paloalto TECHDOCS

NGFW 事件和警示

docs.paloaltonetworks.com

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

警示

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或者 ❑ 或者

為了幫助您維持裝置正常運作並避免業務中斷事件，AIOps for NGFW 根據在防火牆部署中偵測到的一或多個問題產生警示。這些問題或事件可透過以下三種方式之一觸發：

- 當指標發生重大變更時
- 當先前產生的事件發生變更時
- 當使用者或系統執行操作時，例如確認或關閉警示

這項警示指出需要解決的特定問題（防火牆功能降級或遺失）。也可以根據多個事件之間的關聯或整合來產生警示。將事件整合為單一警示有助於分類、簡化團隊之間的警示傳遞、集中關鍵資訊並減少通知疲勞。

根據與其相關聯的指標，警示分為不同的類別。您可以使用警示類別來指定您收到通知的警示類型。例如，硬體、設定限制、資源限制、動態內容以及 PAN-OS 和訂閱。

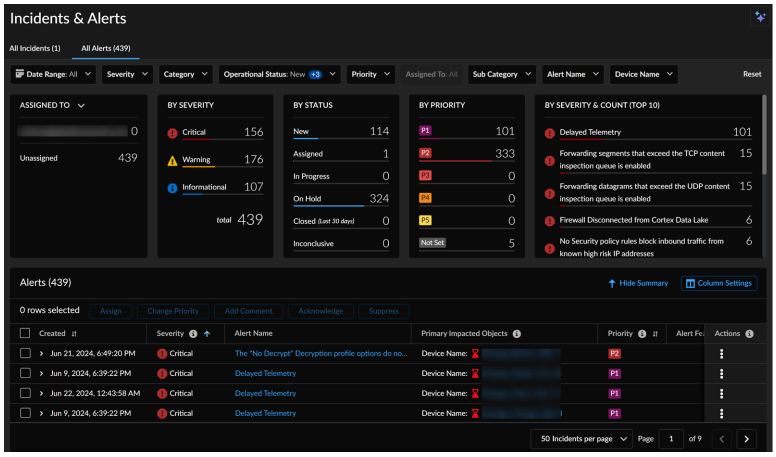
從 **Incidents & Alerts**（事件和警示） > **NGFW** > **All Alerts**（所有警示）中，您可以查看和管理為部署產生的所有警示。在 **Notification Rules**（通知規則）中，您可以設定通知規則，指定事件觸發警示時您希望收到通知的時間和方式。

- 管理 NGFW 警示
- 查看警示詳細資訊
- 檢視可能的原因
- 預測和異常偵測
- 管理功能分析器警示
- AIOps for NGFW 中的 CPU 使用指標
- 建立通知規則
- 與 ServiceNow 整合

管理 NGFW 警示

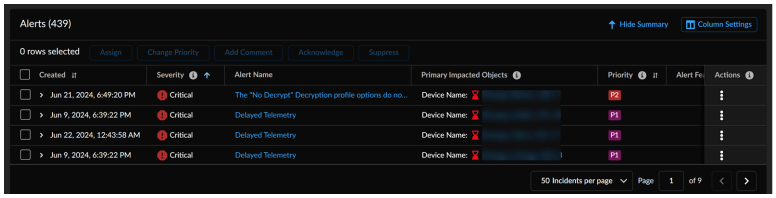
我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或者 ❑ 或者

透過選擇 **Incidents & Alerts**（事件和警示） > **NGFW** > **All Alerts**（所有警示）來取得 NGFW 警示的鳥瞰圖。探索警示頁面，幫助您維持裝置和部署的持續運作狀況，並避免業務中斷。您可以直接存取詳細的警示清單以及關鍵的視覺化摘要。您還可以 **Hide Summary**（隱藏摘要）以隱藏 Widget 並僅以表格格式查看警示。



以下是 **All Alerts**（所有警示）下顯示的資料。

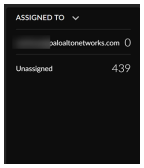
- **Alerts**（警示）：顯示所有警示。

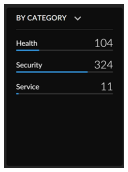


在此表中，您可以執行下列任務：

- 隱藏摘要以隱藏 Widget 並僅以表格格式查看警示。
- 展開警示以查看其說明和影響。
- 在 [Actions（動作）] 下方，您可以執行以下動作：
  - 指派警示給使用者、您自己，或取消指派警示。
  - 變更警示的優先順序或選取 [Not Set（未設定）] 以移除優先順序。
  - 透過選取 [Yes（是）] 來確認警示，確認您已看到該警示。
  - 當您不打算主動解決事件時，抑制功能會將警示設為「保留」作業狀態。
  - 為警示新增註解。
- 按一下警示以檢視其詳細資訊。
- 使用欄設定檢視或隱藏警示的特定欄，並重新排列欄的預設順序。這些變化會在未來的工作階段中持續存在。

- 指派給：顯示按負責解決事件的個人或實體劃分的警示數。在頂部，它顯示指派給目前登入使用者的警示和未指派的警示。您也可以透過在下拉式清單中選取 [BY CATEGORY（依類別）] 來檢視警示數量。





- 依嚴重性和計數（前 **10** 名）：顯示依嚴重性分類的警示，以及每個類別中的警示計數。首先優先考慮嚴重警示，其次是警告警示，最後是資訊警示。

- 依狀態：依狀態顯示警示總數。
  - 「新增」表示尚未指派的事件。
  - 「已指派」表示已指派至使用者的事件。
  - 「進行中」表示該事件正在處理中。
  - 「保留」表示您不打算主動解決該警示。
  - 「已關閉」表示過去 30 天內已關閉的警示。
  - 「不明」表示這些警示沒有解決方案。

- 依嚴重性：顯示分類為「嚴重」、「警告」和「資訊」的警示總數。

- 依優先順序：根據警示的優先順序顯示事件，其中 P1 是最嚴重的警示。

查看警示詳細資訊

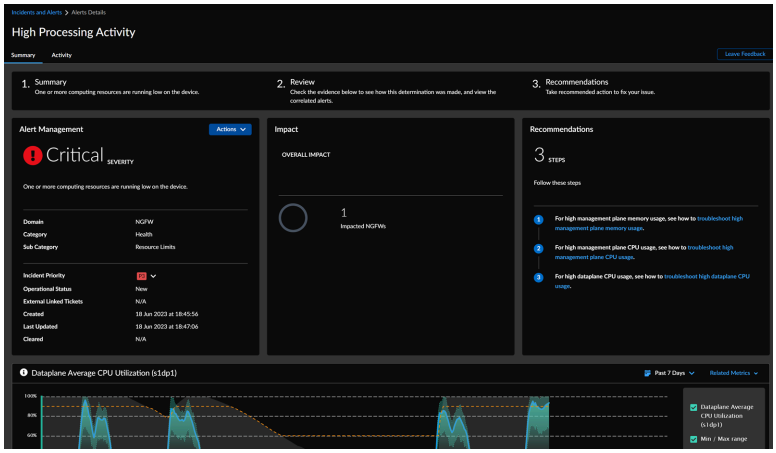
我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或者 ❑ 或者

從 **All Alerts**（所有警示）中，您可以選取一個警示來開啟包含其詳細資訊的頁面。**Summary**（摘要）標籤顯示以下詳細資訊：

1. 警示摘要及詳細資訊。您可以變更警示的優先順序或將其指派給使用者。
2. 警示造成的影響，亦即受影響的 NGFW 數量。
3. 用於解決您的問題的修復建議和資源。

您也可以檢查貢獻事件的圖表。

Activity（活動）標籤顯示警示的記錄活動。



檢視可能的原因

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	❑ 或

使用進階的 AI 功能，AIOps for NGFW 會顯示產生警示的可能原因，並提供有關如何解決基礎問題的建議。此功能透過減少干擾並將網路安全解決方案的效益最大化，以確保最佳的網路效能。

以下是支援可能原因分析的警示：

- 高處理活動
- 流量延遲增加 - 封包緩衝區
- 流量延遲增加 - 晶片上封包描述元
- 允許的威脅
- 流量延遲 - 封包描述元（晶片上）
- 不良資源使用
- 不同步對等 - 設定
- 潛在的認證盜竊濫用
- 提交推送失敗

