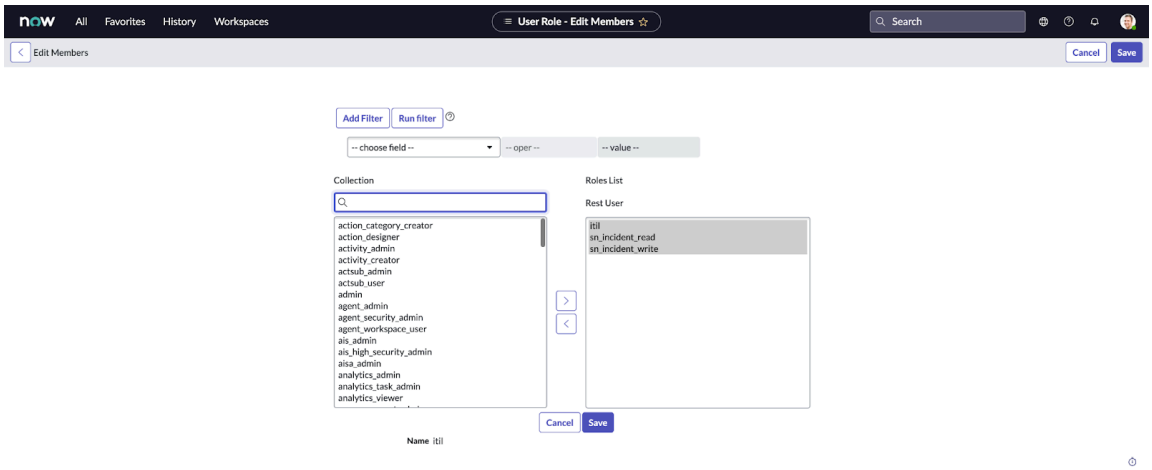
1. ServiceNowでユーザーを作成するには、**[Security (セキュリティ)]** > ［**Users and Groups (ユーザーとグループ)]**の［**User (ユーザー)**］に移動します。



2. **[Web service access only (Web**サービスアクセスのみ**)]**チェック ボックスをオンにして、変更を送信します。

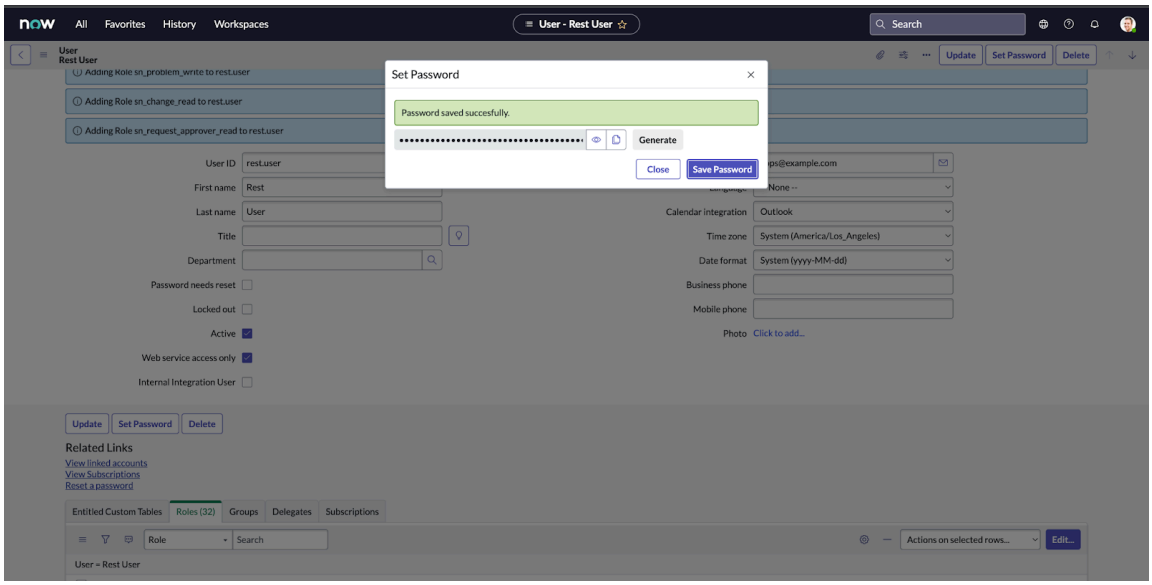


3. 新しく作成したユーザーを検索します。ページ下部の表で**[Roles (ロール)]**タブを選択し、**[Edit (編集)]**をクリックします。**itil**、**sn_incident_read**、**sn_incident_write**の3つのロールに対する権限をユーザーに付与する必要があります。変更を保存します。



4. [User (ユーザー)]ページで**[Set Pasword (パスワードの設定)]**をクリックします。ポップアップウィンドウで、**[Generate (生成)]**と**[Save Password (パスワードを保存)]**をクリッ

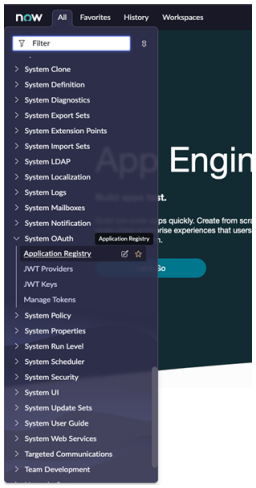
クします。パスワードは、ユーザーIDとともに安全な場所にコピーしてください。この情報は、AIOps for NGFWの**ServiceNow**ユーザー資格情報の入力に使用されます。



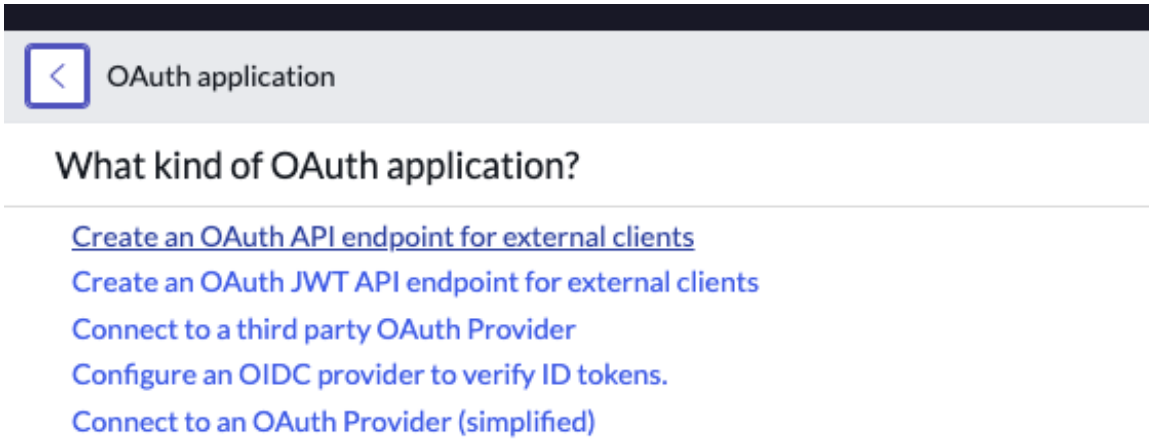
STEP 2 | Web OAuthクライアントを作成します。

AIOps for NGFWがServiceNowインスタンスに認証するには、OAuthクライアントが必要です。

1. **[System OAuth (**システム**OAuth)] > [Application Registry (**アプリケーション レジストリ**)]**の順に移動します。