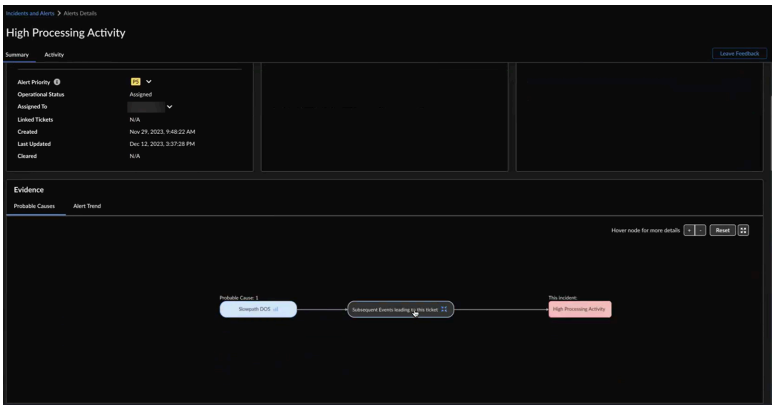
可能原因分析已增強，以利用 Strata Logging Service 日誌並提供額外的中繼資料，以便指出導致建立警示或事件的可能原因。此增強功能可讓您精確地指出可能導致警示的原則、應用程式、來源區域、URL、來源 IP 和地區。

您可以檢視下列情況的可能原因：

- 高處理活動（高處理活動警示）：當資料平板 CPU 使用率高時，可能會導致各種問題，例如防火牆不穩定、防火牆中止或卡住狀態，以及封包遺失或延遲問題。這可能會對您的業務營運造成負面影響。如果資料平面 CPU 使用率至少為 60%，且使用率有顯著飆升，則 AIOps for NGFW 會在「高處理活動」警示中顯示可能的原因。但是，如果資料平板 CPU 使用率長時間維持在高水平而沒有變化，則造成原因會不明確而無法輕鬆判定，因此不會顯示任何可能的原因。例如，如果資料平面 CPU 使用率長時間內持續為 70%，AIOps for NGFW 將不會顯示任何可能的原因。
- 單一或多個窮盡工作階段偵測和修復（高處理活動警示）：對防火牆的窮盡工作階段攻擊是指攻擊者快速建立多個連線，利用防火牆的內部資源，而可能導致資源耗盡和拒絕服務 (DoS) 事件。AIOps for NGFW 可以偵測出這些問題並顯示可能的原因。
- 工作階段耗盡與連線遺失（高處理活動警示）：當防火牆接收流量時，它會為該流量建立一個工作階段以追蹤其狀態，並執行必要的安全性檢查。每個工作階段都會消耗系統資源，包括記憶體和 CPU 週期。如果防火牆達到同時工作階段的最大容量，就會導致工作階段耗盡。此問題可能由於多個原因引起，包括流量過大、安全性原則設定錯誤，以及不當的工作階段逾時設定。AIOps for NGFW 利用進階的 AI 功能，主動偵測網路裝置中的工作階段耗盡問題。這可實現最佳化的資源配置、提高網路效能，並減輕連線問題，以確保不間斷的服務可用性。

- 由於單一應用程式導致的高封包緩衝使用率（增加流量延遲 - 封包緩衝區）：AIOps for NGFW 偵測到由於單一應用程式獨佔封包緩衝區，導致封包緩衝區使用率高的可能根本原因。AIOps for NGFW 利用進階的 AI 功能，透過及時提醒資源配置不當，並防止效能降級，以確保最佳的網路效能。
- 由於單一應用程式導致的高封包描述元晶片上使用率（增加流量延遲 - 晶片上封包描述元）：AIOps for NGFW 可偵測晶片上封包描述元使用率高的可能根本原因。這有助於主動識別和解決由單一應用程式獨佔晶片上封包描述元所造成的網路擁塞。
- 低速路徑 **DoS** 攻擊偵測和修復建議（高處理活動警示）：AIOps for NGFW 利用 AI 技術偵測低速路徑 DoS 攻擊，確保網路安全性和不間斷的服務可用性。它會根據因果關係分析執行高資料平面處理活動警示、高原則拒絕活動根本原因分析，以及修復建議。
- 高 **URL** 快取查找活動偵測和修復（高處理活動警示）：AIOps for NGFW 可偵測並解決高 URL 快取查找活動，從而將處理效率最佳化並維持系統穩定性。此功能會將 URL 快取查找活動與 DP CPU 使用率相關聯，識別高 CPU 使用率，並提供修復建議，以防止接近飽和情況。
- 高內容處理活動偵測和修復（高處理活動警示）：AIOps for NGFW 功能可偵測高內容處理活動。此功能會分析各種內容處理階段與資料平面 CPU 使用率之間的關聯性，識別高 CPU 使用率或接近飽和情況的執行個體，並提供可行的修復建議以提高系統穩定性。
- 憑證太長的 **RCA** 報告（提交推送失敗警示）：AIOps for NGFW 偵測到提交失敗並概述提交失敗的潛在原因，尤其是當憑證長度超過緩衝區大小時。

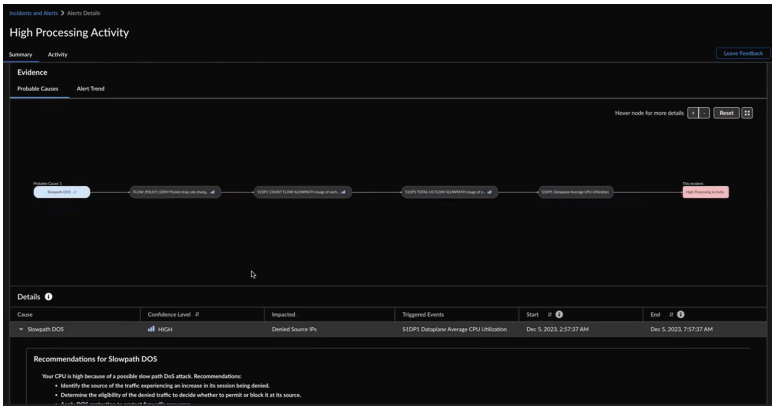
STEP 1 | 從**Incidents & Alerts**（事件和警示） > **Alerts**（警示）中，選取警示以開啟包含警示詳細資訊的頁面。



流程圖表示：

- 觸發高處理活動警示的事件
- 觸發事件的可能原因

您也可以將游標暫留在節點上以檢視更多詳細資訊，例如可能的原因、信賴等級、觸發的事件以及影響的持續時間。當事件節點達到三個或更多時，您可以按一下並展開事件以檢視詳細資訊。



AIOps for NFGW 也以表格格式顯示相同的資訊。您可以將游標暫留在表格中可能的原因上，以查看流程圖中反白顯示的節點和路徑。您也可以按一下流程圖中可能的原因，以表格格式檢視其詳細資訊。

Confidence Level（信賴等級）指出某些 AIOps for NGFW 如何識別高處理活動警示的原因。可能的原因會按信賴等級以遞減順序排序。您可以從檢查高信賴等級的原因開始。

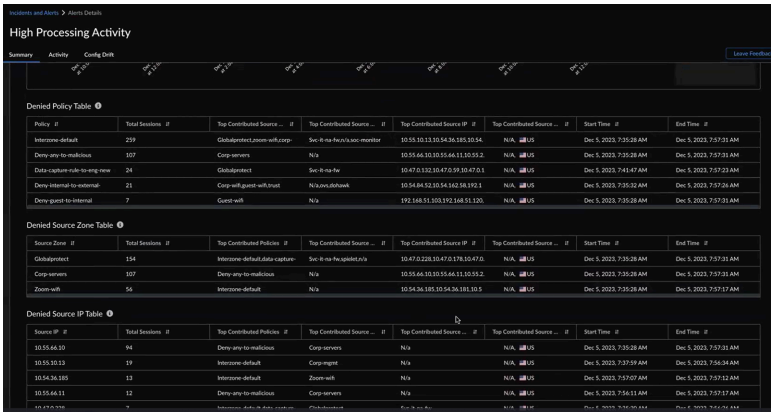
STEP 2 | 在表格中展開一個可能原因，以檢視您所要調查可能與觸發警示相關的圖形和受影響的指標。

STEP 3 | 使用圖表工具來檢查圖形。

因果關係期間可讓您將警示的 **Cause**（原因）與 **Triggered Event**（觸發事件）之間隨時間變化的因果關係視覺化。

您可以在圖表中檢視影響之前和之後的 6 小時、24 小時或 48 小時的情況。

可能原因分析會增強，以使用 SLS 記錄檔，並為導致建立警示或事件的可能原因提供額外的中繼資料。此增強功能可讓您精確地指出可能導致警示的原則、應用程式、來源區域、URL、來源 IP 和地區。例如，當高資料平面 CPU 使用率觸發 **High Processing Activity**（高處理活動）警示時，您可以利用可能的原因分析來識別警示的主要參與者，並遵循建議的修復建議。