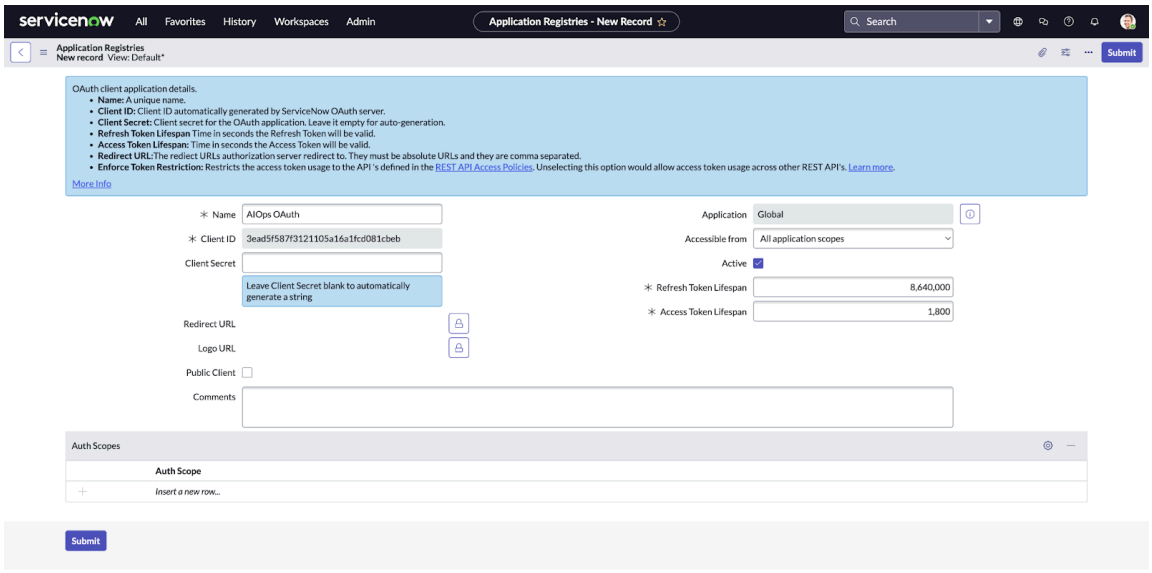


2. 新規エントリーを作成し、以下のページで**[Create an OAuth API endpoint for external clients (**外部クライアント用の**OAuth API**エンドポイントを作成する**)]**を選択します。



3. OAuthの名前を追加し、クライアントシークレットを作成します。自動生成秘密が必要な場合は、**[Client Secret (**クライアント シークレット**)]**を空白にすることもできます。**[Submit (**送信**)]**をクリックしてからアプリケーション レジストリ エントリに戻り、**[Client ID (**クライアント**ID)]**と**[Client Secret (**クライアント シークレット**)]**の両方を

安全な場所に保存します。この情報は、AIOps for NGFWのクライアント認証フォームで使用されます。



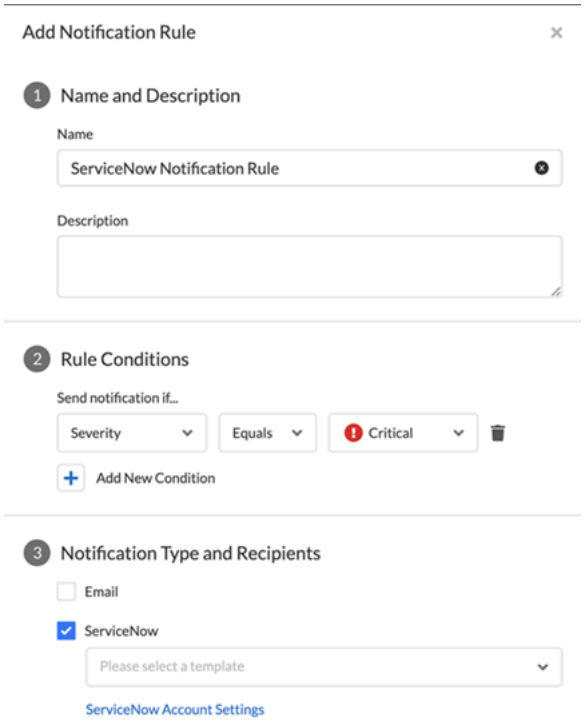
STEP 3 | ServiceNowのアカウント設定情報をAIOps for NGFWに追加します。

ServiceNow とAIOps for NGFWの統合を完了するAIOps for NGFWに、これまでの手順の情報を追加します。

以下の設定が必要です。

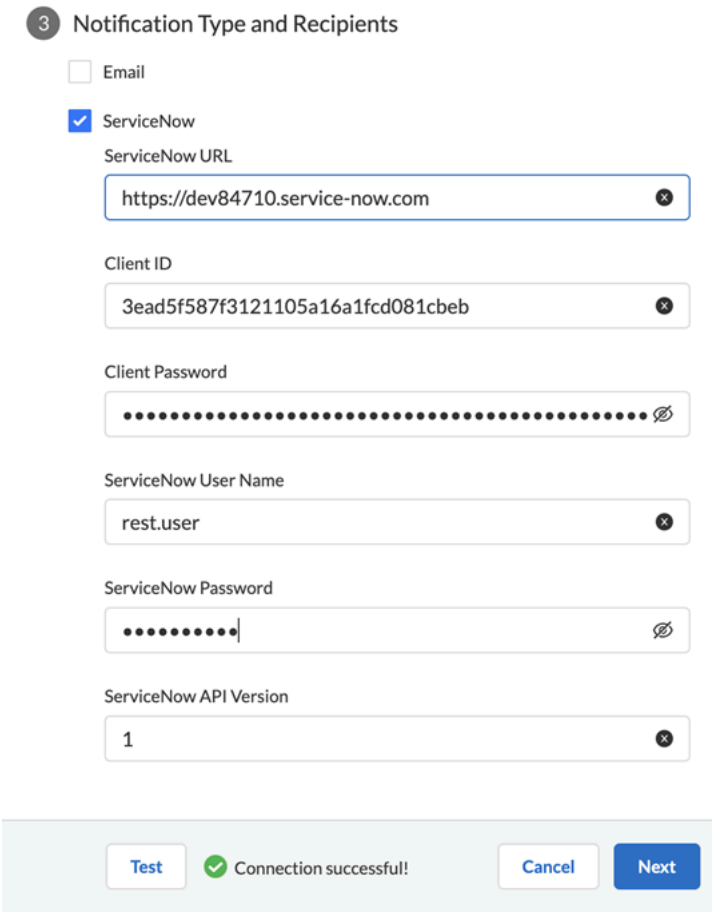
- **ServiceNow**インスタンス**URL**
- **ServiceNow**のユーザーとパスワード（手順1より）
- 手順2のクライアント**ID**とクライアント シークレット