預測和異常偵測

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或者 ❑ 或者

一般情況下，AIOps for NGFW 透過將固定規則應用於部署中的指標來偵測問題。例如，如果管理平面 CPU 使用率超過 85%，則該指標會進入「嚴重」狀態。

但是，為了提醒您固定規則可能遺漏的事件，AIOps for NGFW 可以使用機器學習來了解您的部署，並根據您的使用趨勢提供量身打造的其他警示和事件。

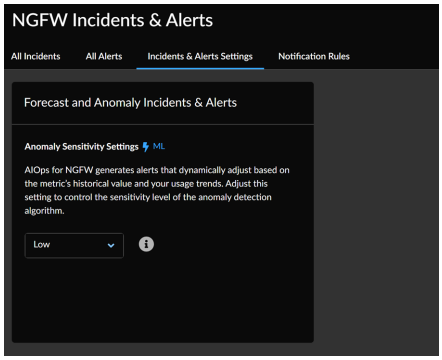
- **Forecast-Based Alerts**（基於預測的警示）可協助您透過預測裝置指標的變化來提前識別問題，並根據預測結果向您發出警示。
- **Anomaly-Based Alerts**（基於異常的警示）為裝置指標建立基準行為，並在該指標超出指定的 **Anomaly Sensitivity Settings**（異常敏感度設定）時向您發出警示。

預測和異常偵測的好處如下：

- 主動管理：透過提早預測潛在問題並識別異常情況，管理員可以採取主動措施來防止問題發生、減少停機時間並提升整體網路效能。
- 增強安全性：偵測異常模式和行為可協助識別安全威脅和弱點，從而及時介入和降低風險。
- 最佳化資源：預測功能有助於將資源做更好的規劃和配置，確保網路基礎設施做好充分準備以應對未來的需求。

導航至 **Incidents & Alerts**（事件和警示） > **Incident & Alert Settings**（事件和警示設定） > **Forecast and Anomaly Incidents & Alerts**（預測和異常事件和警示）。

AIOps for NGFW 產生根據指標的歷史值和您的使用趨勢動態調整的警示和事件。偏離正常範圍可能表示有潛在問題。您可以調整此設定來控制異常偵測演算法的敏感度層級。



管理功能分析器警示

我可以在哪裡使用這個？	我需要哪些內容？
•	❑ 或

容量分析器使用機器學習模型來預測接近其最大容量的資源耗用量並發出警示。容量分析器警示會提前生成以識別潛在的容量瓶頸。

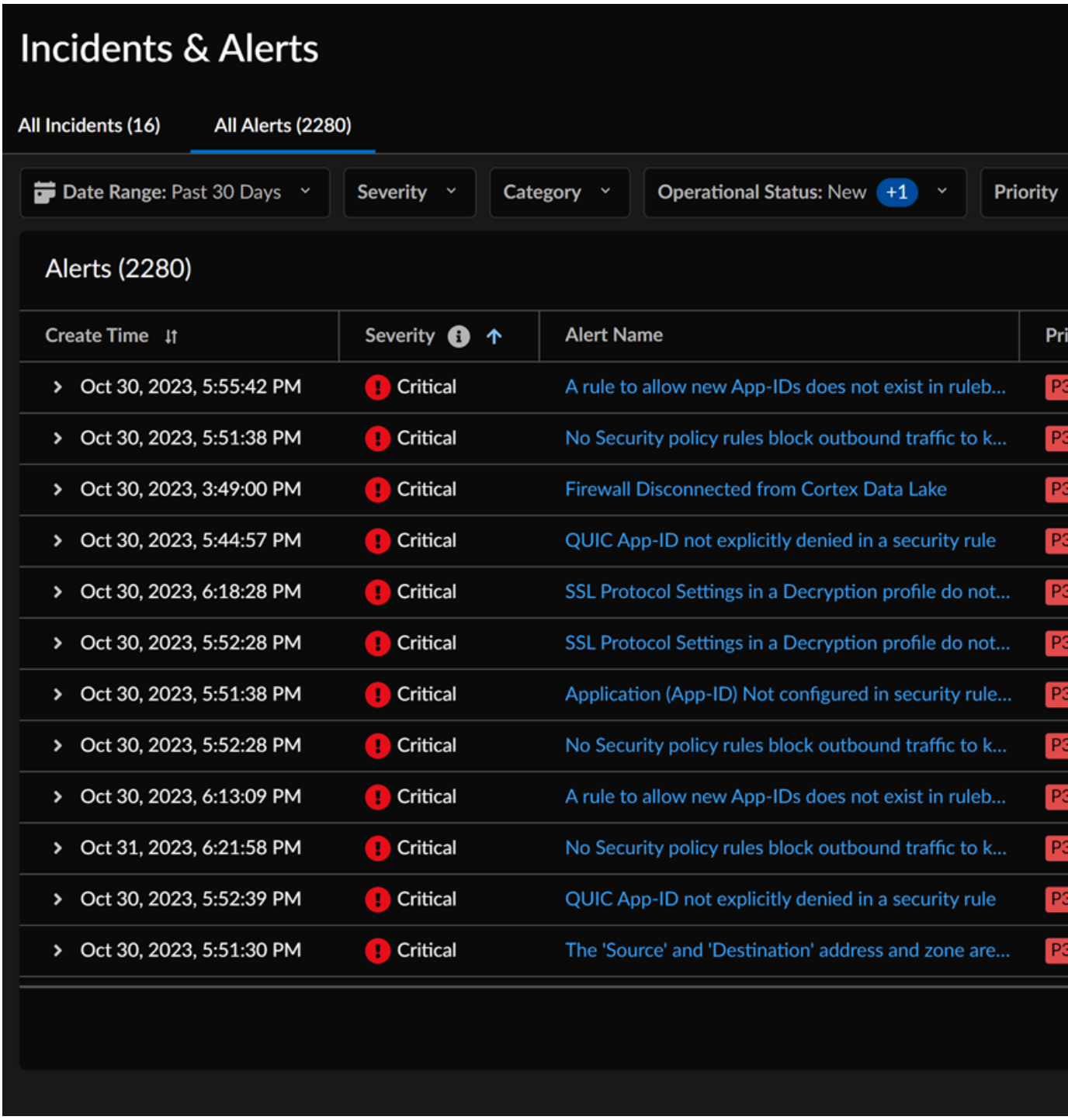
您也可以建立通知規則，以觸發容量分析器警示的通知。

STEP 1 | 導覽至 **Incidents & Alerts**（事件和警示） **>NGFW > All Alerts**（所有警示），然後按一下 **List View**（清單檢視）。

STEP 2 | 在 **Alert Name**（警示名稱）下，搜尋 **approaching max alerts**（接近最大警示）。

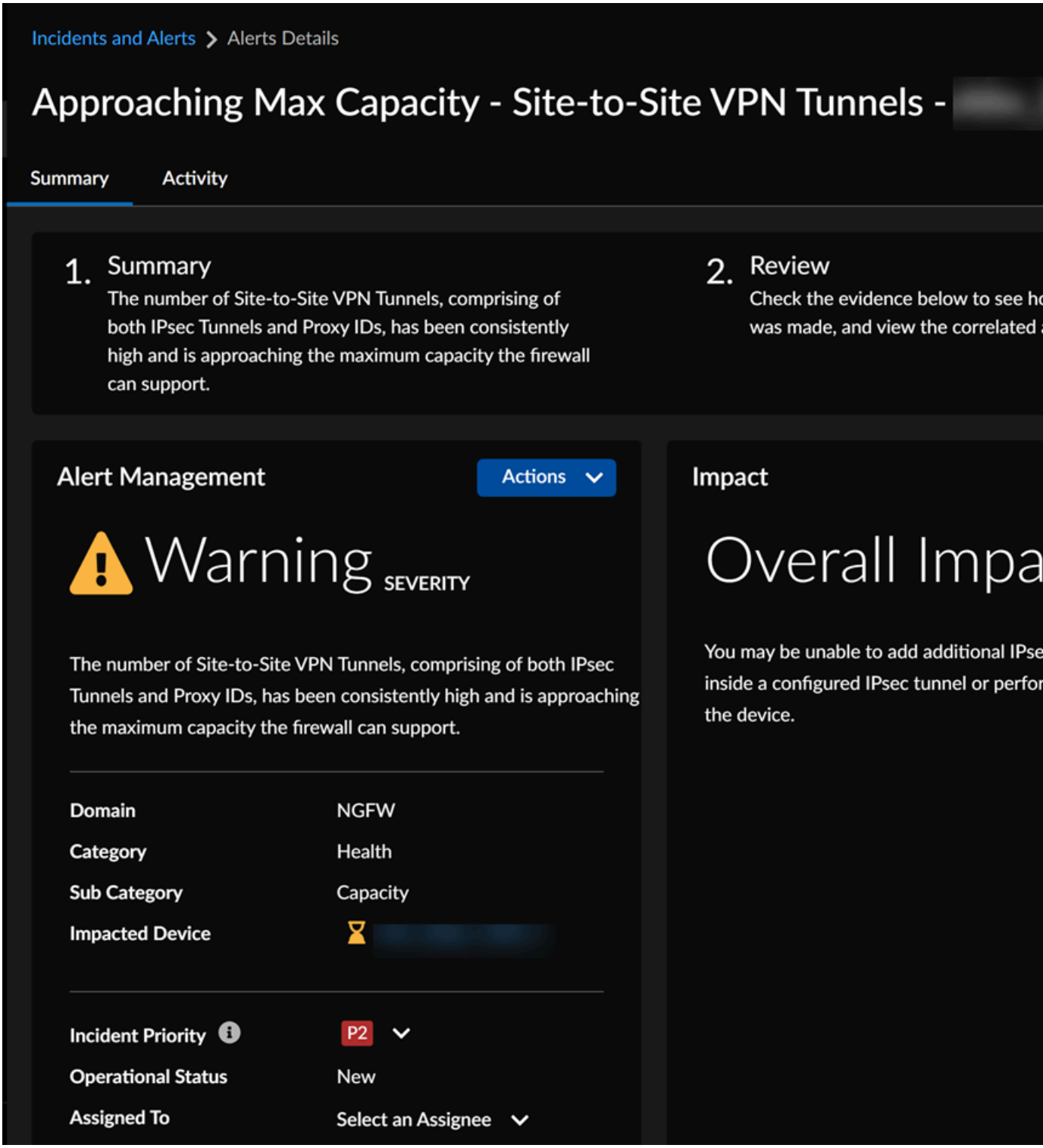
針對容量分析器功能發出的警示命名為：

接近最大容量 - <*Metric-Name*>。



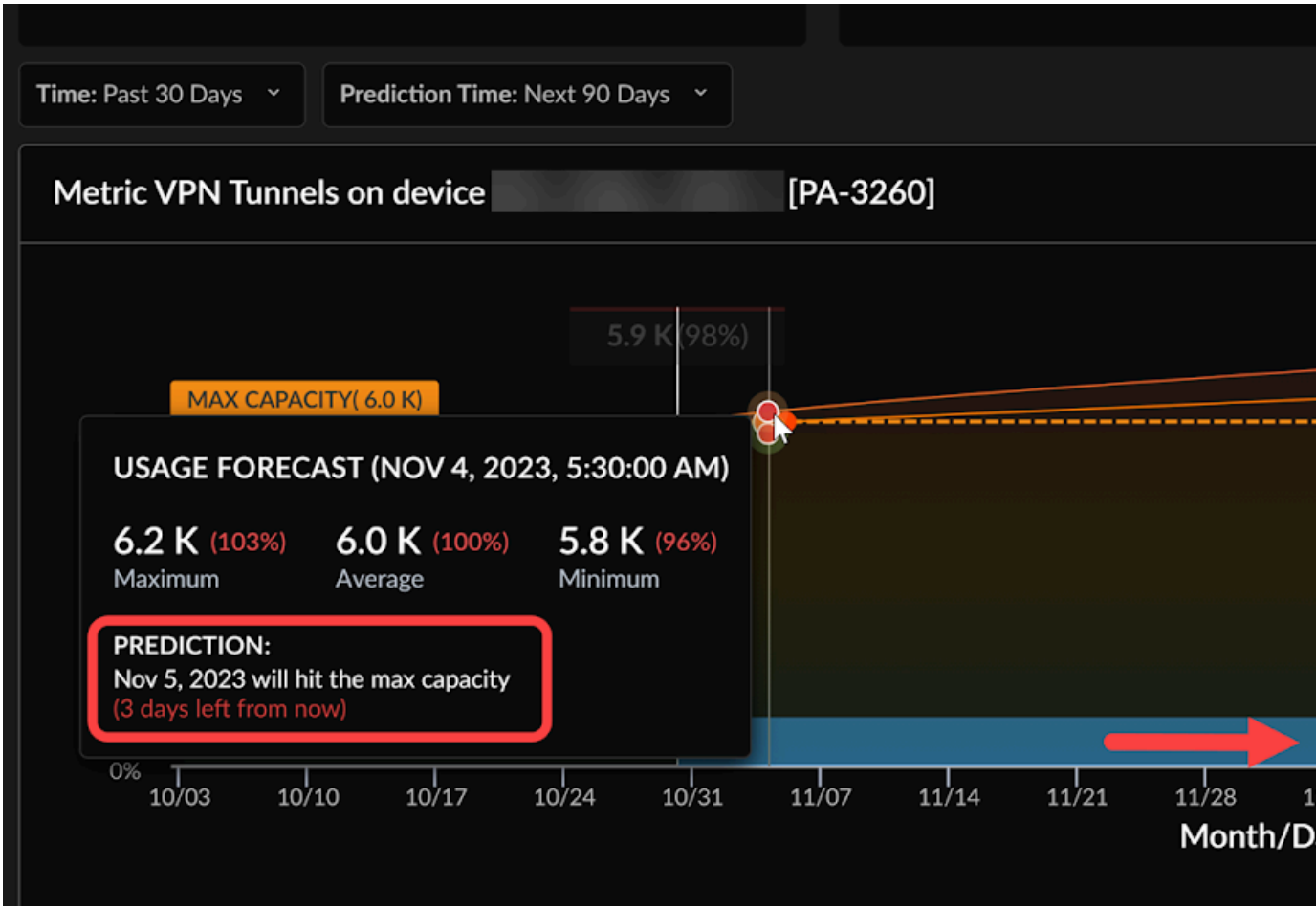
STEP 3 | 選擇其中一個警示以檢視其詳細資訊，其中包括：

- 警示摘要及詳細資訊。
- 警示造成的影響。
- 建議採取的動作來解決您的問題。

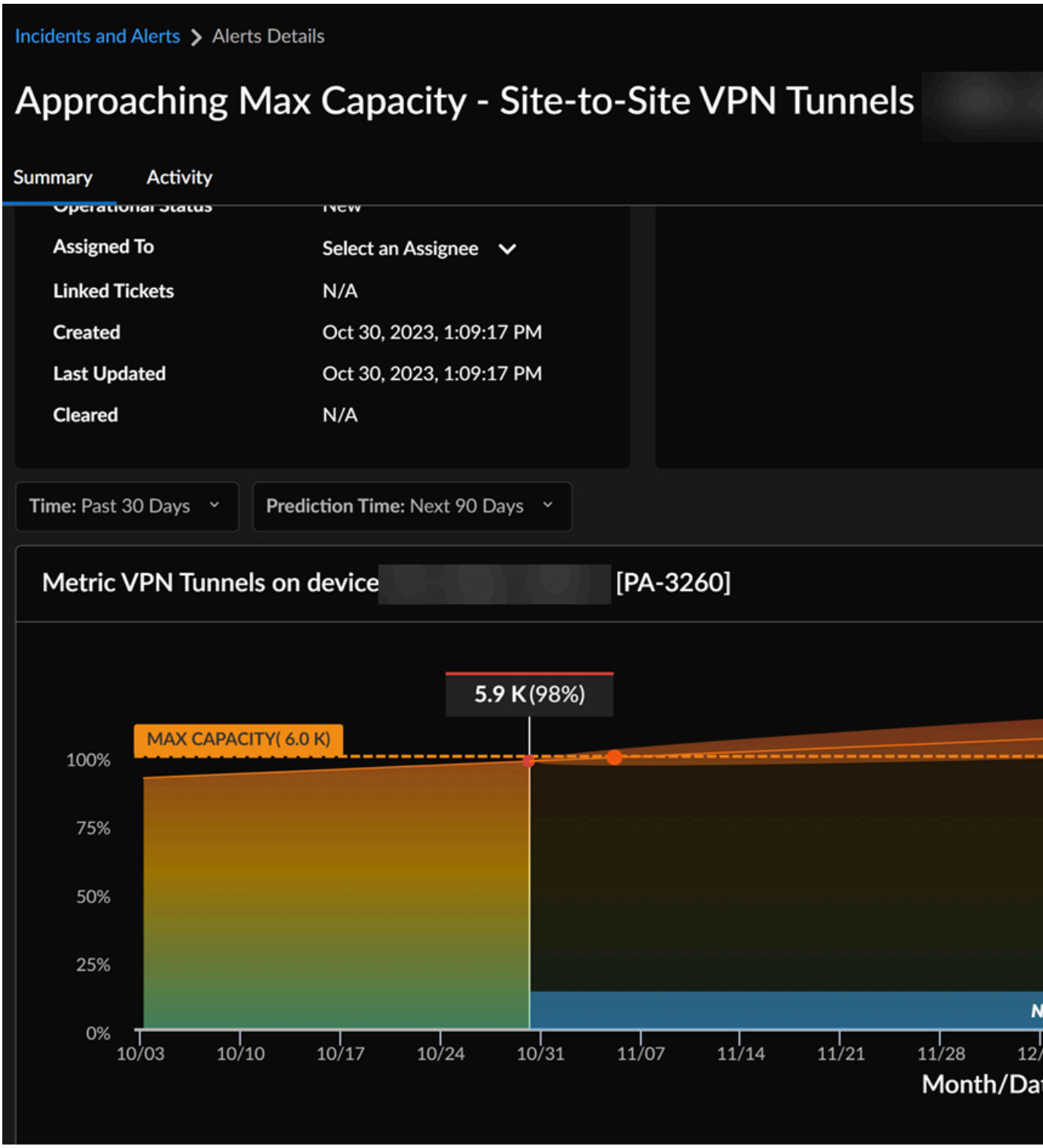


在警示詳細資訊中，您還可以查看顯示指標趨勢的圖表。Strata Cloud Manager 預測指標達到最大容量的日期。您可以將游標停留在圖表上以檢查任何特定時間點的指標容量。您可以選取未來 30 天或 90 天的 **Prediction Time**（預測時間）。

在此範例中，您可以看到裝置上的 VPN 通道指標將在 **Nov 5, 2023**（**2023** 年 **11** 月 **5** 日）達到最大容量。



STEP 4 | 從 **Alerts**（警示）頁面，您可以 **Go to Capacity Analyzer Page**（前往容量分析器頁面）以檢視容量分析器熱圖。



如需如何使用容量分析器熱圖並檢查容量警示的相關資訊，請參閱分析指標容量。

AIOps for NGFW 中的 CPU 使用指標

我可以在哪裡使用這個？	我需要哪些內容？
• ， 包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或者 ❑ 或者

使用以下指標追蹤 AIOps for NGFW 中的 CPU 使用率：

- **mp_system_resources.mp_cpu**：表示 CPU 使用率總計。
- **mp_system_resources_daemon.cpu_usage_sum**：表示在管理平面 CPU (MP-CPU) 中執行的管理平面任務所產生的 CPU 使用率。此指標相當於 SNMP 中 CPU 使用率。
- **mp_system_resources_daemon.pan_task_cpu_usage**：表示來自 MP-CPU 上執行資料平面類型操作的 PAN 任務所產生的 CPU 使用率。此資料不是 SNMP 和 **mp_system_resources_daemon.pan_task_cpu_usage** 指標的一部分。

CPU 使用率總計如下：

mp_system_resources.mp_cpu = mp_system_resources_daemon.cpu_usage_sum + mp_system_resources_daemon.pan_task_cpu_usage

建立通知規則

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或者 ❑ 或者

將 Strata Cloud Manager 整合到您現有的操作中，涉及設定主動警示，使您能夠在潛在問題升級為嚴重複雜的問題之前，及早偵測和管理潛在問題。這些警示可以根據您的營運團隊的案例管理通訊協定量身打造，例如常用的 P1 或 P2。