1. AIOps for NGFWで、**[Alert Notification Rules (**アラート通知ルール**)]**に移動し、**[Add Notification Rule (**通知ルールを追加**)]**をクリックします。

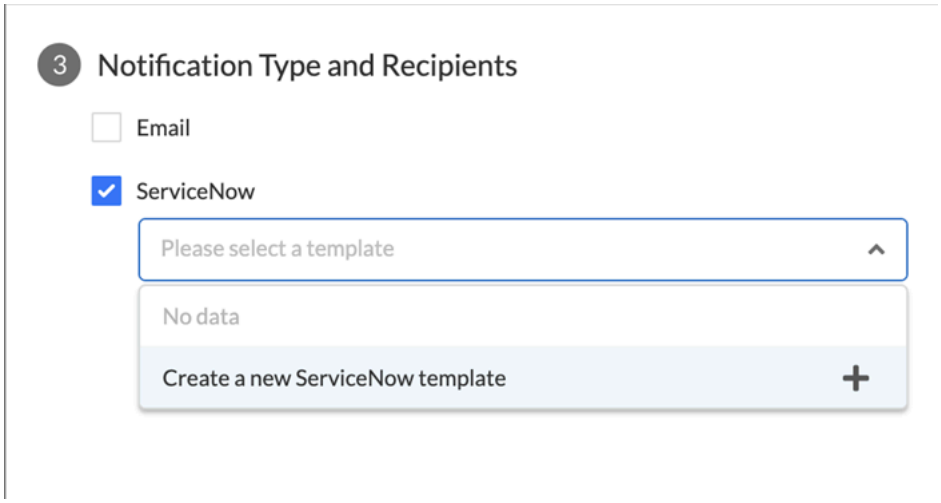


2. **[Rule Name (**ルール名**)]**や**[Alert Condition (**アラート条件**)]**などのフィールドに入力し、**[Notification Type and Recipients (**通知の種類と受信者**)]**の下にある**[ServiceNow]**のチェック ボックスをクリックします。
3. サイドバー下部の**[ServiceNow Account Settings (ServiceNow**アカウント設定**)]**をクリックします。以下のフォームに以前保存した情報を入力します。残りのユーザーをセットアップしたステップ1の**[ServiceNow User (ServiceNow**ユーザー**)]**と**[ServiceNow Password (ServiceNow**パスワード**)]**。アプリケーション登録をセットアップしたステップ2のクライアント**ID**とクライアント シークレット。バージョンはそのままにします。［**Test (**テスト**)**］をクリックして設定を保存し、ServiceNowインスタンスにテ

ストインシデントを投稿します。これが成功しなければ、先に進めません。**Next**（次へ）をクリックします。



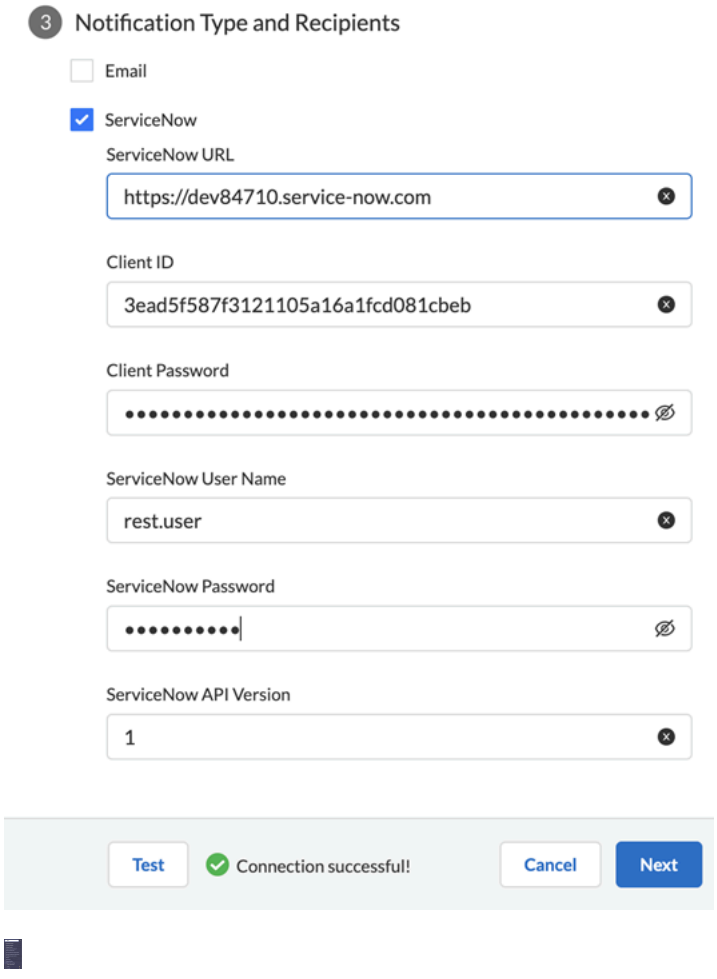
4. **[Please select a template (**テンプレートを選択してください**)]**ドロップダウンを展開し、**[Create a new ServiceNow Template (**新しい**ServiceNow**テンプレートを作成する**)]**をクリックします。



5. **[ServiceNow Template Name (ServiceNowテンプレート名)]**を入力し、**[Assignment Group (割り当てグループ)]**ドロップダウンリストからグループを選択します。［**Assignee (割当先)**］ドロップダウン リストから割当て先を選択します。これらのドロップダウン リストは、ServiceNowインスタンスから以下のテーブルを呼び出すことで読み込まれることに注意してください。

   - **[System Security (システム セキュリティ)] > [Users and Groups (ユーザーとグループ)] >[Users (ユーザー)]**
   - **[System Security (システム セキュリティ)] > [Users and Groups (ユーザーとグループ)] >[Groups (グループ)]**

   グループが定義されていない場合、**[Assignment Group (割り当てグループ)]**ドロップダウン リストにはデータが表示されません。特定のグループに割り当てられているユーザーがいない場合、**[Assignees (割当先)]**ドロップダウン リストにはデータが表示されません。**[Next (次へ)]**をクリックし、**[Save Rule (ルールを保存)]**をクリックします。