例如，您可以設定一個警示系統，其中代表最嚴重問題的嚴重警示會即時升級到您的安全團隊，以供其立即處理。另一方面，繁告類繁示的緊急程度較低，但仍然具有重要性，可以安排每日審查。這種安排可確保高效率的事件管理，同時保持營運的順利運作。

另一種選擇是根據團隊路由警示；某些類別的警示，甚至特定的警示，可以路由到最有能力處理這些問題的不同團隊。您可以定義通知偏好設定，例如哪些警示觸發通知、接收通知的方式以及接收通知的頻率，來建立通知規則。

以下影片示範如何建立通知規則。

STEP 1 | 選取 **Incidents & Alerts**（事件和警示） > **Incident & Alert Settings**（事件和警示設定） > **Notification Rules**（通知規則） > **+ Add Notification Rule**（+ 新增通知規則）

STEP 2 | 輸入名稱及說明。

STEP 3 | **Add New Condition**（新增條件）以指定將觸發通知的 `Rule Conditions`（規則條件）。

例如，若要建立硬體警示通知，請選取 **subCategory**、**Equals**（等於）和 **Hardware**（硬體）。

STEP 4 | 選擇通知的通知類型和收件者。

1. 如果選取 **Email**（電子郵件），請選取一個電子郵件群組（接收電子郵件通知的使用者群組），或 **Create a New Email Group**（建立新電子郵件群組）。
   1. 若要建立新的電子郵件群組，請輸入電子郵件群組名稱，然後開始輸入要新增至群組的電子郵件地址。填寫完每個電子郵件地址後，按下 Return 鍵。
   2. 選取 **Next**（下一步）。
   3. 選取您要傳送這些通知的頻率：
      - 立即
      - 每 4 小時分組傳送一次
      - 每天分組傳送一次
2. 如果選擇 **ServiceNow**，請輸入 `ServiceNow URL`、用戶端憑證、ServiceNow 憑證和 `ServiceNow API` 版本。
   1. **Test**（測試）您的連線以確保整合正常運作。
   2. 選取 **Next**（下一步）。

STEP 5 | **Save Rule**（儲存規則）。

與 ServiceNow 整合

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	❑ 或

在 AIOps for NGFW 通知規則上設定 ServiceNow 整合時，您需要下列項目：

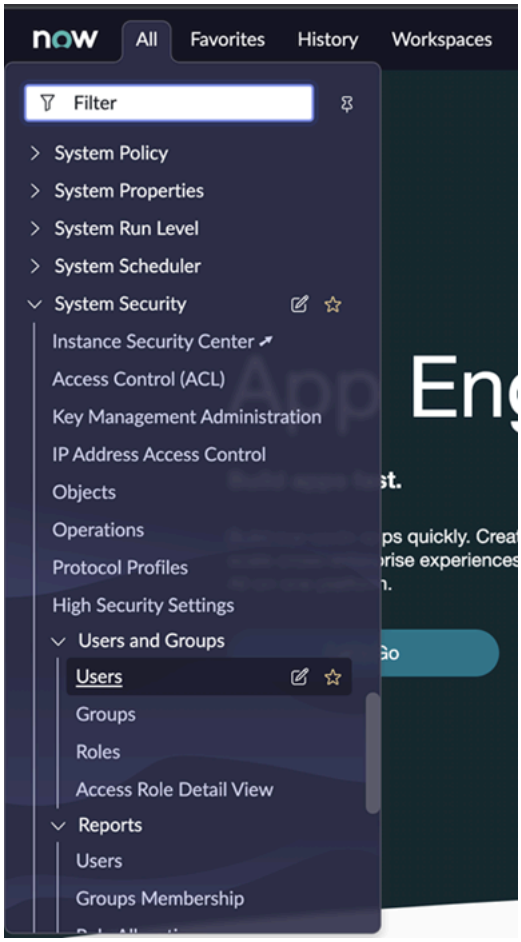
- 設定具有管理存取權的 ServiceNow 執行個體
- ServiceNow 使用者名稱和密碼，具有 Web 存取和特定角色，用於建立事件或查詢各種表格
- 在應用程式登錄下建立的用戶端 ID 和密碼，用於授權 AIOps 存取您的 ServiceNow 執行個體
- 您的 ServiceNow 執行個體的 URL

您的 ServiceNow 執行個體應該還包含一個 **Incident**（事件）表格，用於讓 AIOps 傳送警示，並應該設有 **Assignment Groups**（指派群組）和 **Assignees**（指派者），以便將這些警示發給特定人員。