AIOps for NGFWアラート リファレンス

AIOps for NGFWアラート リファレンスへようこそ。ヘルス アラートは、プラットフォームの健全性とパフォーマンスをリアルタイムでアクティブに監視します。このアプローチは、問題の特定、潜在的な問題の予測、およびデバイスが最適に機能するための改善措置の実施に役立ちます。以下にいくつかの重要な側面を示します。

- 監視メトリック:CPU使用率、メモリ使用率、ディスク容量、ネットワーク スループット、その他の関連するパフォーマンス指標など、NGFWからのさまざまなメトリックを継続的に監視します。この常時モニタリングにより、通常のパフォーマンスからの逸脱が迅速に特定されます。
- 異常検知:メトリックの履歴値と利用傾向に基づいて動的に調整するアラートを生成します。履歴データを活用することで、潜在的な問題を示す可能性のある異常を検出できるため、プロアクティブな管理が可能になります。
- 予測解析:過去のデータやパターンを分析することで、特定のしきい値を超えたり、特定のイベントが発生したりすることを予測できます。これにより、潜在的な問題がエスカレートする前に予測することができます。

以下のページでは、AIOps for NGFWで発生する可能性のあるアラートを示します。

- プレミアム ヘルス アラート:Strata Cloud Managerで発生する可能性のあるプレミアム アラートのうち、プラットフォームの健全性に関連するものを表示します。
- フリー ヘルス アラート:AIOps for NGFWで発生する可能性のある、プラットフォームの健全性に関連するフリー アラートを表示します。
- サービス アラート:AIOps for NGFWで発生する可能性のある、接続されているサービスに関連するアラートを表示します。
- 機械学習を活用して発生するアラート:Strata Cloud Managerが機械学習を活用して発生する可能性のあるアラートを表示します。

AIOps for NGFWで発生する可能性のあるセキュリティ ポスチャ チェックについては、**[Manage (管理)]** > ［**Security Posture (セキュリティ ポスチャ)**］ > ［**Settings (設定)**］> ［**Security Checks (セキュリティ チェック)**］テーブルに移動してチェックを表示します。

プレミアム ヘルス アラート

以下の表に、Strata Cloud Managerで発生する可能性のある、プラットフォームの健全性に関連するプレミアム アラートを表示します。

AIOps for NGFWプレミアム ライセンスは、Strata Cloud Managerがこれらのアラートを発生させるために必要です。

アラート	詳説
ACCクエリの失敗 (プレミアム アラート)	このアラートは、Application Command Center (アプリケーション コマンド センター - ACC)クエリが失敗したかどうかを検出します。 クラス:ヘルス カテゴリ:とレポート作成 アプリ内サポート チケット:いいえ
逆暗号化トラフィックのリソース使用率 (プレミアム アラート)	暗号化されたトラフィック リソースが不足しています。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:いいえ
リソースの不利な使用 (プレミアム アラート)	ファイアウォールには、1 秒あたりの接続数 (CPS)、スループット、またはセッション数の異常な値があります。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:いいえ
最大容量に近づいています-ARPテーブル (プレミアム アラート)	データ予測解析によると、ARPテーブルのエントリはまもなくファイアウォールの最大容量に達する見込みです。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-アドレス グループ (プレミアム アラート)	アドレス グループ オブジェクトの数は一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量

アラート	詳説
	アプリ内サポート チケット:いいえ
最大容量に近づいています-アドレス オブジェクト (プレミアム アラート)	アドレス オブジェクトの数が一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています - データプレーンCPU (プレミアム アラート)	データ プレーン(DP)のCPU使用率が長期にわたって一貫して高く、デバイスがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています - 復号化の使用量 (プレミアム アラート)	データ予測解析によると、SSL復号化セッションはまもなくファイアウォールの最大容量に達する見込みです。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています - FQDNアドレス (プレミアム アラート)	FQDNアドレス オブジェクトの数は一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています - GlobalProtect トンネル(クライアントレス) (プレミアム アラート)	クライアントレスのGlobalProtect VPNトンネルの数は、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています - IKEピア (プレミアム アラート)	IKEピアの数が一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量

アラート	詳説
	アプリ内サポート チケット:いいえ
最大容量に近づいています - 管理プレーンCPU (プレミアム アラート)	管理プレーン(MP)のCPU 使用率が一貫して高く、デバイスがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています - 管理プレーン メモリ (プレミアム アラート)	管理プレーン(MP)のメモリ使用量が一貫して高く、デバイスがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています - NAT ポリシー (プレミアム アラート)	NATポリシー ルールの数が長期にわたって一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています - セキュリティ ポリシー (プレミアム アラート)	セキュリティ ポリシー ルールの数が一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています - サービス グループ (プレミアム アラート)	サービス グループ オブジェクトの数は一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています - サービス オブジェクト (プレミアム アラート)	サービス オブジェクトの数が一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量

アラート	詳説
	アプリ内サポート チケット:いいえ
最大容量に近づいています - セッション テーブル使用率 (プレミアム アラート)	セッションテーブルの使用率(%)が長期にわたって一貫して高く、ファイアウォールまたはVMライセンスがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています - サイト間VPNトンネル (プレミアム アラート)	IPSecトンネルとプロキシIDの両方で構成されるサイト間VPNトンネルの数が一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています - EDL内のURLまたはIP (プレミアム アラート)	このファイアウォールのポリシーで使用される設定済みEDL内のURL、IP、またはドメインの数が、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:いいえ
最大容量に近づいています - 仮想システム (プレミアム アラート)	データ予測解析によると、仮想システムの設定は、ファイアウォールのライセンスでサポートされる最大容量に達する見込みです。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大設定制限に近づいています (プレミアム アラート)	ルール、グループ、セキュリティ プロファイルなどのファイアウォール オブジェクトがデバイスの制限に近づいています。 クラス:ヘルス カテゴリ:設定制限 アプリ内サポート チケット:いいえ
証明書の有効期限	ファイアウォール上の 1 つ以上の証明書が失効しているか、まもなく期限切れになります。