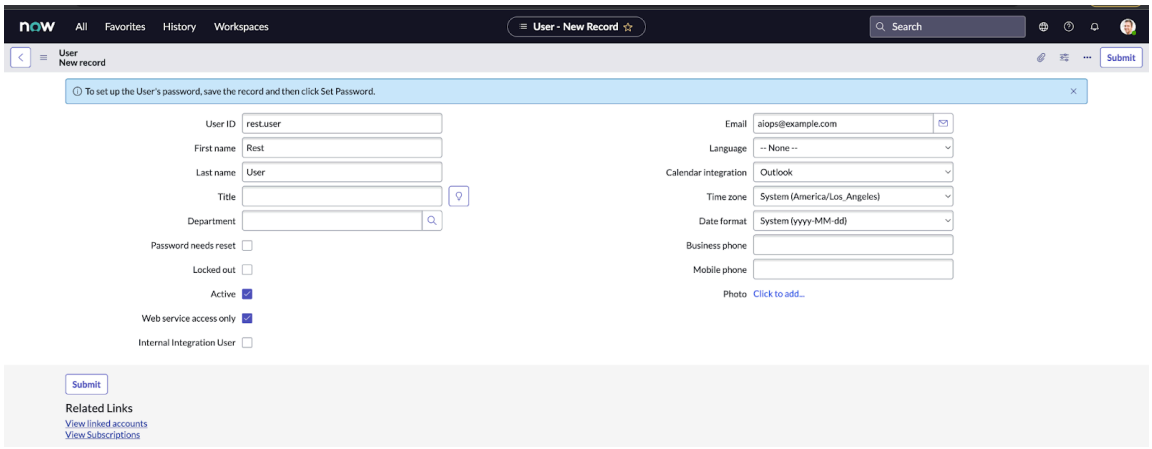
STEP 1 | 建立 ServiceNow Rest User。

建立具有特定角色的新 ServiceNow 使用者，以讀取和寫入整合所需的各種表格（事件、指派群組和指派者）。

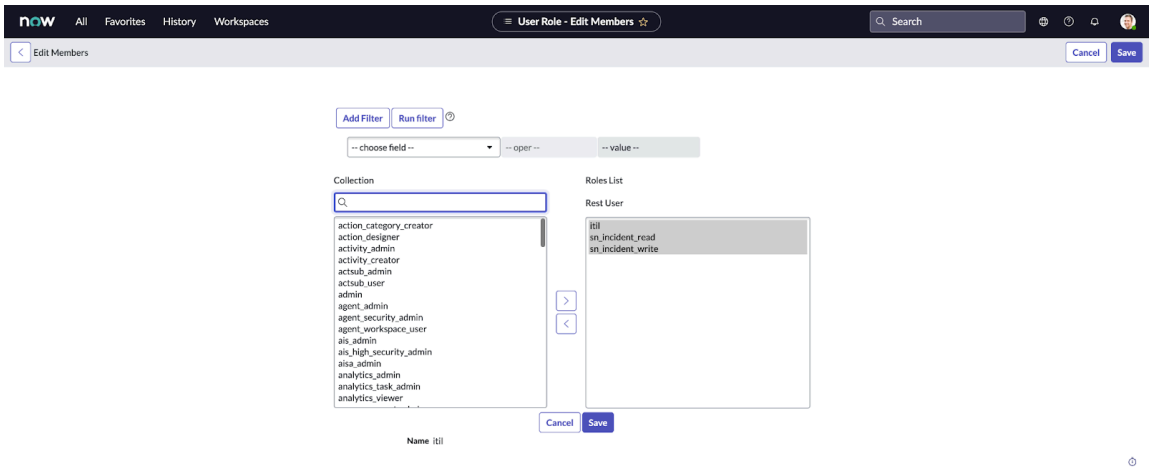
1. 若要在 ServiceNow 中建立使用者，請瀏覽至 **Security**（安全性）**> Users and Groups**（使用者和群組）下的 **Users**（使用者）。



2. 勾選 **Web service access only**（僅限 **Web** 服務存取）核取方塊並提交變更。

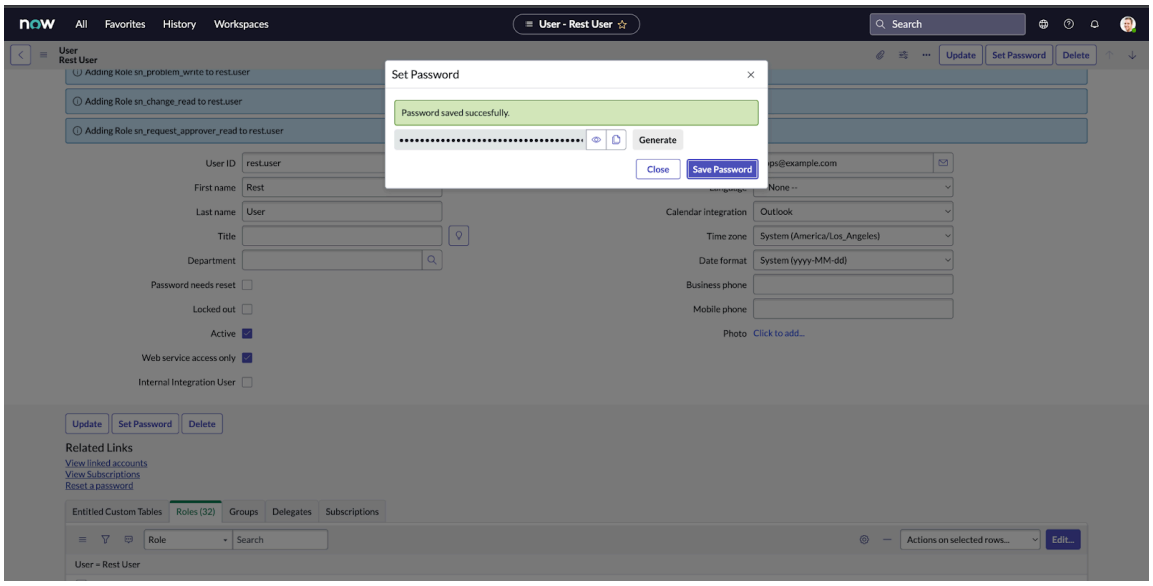


3. 搜尋新建立的使用者。在頁面底部的表格中選取 **Roles**（角色）索引標籤，然後按一下 **Edit**（編輯）。您需要授予使用者以下三個角色的權限：**itil**、**sn_incident_read** 以及 **sn_incident_write**。儲存變更。



4. 按一下 [User（使用者）] 頁面上的 **Set Password**（設定密碼）。在彈出式視窗中，按一下 **Generate**（產生）並 **Save Password**（儲存密碼）。請務必將密碼與使用者

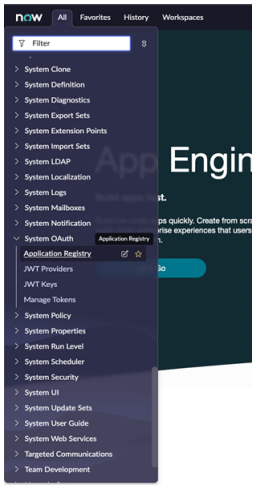
ID 一起複製到安全的位置。此資訊會用於填入 AIOps for NGFW 中的 **ServiceNow User**（**ServiceNow** 使用者）認證。