アラート	詳説
(プレミアム アラート)	クラス:ヘルス カテゴリ:証明書 アプリ内サポート チケット:いいえ
コミット プッシュの失敗 (プレミアム アラート)	設定のプッシュに失敗しました。 クラス:ヘルス カテゴリ:設定 アプリ内サポート チケット:いいえ
構成メモリ使用量が最大制限に近づいています (プレミアム アラート)	ファイアウォールの設定が最大メモリ使用量の制限に近づいています。コミット中、ファイアウォールの合計設定メモリは、現在の「使用中」の設定と新しい「使用予定」の設定の2つのコピーを収容する必要があります。設定ごとに割り当てられたメモリが50%を超えると、ファイアウォールが容量に達し、コミットが失敗します。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:いいえ
DPパケット ドロップ (プレミアム アラート)	アラートは、さまざまな理由で異常なパケット ドロップを検出します クラス:ヘルス カテゴリ:パフォーマンス アプリ内サポート チケット:いいえ
HAリンクのステータス (プレミアム アラート)	ファイアウォールに接続されているリンクの正常性。ファイアウォールは、さまざまなサービスのためにさまざまなシステムに接続されています。このアラートは、これらの接続の正常性を提供します。 クラス:ヘルス カテゴリ:高可用性 アプリ内サポート チケット:いいえ
高いログ取り込みレート (プレミアム アラート)	ログ コレクタが、サポートされている最大取り込みレートに近づいています。 クラス:ヘルス カテゴリ:ロギング

アラート	詳説
	アプリ内サポート チケット:いいえ
高いログのクエリ アクティビティ (プレミアム アラート)	ログ コレクタは、クエリ ジョブまたはレポートの容量に近づいています。 クラス:ヘルス カテゴリ:ロギング アプリ内サポート チケット:いいえ
トラフィック レイテンシの増加 - パケット バッファ (プレミアム アラート)	デバイスのパケット バッファ リソースが不足しています。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:あり
トラフィック レイテンシの増加 - パケット記述子 (プレミアム アラート)	デバイスのパケット記述子リソースが不足しています。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:あり
トラフィック遅延の増加 - 不明なTCPまたはUDP (プレミアム アラート)	ファイアウォールは、アプリケーションがunknown-tcpまたはunknown-udpに分類される大量のトラフィックを受信しました。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:いいえ
ログ転送先への接続が失われました (プレミアム アラート)	デバイスがログの転送先に接続できません。 クラス:ヘルス カテゴリ:ロギング アプリ内サポート チケット:いいえ
ログの最小保持期間を超えました (プレミアム アラート)	ログ コレクタには、定義された最小保持期間よりも古いログが含まれています。 クラス:ヘルス カテゴリ:ロギング アプリ内サポート チケット:いいえ

アラート	詳説
NAT 割り当ての失敗 (プレミアム アラート)	少なくとも 1 つの NAT ルールが、変換に十分なリソースを割り当てることができません。 クラス:ヘルス カテゴリ:NATプール リソース アプリ内サポート チケット:あり
NAT プールの使用 (プレミアム アラート)	1 つ以上の NAT ルールでリソース使用率が高くなっています。 クラス:ヘルス カテゴリ:NATプール リソース アプリ内サポート チケット:いいえ
NGFW SD-WAN アプリケーションパフォーマンスアラート (プレミアム アラート)	リンク パフォーマンスの低下の影響を受けるアプリケーションのリストを示します。 クラス:ヘルス カテゴリ:SD-WAN パフォーマンス アプリ内サポート チケット:いいえ
NGFW SD-WAN リンクパフォーマンスアラート (プレミアム アラート)	アプリやサービス、リンクのパフォーマンス低下の原因を示します。 クラス:ヘルス カテゴリ:SD-WAN パフォーマンス アプリ内サポート チケット:いいえ
デフォルト以外のログレベル (プレミアム アラート)	このアラートは、サービスのログ レベルがデフォルト設定に設定されていない場合にトリガーされます。このアラートにより、サービスは指定されたログ設定を一貫して維持します。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:いいえ
PAN-OS統合User-IDエージェント監視対象サーバーが切断されました (プレミアム アラート)	このアラートは、PAN-OS統合User-IDエージェント(エージェントレスUser-ID)によって監視されているサーバーがファイアウォールとの接続を失ったときにトリガーされます。この監視対象サーバーは、ユーザーIDをネットワーク アクティビティにマッピングするための重要なコンポーネントです。 クラス:ヘルス カテゴリ:

アラート	詳説
	アプリ内サポート チケット:いいえ
ポリシー設定のメモリ使用量が最大制限に近づいています (プレミアム アラート)	このアラートは、ポリシー構成のメモリ使用量が重大なしきい値を超えたかどうかを検出します。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:いいえ
トラフィック レイテンシ - パケット記述子 (オンチップ) (プレミアム アラート)	デバイスのパケット記述子 (オンチップ) リソースが不足しています。 クラス:ヘルス カテゴリ:フラッド/DoS アプリ内サポート チケット:いいえ
トンネルダウン (プレミアム アラート)	1 つ以上の Site-to-Site VPN トンネルがダウンしています。 クラス:ヘルス カテゴリ:サイト間VPN アプリ内サポート チケット:あり
ゾーン保護 プロファイル - フラッド検知 (プレミアム アラート)	ゾーンで確立された接続または着信パケット レートが過剰または異常です。 クラス:ヘルス カテゴリ:フラッド/DoS アプリ内サポート チケット:あり
ゾーン保護プロファイル - しきい値の推奨 (プレミアム アラート)	ゾーンにゾーン保護プロファイルがないか、ゾーン保護プロファイルのしきい値を調整する必要があります。 クラス:ヘルス カテゴリ:フラッド/DoS アプリ内サポート チケット:いいえ

フリー ヘルス アラート

以下の表に、AIOps for NGFWで発生する可能性のある、プラットフォームの健全性に関連するフリー アラートを表示します。

AIOps for NGFWがこれらの警告を発するのにプレミアム ライセンスは必要ありません。

アラート	詳説
カード電源障害 (フリー アラート)	カード障害が検出されました。カードまたはシャーシ内のカードの取り付けに問題がある可能性があります。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ
設定サイズがデバイス容量の制限に達しました (フリー アラート)	このデバイスの設定サイズが容量の制限に達しました。 クラス:ヘルス カテゴリ:設定 アプリ内サポート チケット:いいえ
システム ドライブの劣化 (フリー アラート)	属性値を監視することにより、劣化したシステム ドライブが特定されました。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ
遅延テレメトリ (フリー アラート)	分析エンジンには、このNGFW/Panoramaからの新しいテレメトリはありません。 クラス:ヘルス カテゴリ:テレメトリ アプリ内サポート チケット:あり
FE100障害 (フリー アラート)	ファイアウォールのFE100チップでキャリブレーション エラーが検出されました。この問題は通常、ハードウェア障害を示します。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ

アラート	詳説
ファンの問題 (フリー アラート)	ファンまたはファン トレーにより、デバイスでアラームがトリガーされました。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ
致命的なマシン チェックの失敗 (フリー アラート)	致命的なマシン チェック エラーが検出されました。この問題は通常、CPUのハードウェア障害を示しています。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ
ファイアウォールがCortex Data Lake から切断されました (フリー アラート)	FWとStrata Logging Service間の接続が失われました。 クラス:ヘルス カテゴリ:SLS接続性 アプリ内サポート チケット:いいえ
ファイアウォールがPanoramaから切断されました (フリー アラート)	ファイアウォールとPanorama間の接続が失われました。 クラス:ヘルス カテゴリ:接続失敗 アプリ内サポート チケット:いいえ
HA バックアップ (フリー アラート)	HA バックアップ リンクは現在設定されていません。 クラス:ヘルス カテゴリ:高可用性 アプリ内サポート チケット:いいえ
HA ピア接続ステータス (フリー アラート)	HA ペアのファイアウォールの 1 つが異常な状態です。 クラス:ヘルス カテゴリ:高可用性 アプリ内サポート チケット:あり
ディスク容量の使用率が高い - Pancfg パーティション	ハード ディスクのパーティションが容量に近づいているか、容量に達しています。 クラス:ヘルス

アラート	詳説
(フリー アラート)	カテゴリ:リソース 使用率 アプリ内サポート チケット:あり
ディスク容量の使用率が高い - Panlogs パーティション (フリー アラート)	ハード ディスクのパーティションが容量に近づいているか、容量に達しています。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:あり
ディスク容量の使用率が高い - ルート パーティション (フリー アラート)	ハード ディスクのパーティションが容量に近づいているか、容量に達しています。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:あり
高い処理活動 (フリー アラート)	デバイスで 1 つ以上のコンピューティング リソースが不足しています。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:いいえ
IPQエラー (フリー アラート)	ファイアウォールのFE100チップの1つでIPQ (Ingress Packet Queue)エラーが検出されました。このエラーは通常、再装着が必要である、またはハードウェアが故障していることを示します。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ
不規則な入力電力 (フリー アラート)	デバイスの電力レベルが正常範囲外です。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ
ライセンス失効 (フリー アラート)	1 つまたは複数のライセンスの有効期限が近づいているか、期限に達しています。 クラス:ヘルス

アラート	詳説
	カテゴリ:PanOSとサブスクリプション アプリ内サポート チケット:いいえ
ロギング ドライブの故障 (フリー アラート)	ファイアウォールのディスク ステータスのモニタリングにより、障害が発生したロギング ドライブが特定されました。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ
MPCカード - CPLD障害 (フリー アラート)	管理プロセッサ カード(MPC)は、管理、ログ記録、高可用性機能を提供するPA-5450の重要なコンポーネントです。MPCカードは、そのコンポーネントであるComplex Programmable Logic Device (CPLD) の問題により障害が発生しました。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ
NGFW/Panorama管理証明書の有効期限 (フリー アラート)	このアラートは、NGFW/Panorama管理証明書の有効期限を検出します。 クラス:ヘルス カテゴリ:証明書 アプリ内サポート チケット:いいえ
NPC カード - FE100障害 (フリー アラート)	Network Processing Card (ネットワーク プロセッシング カード - NPC)はネットワーク接続を提供し、ネットワーク トラフィック処理に不可欠です。NPCカードのFE100コンポーネントに問題が発生し、故障しました。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ
非同期ピア - 設定 (フリー アラート)	高可用性 ピアのシステム設定が一致しません。 クラス:ヘルス カテゴリ:高可用性 アプリ内サポート チケット:いいえ

アラート	詳説
非同期ピア - 動的コンテンツ (フリー アラート)	アンチウイルスやアプリケーションと脅威などの動的コンテンツは、高可用性ピア間で一致しません。 クラス:ヘルス カテゴリ:高可用性 アプリ内サポート チケット:いいえ
非同期ピア - セッション (フリー アラート)	高可用性ピア間でセッションが一致していないか、最新ではありません。 クラス:ヘルス カテゴリ:高可用性 アプリ内サポート チケット:いいえ
非同期ピア - ソフトウェア (フリー アラート)	高可用性ピアの PAN-OS ソフトウェア バージョンが一致しません。 クラス:ヘルス カテゴリ:高可用性 アプリ内サポート チケット:いいえ
古い動的コンテンツ (フリー アラート)	デバイスにインストールされた動的コンテンツは、更新サーバーで利用可能なコンテンツと比較すると古くなっています。 クラス:ヘルス カテゴリ:動的コンテンツ アプリ内サポート チケット:いいえ
PAN-OS のサポート終了 (フリー アラート)	PAN-OS の現在のバージョンはサポートされなくなりました。 クラス:ヘルス カテゴリ:PanOSとサブスクリプション アプリ内サポート チケット:いいえ
PAN-OS の既知の脆弱性 (フリー アラート)	PAN-OS の現在のバージョンには、既知の脆弱性があります。 クラス:ヘルス カテゴリ:動的コンテンツ アプリ内サポート チケット:いいえ

アラート	詳説
PAN-OSルート証明書とデフォルト証明書の有効期限 - シナリオ 1 (フリー アラート)	ファイアウォールのルート証明書とデフォルト証明書の有効期限が切れました。 クラス:ヘルス カテゴリ:証明書 アプリ内サポート チケット:いいえ
PCIエラー (フリー アラート)	周辺機器相互接続(PCI)は、管理プレーン(MP)を制御プレーン(CP)に接続する役割を担います。このコンポーネントに関連する特定のエラーは、その機能に障害があることを示します。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ
パス モニター障害 - カード (フリー アラート)	ファイアウォールのスロット内にあるカードでパス モニタリング障害が検出されました。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ
ポート障害 (フリー アラート)	管理物理ポートまたは高可用性物理ポートの1つに関連する障害が検出されました。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ
プロセス メモリの枯渇 - Configd (フリー アラート)	デバイスの管理プレーン プロセスが、使用可能なメモリを使い果たしています。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:あり
プロセス メモリの枯渇 - デバイス サーバー (フリー アラート)	デバイスの管理プレーン プロセスが、使用可能なメモリを使い果たしています。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:あり

アラート	詳説
プロセス メモリの枯渇 - ログ レシーバ (フリー アラート)	デバイスの管理プレーン プロセスが、使用可能なメモリを使い果たしています。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:あり
プロセス メモリの枯渇 - 管理サーバー (フリー アラート)	デバイスの管理プレーン プロセスが、使用可能なメモリを使い果たしています。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:あり
プロセス メモリの枯渇 - ユーザー ID (フリー アラート)	デバイスの管理プレーン プロセスが、使用可能なメモリを使い果たしています。 クラス:ヘルス カテゴリ:リソース 使用率 アプリ内サポート チケット:あり
冗長電源の障害 (フリー アラート)	電源が挿入されていない、電源が故障している、または完全な冗長性が実現されていないため、電源の冗長性が達成されません。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:あり
Strata Logging Serviceログ転送遅延 (フリー アラート)	Strata Logging Serviceの転送遅延が許容値を超えています。 クラス:ヘルス カテゴリ:SLSの健全性 アプリ内サポート チケット:いいえ
Strata Logging Serviceログ転送オフライン (フリー アラート)	Strata Logging Serviceログ転送サービスが機能していません クラス:ヘルス カテゴリ:SLSの健全性 アプリ内サポート チケット:いいえ