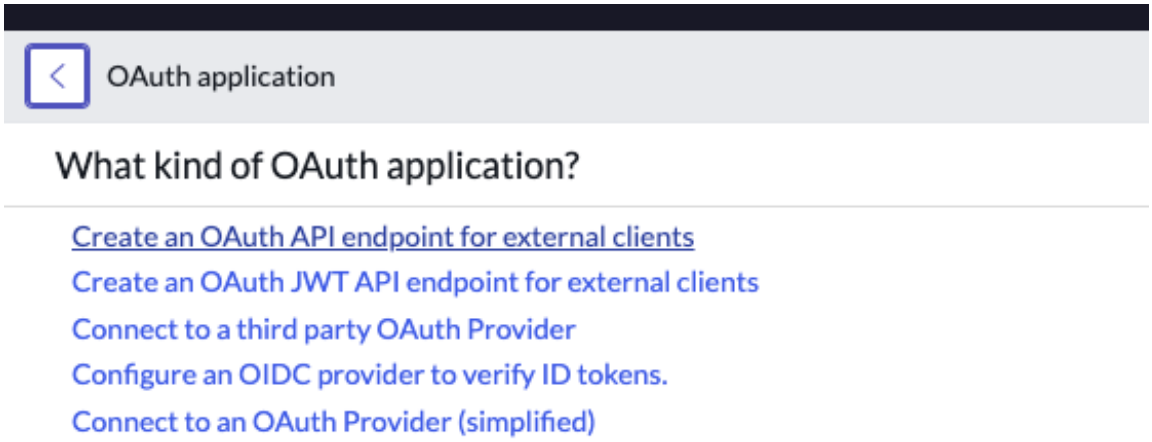
STEP 2 | 建立一個 Web OAuth 用戶端。

AIOps for NGFW 需要 OAuth 用戶端才能對您的 ServiceNow 執行個體進行身分驗證。

1. 導覽至 **System OAuth**（系統 **OAuth**）**> Application Registry**（應用程式登錄）。

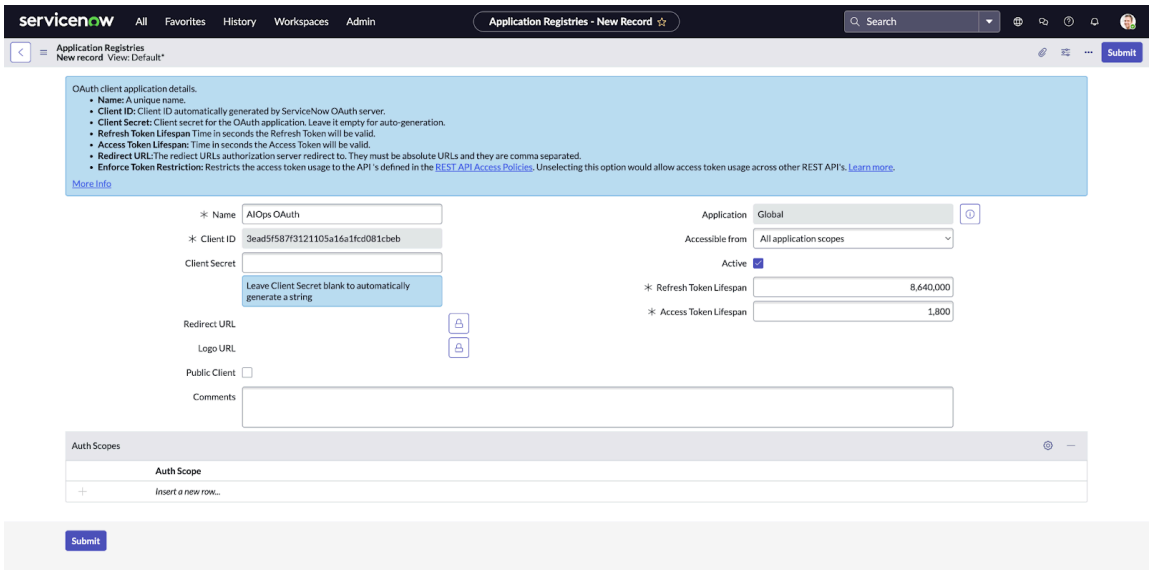


2. 建立一個新項目，並在以下頁面中選取 **Create an OAuth API endpoint for external clients**（為外部用戶端建立 **OAuth API** 端點）。



3. 為 OAuth 新增一個名稱並建立一個 **Client Secret**（用戶端密碼）。如果需要自動產生的密碼，則 **Client Secret**（用戶端密碼）也可以保留空白。按一下 **Submit**（提交），然後瀏覽回應用程式登錄項目，並將 **Client ID**（用戶端 **ID**）和 **Client Secret**（用戶端密

碼）儲存在安全的位置。此資訊會在 AIOps for NGFW 中的 **Client credential**（用戶端認證）表格下使用。



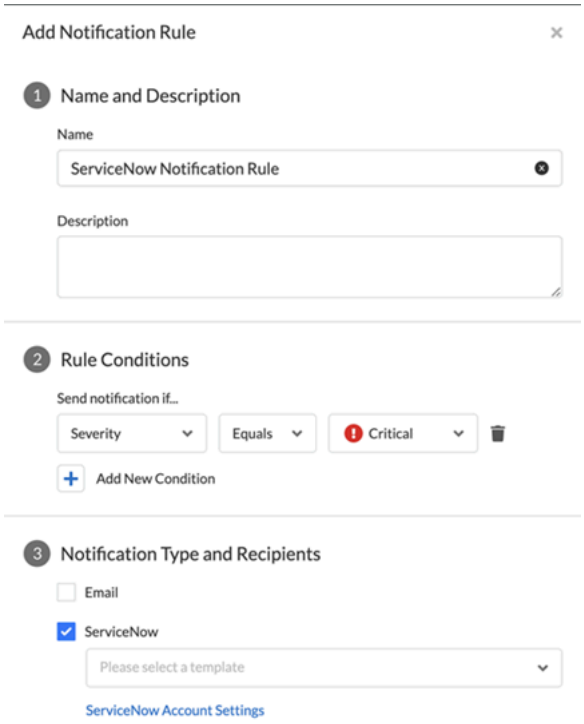
STEP 3 | 在 AIOps for NGFW 中新增 ServiceNow 帳戶設定資訊。

在 AIOps for NGFW 中新增先前步驟中的資訊，以完成 ServiceNow 與 AIOps for NGFW 之間的整合。

您必須執行下列操作：

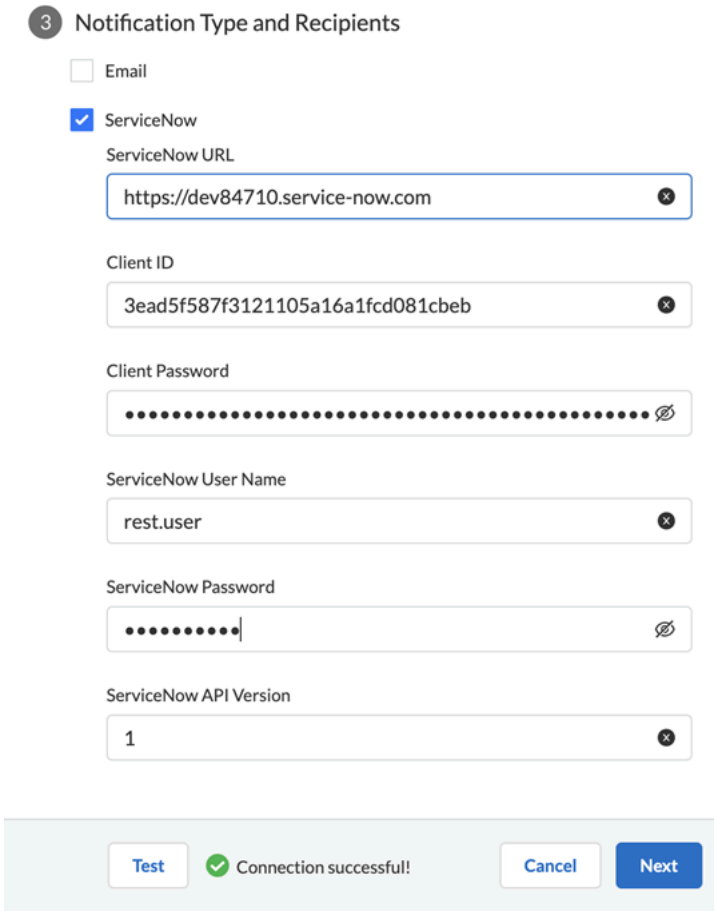
- **ServiceNow** 執行個體 **URL**
- 從步驟 1 開始的 **ServiceNow** 使用者和密碼
- 從步驟 2 開始的用戶端 **ID** 和用戶端密碼

1. 在 AIOps for NGFW 中，導覽至警示通知規則，然後按一下 [Add Notification Rule（新增通知規則）]。

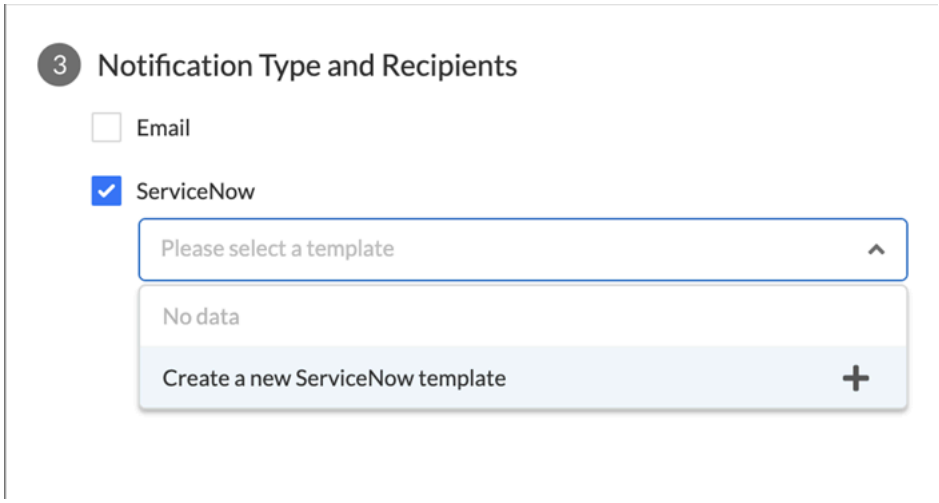


2. 填寫如 **Rule Name**（規則名稱）和 **Alert Condition**（警示條件）等欄位，然後按一下 **Notification Type and Recipients**（通知類型和收件者）下的 **ServiceNow** 核取方塊。
3. 按一下側邊欄底部的 [ServiceNow Account Settings（ServiceNow 帳戶設定）]。以先前儲存的資訊填寫以下表單。來自步驟 1 中設定 Rest User 的 **ServiceNow** 使用者 和 **ServiceNow** 密碼。來自步驟 2 中設定應用程式註冊的 用戶端 **ID** 和 用戶端密碼。將版本