アラート	詳説
Strata Logging Serviceログ取り込み遅延 (フリー アラート)	Strata Logging Serviceの取り込み遅延が許容値を超えています。 クラス:ヘルス カテゴリ:SLSの健全性 アプリ内サポート チケット:いいえ
Strata Logging Serviceログ取り込みオフライン (フリー アラート)	Strata Logging Service取り込みサービスが機能していません。 クラス:ヘルス カテゴリ:SLSの健全性 アプリ内サポート チケット:いいえ
Strata Logging Serviceのログ保存容量が限界に近づいています (フリー アラート)	ログの種類が設定されたストレージの上限に近づいています。 クラス:ヘルス カテゴリ:ロギング アプリ内サポート チケット:いいえ
熱の問題 (フリー アラート)	デバイスの温度が正常範囲外です。 クラス:ヘルス カテゴリ:ハードウェア アプリ内サポート チケット:いいえ

サービス アラート

以下の表は、AIOps for NGFWで発生する可能性のある、接続されているサービスに関連するアラートを示しています。

アラート	詳説
ファイアウォールがStrata Logging Serviceから切断されました (フリー アラート)	FWとSLSの接続が5分以上途絶えています。 カテゴリ:SLS接続性 アプリ内サポート チケット:いいえ
Strata Logging Serviceログ取り込みオフライン (フリー アラート)	SLS取り込みサービスが5分以上機能しません。 カテゴリ:SLSの健全性 アプリ内サポート チケット:いいえ
Strata Logging Serviceログ転送オフライン (フリー アラート)	SLSログ転送サービスが5分以上機能しません。 カテゴリ:SLSの健全性 アプリ内サポート チケット:いいえ
Strata Logging Serviceのログ取り込み遅延 (フリー アラート)	SLSの取り込み遅延は、過去15分間で10分を超えています。 カテゴリ:SLSの健全性 アプリ内サポート チケット:いいえ
Strata Logging Serviceログ転送遅延 (フリー アラート)	SLSの転送遅延が過去15分間で10分を超えています。 カテゴリ:SLSの健全性 アプリ内サポート チケット:いいえ
Strata Logging Serviceのログ保存容量が限界に近づいています (フリー アラート)	ログの種類が設定されたストレージの上限に近づいています。 カテゴリ:ロギング アプリ内サポート チケット:いいえ

機械学習を活用して発生するアラート

以下の表は、機械学習を活用することでAIOps for NGFWで発生する可能性のあるアラートを示しています。

アラート	詳説
逆暗号化トラフィックのリソース使用率 (プレミアム アラート)	暗号化されたトラフィック リソースが不足しています。 クラス:ヘルス カテゴリ:リソース使用率 アプリ内サポート チケット:いいえ 検出時間:異常
リソースの不利な使用 (プレミアム アラート)	ファイアウォールには、1 秒あたりの接続数 (CPS)、スループット、またはセッション数の異常な値があります。 クラス:ヘルス カテゴリ:リソース使用率 アプリ内サポート チケット:いいえ 検出時間:異常
最大設定制限に近づいています (プレミアム アラート)	ルール、グループ、セキュリティ プロファイルなどのファイアウォール オブジェクトがデバイスの制限に近づいています。 クラス:ヘルス カテゴリ:設定制限 アプリ内サポート チケット:いいえ 検出時間:異常
高い処理活動 (フリー アラート)	デバイスで 1 つ以上のコンピューティング リソースが不足しています。 クラス:ヘルス カテゴリ:リソース使用率 アプリ内サポート チケット:いいえ
トラフィック レイテンシの増加 - パケット バッファ (プレミアム アラート)	デバイスのパケット バッファ リソースが不足しています。 クラス:ヘルス カテゴリ:リソース使用率 アプリ内サポート チケット:あり

アラート	詳説
	検出時間:異常
トラフィック レイテンシの増加 - パケット記述子 (プレミアム アラート)	デバイスのパケット記述子リソースが不足しています。 クラス:ヘルス カテゴリ:リソース使用率 アプリ内サポート チケット:あり 検出時間:異常
トラフィック レイテンシ - パケット記述子 (オンチップ) (プレミアム アラート)	デバイスのパケット記述子 (オンチップ) リソースが不足しています。 クラス:ヘルス カテゴリ:フラッド/DoS アプリ内サポート チケット:いいえ 検出時間:異常
最大容量に近づいています-ARPテーブル (プレミアム アラート)	データ予測解析によると、ARPテーブルのエントリはまもなくファイアウォールの最大容量に達する見込みです。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-アドレス グループ (プレミアム アラート)	アドレス グループ オブジェクトの数は一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-アドレス オブジェクト (プレミアム アラート)	アドレス オブジェクトの数が一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-データプレーンCPU (プレミアム アラート)	データプレーン(DP)のCPU使用率は長期にわたって一貫して高く、デバイスがサポートできる最大容量に近づいています。 クラス:ヘルス

アラート	詳説
	カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-復号化の使用状況 (プレミアム アラート)	データ予測解析によると、SSL復号化セッションはまもなくファイアウォールの最大容量に達する見込みです。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-FQDNアドレス (プレミアム アラート)	FQDNアドレス オブジェクトの数は一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-GlobalProtect トンネル(クライアントレス) (プレミアム アラート)	クライアントレスのGlobalProtect VPNトンネルの数は、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-IKEピア (プレミアム アラート)	IKEピアの数が一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-管理プレーンCPU (プレミアム アラート)	管理プレーン(MP)のCPU 使用率が一貫して高く、デバイスがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-管理プレーン メモリ (プレミアム アラート)	管理プレーン(MP)のメモリ使用率が一貫して高く、デバイスがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量

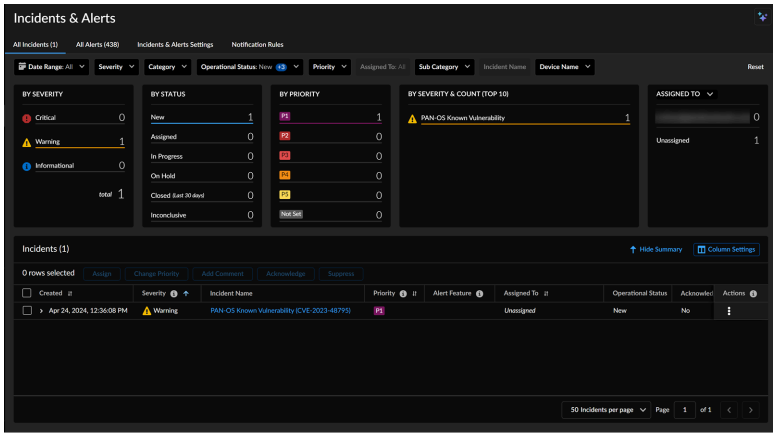
アラート	詳説
	アプリ内サポート チケット:いいえ
最大容量に近づいています-NAT ポリシー (プレミアム アラート)	NATポリシー ルールの数が長期にわたって一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-セキュリティ ポリシー (プレミアム アラート)	セキュリティ ポリシー ルールの数が一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-サービス グループ (プレミアム アラート)	サービス グループ オブジェクトの数は一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-サービス オブジェクト (プレミアム アラート)	サービス オブジェクトの数が一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-セッション テーブル使用率 (プレミアム アラート)	セッション テーブルの使用率(%)が長期にわたって一貫して高く、ファイアウォールまたはVMライセンスがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-仮想システム (プレミアム アラート)	データ予測解析によると、仮想システムの設定は、ファイアウォールのライセンスでサポートされる最大容量に達する見込みです。 クラス:ヘルス

アラート	詳説
	カテゴリ:容量 アプリ内サポート チケット:いいえ
最大容量に近づいています-サイト間VPNトンネル (プレミアム アラート)	IPSecトンネルとプロキシIDの両方で構成されるサイト間VPNトンネルの数が一貫して多く、ファイアウォールがサポートできる最大容量に近づいています。 クラス:ヘルス カテゴリ:容量 アプリ内サポート チケット:いいえ
NGFW SD-WAN アプリケーションパフォーマンスアラート (プレミアム アラート)	リンク パフォーマンスの低下の影響を受けるアプリケーションのリストを示します。 クラス:ヘルス カテゴリ:SD-WAN パフォーマンス アプリ内サポート チケット:いいえ 検出時間:異常
NGFW SD-WAN リンクパフォーマンスアラート (プレミアム アラート)	アプリやサービス、リンクのパフォーマンス低下の原因を示します。 クラス:ヘルス カテゴリ:SD-WAN パフォーマンス アプリ内サポート チケット:いいえ 検出時間:異常

NGFWインシデントの管理

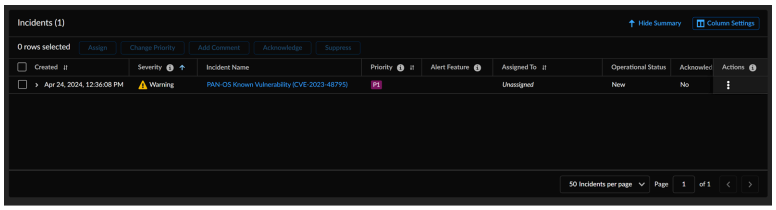
どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	以下のいずれかです: ❑ 又は ❑ 又は

［**Incidents & Alerts (**インシデントとアラート**)]** > **[NGFW]** > **[All Incidents (**すべてのインシデント**)]**］を選択すると、NGFWインシデントを俯瞰できます。インシデントページを調べて、デプロイメント環境の変更について常に把握できるようにし、必要に応じて予防処置を実施できるようにします。重要な視覚的な要約とともに、インシデントの詳細なリストに直接アクセスできます。**[Hide Summary (**サマリーを非表示にする**)]**では、ウィジェットを非表示にして、インシデントを表形式でのみ表示することもできます。



[All Incidents (すべてのインシデント**)]**下に表示されているデータです。

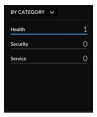
- インシデント:すべてのインシデントを表示します。



この表では、以下のタスクを実行できます。

- **[Hide Summary (**サマリーを非表示にする**)]**でウィジェットを非表示にして、インシデントを表形式でのみ表示することもできます。
- インシデントを展開すると、その説明と影響が表示されます。
- [Actions (アクション)]では、以下のアクションを実行できます。
  - ユーザー、お客様自身にインシデントを割り当てるか、インシデントの割り当てを解除します。
  - インシデントの優先度を変更するか、「未設定」を選択して優先度を削除します。
  - **[Yes (**はい**)]**を選択してインシデントを承認します 。これにより、インシデントを確認したことが確認されます。
  - インシデントを積極的に解決する予定がない場合、抑制するとインシデントを「保留中」の運用ステータスに設定します。
  - インシデントにコメントを追加します 。
- インシデントをクリックすると、その詳細が表示されます。
- ［**Column Settings (**カラムの設定**)**］を使用して、インシデントの特定のカラムを表示または非表示にし、カラムのデフォルトの順序を並べ替えます。これらの変更は、今後のセッションでも継続されます。

- **ASSIGNED TO**（担当者）:解決のタスクを持つ個人またはエンティティ別のインシデント数を表示します。上部には、現在ログインしているユーザーに割り当てられているインシデントと、割り当てられていないインシデントが表示されます。また、ドロップダウン リストでインシデントを選択して、カテゴリ別のインシデント数を表示することもできます。



- 重大度と数**(**トップ**10):**重大度別に分類されたインシデントを、各カテゴリのインシデント数とともに表示します。重大インシデントの優先順位は、最初に警告インシデント、次に情報インシデントの順になります。

- ステータスごと:インシデントの総数をステータス別に表示します。
  - [New (新規)]は未割り当てのインシデントを示します。
  - [Assigned (割り当て済み)]は、ユーザーに割り当てられているインシデントを示します。
  - [In Progress (進行中)]は、インシデントの処理中であることを示します。
  - [On Hold (保留)]は、インシデントを解決するまたはインシデントを積極的に解決する予定がないことを示します。
  - [Closed (クローズ済み)]は、過去30日間にクローズされたインシデントを示します。
  - [Inconclusive (不確定)]は、これらのインシデントに対する解決策がないことを示しています。

- 重要度別:[Critical (重大)]、[Warning (警告)]、および[Informational (情報)]に分類されたインシデントの総数が表示されます。

- 優先順位ごと:インシデントを優先度に従って表示します。P1が最も重大です。

インシデントの詳細の表示

どこで使用できますか?	何が必要ですか?
• Software NGFW Creditsによって資金提供されたものを含む	以下のいずれかです: ❑ 又は ❑ 又は

[All Incidents (すべてのインシデント)]で、インシデントを選択すると、そのインシデントの詳細が記載されたページを開くことができます。**[Summary (概要)]**タブには、以下の詳細が表示されます。

1. インシデントの概要と詳細。インシデントの優先度を変更したり、ユーザーに割り当てることができます。
2. インシデントによって引き起こされた影響、つまり影響を受けたNGFWの数。
3. 問題を解決するための推奨処置。

CVEをクリックして、その詳細をPalo Alto Networksセキュリティ アドバイザリとPAN-OSバージョンの脆弱性で表示することもできます。

[Correlated Alerts & Activity (相関アラートとアクティビティ)] タブには、以下の詳細が表示されます。

- 選択したインシデントの相関アラート
- インシデントの記録されたアクティビティ