保留不變。按一下 [Test（測試）]以儲存設定，並將測試事件發佈至 ServiceNow 執行個體。此步驟必須成功才能繼續。按一下 [Next（下一步）]。



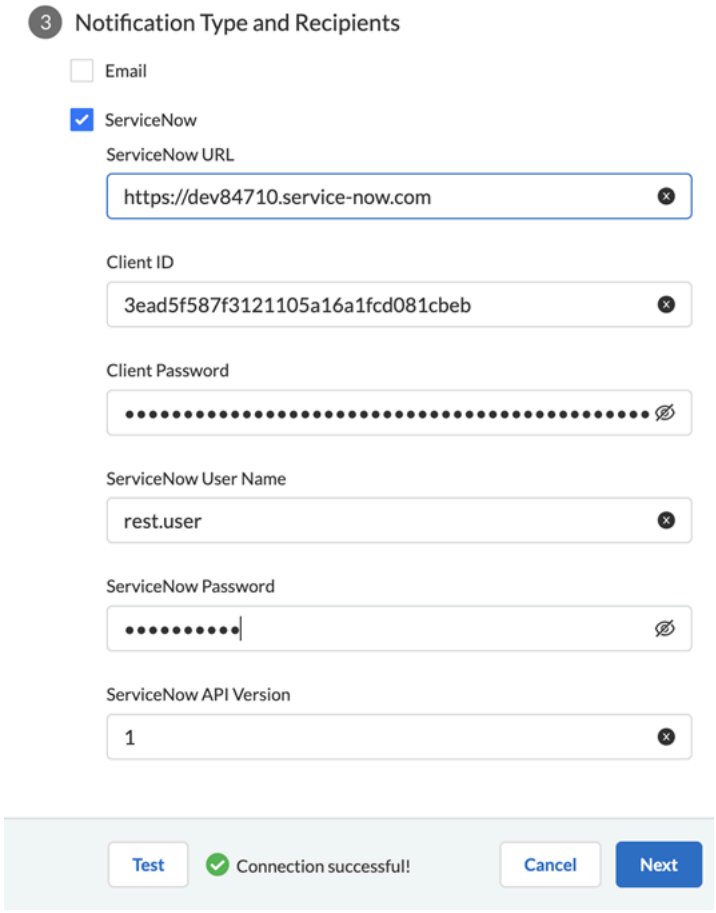
4. 展開 [Please select a template（請選取範本）] 下拉式清單，然後按一下 [Create a new ServiceNow Template（建立新的 ServiceNow 範本）]。



5. 輸入 **ServiceNow** 範本名稱，然後從 [Assignment Group（指派群組）] 下拉式清單中選擇群組。從 [Assignee（指派者）] 下拉式清單中選擇指派者。請注意，這些下拉式清單是透過從 ServiceNow 執行個體叫用下表來填入：

   - 系統安全性 > 使用者和群組 > 使用者
   - 系統安全性 > 使用者和群組 > 群組

   如果沒有定義群組，則 **Assignment Group**（指派群組）下拉式清單將不會填入。如果沒有使用者指定給特定群組，則 **Assignees**（指派者）下拉式清單將不會填入。按一下 **Next**（下一步），然後按一下 **Save Rule**（儲存規則）。



AIOps for NGFW 警示參考

歡迎使用 AIOps for NGFW 警示參考。健康情況的警示會主動即時監控您的平台健康情況和效能。這種方法有助於識別問題、預測潛在問題，以及實施補救措施，以確保您的裝置以最佳狀態運作。以下是一些關鍵方面：

- 監控指標：持續監控 NGFW 的各種指標，包括 CPU 使用率、記憶體使用量、磁碟空間、網路輸送量和其他相關效能指標。這種持續監控可確保任何偏離了正常效能的情況都能快速識別出來。
- 異常偵測：產生根據指標的歷史值和您的使用趨勢動態調整的警示。透過利用歷史資料，系統可以偵測可能指出潛在問題的異常情況，進而主動管理。
- 預測分析：透過分析歷史資料和模式，預測何時會超過某些閾值或何時會發生特定事件。這有助於在潛在問題升級之前先預測潛在問題。

下列頁面識別了 AIOps for NGFW 可顯示的警示。

- 進階健康情況警示：檢視 Strata Cloud Manager 可顯示與平台健康情況相關的進階警示。
- 免費健康情況警示：檢視 AIOps for NGFW 可顯示與平台健康情況相關的免費警示。
- 服務警示：檢視 AIOps for NGFW 可顯示與其連線服務相關的警示。
- 透過利用機器學習顯示的警示：檢視 Strata Cloud Manager 可透過利用機器學習來顯示的警示。

如需 AIOps for NGFW 可能顯示的安全性狀態檢查相關資訊，請瀏覽至**Manage**（管理）> **Security Posture**（安全性狀態）> **Settings**（設定）> **Security Checks**（安全性檢查）表格以查看檢查內容。

進階健康情況警示

下表識別了 Strata Cloud Manager 可顯示與您的平台健康情況相關的進階警示。

需要 AIOps for NGFW 進階授權，Strata Cloud Manager 才能顯示這些警示。

警示	說明
ACC 查詢失敗 （進階警示）	此警示可偵測應用程式控管中心 (ACC) 查詢是否失敗。 Class（類別）：健康情況 Category（類別）：報告 應用程式內支援票證：否。
逆向加密流量資源使用 （進階警示）	加密流量資源不足。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：否。
不良資源使用 （進階警示）	防火牆的每秒連線數 (CPS)、吞吐量或工作階段數量存在異常值。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：否。
接近最大容量 - ARP 表 （進階警示）	資料預測分析顯示 ARP 表項目即將達到防火牆的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 地址群組 （進階警示）	地址群組物件的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 位址物件 （進階警示）	位址物件的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能

警示	說明
	應用程式內支援票證：否。
接近最大容量 - 資料平面 CPU （進階警示）	資料平面 (DP) CPU 的使用率長時間持續較高，並且已接近裝置可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 解密使用情況 （進階警示）	資料預測分析顯示 SSL 解密工作階段即將達到防火牆的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - FQDN 位址 （進階警示）	FQDN 位址物件的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - GlobalProtect 通道（無用戶端） （進階警示）	無用戶端 GlobalProtect VPN 通道的數量正在接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - IKE 對等 （進階警示）	IKE 對等的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 管理平面 CPU （進階警示）	管理平面 (MP) CPU 使用率持續較高，並且已接近裝置可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。

警示	說明
接近最大容量 - 管理平面記憶體 （進階警示）	管理平面 (MP) 記憶體使用量持續較高，並且已接近裝置可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - NAT 政策 （進階警示）	NAT 政策規則的數量隨著時間持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 安全政策 （進階警示）	安全性政策規則的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 服務群組 （進階警示）	服務群組物件的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 服務物件 （進階警示）	服務物件的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 工作階段表使用率 （進階警示）	工作階段表的使用率 (%) 隨著時間持續較高，並且已接近防火牆或 VM 授權可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。

警示	說明
接近最大容量 - 站台對站台 VPN 通道 （進階警示）	由 IPsec 通道和 Proxy ID 組成的站台對站台 VPN 通道的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - EDL 內的 URL 或 IP （進階警示）	此防火牆的政策中使用的已設定 EDL 內的 URL、IP 或網域的數量正在接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：否。
接近最大容量 - 虛擬系統 （進階警示）	資料預測分析顯示虛擬系統設定即將達到防火牆授權支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大設定限制 （進階警示）	規則、群組和安全性設定檔等防火牆物件已接近裝置限制。 Class（類別）：健康情況 Category（類別）：設定限制 應用程式內支援票證：否。
憑證到期 （進階警示）	防火牆上的一或多個憑證已被撤銷或即將到期。 Class（類別）：健康情況 Category（類別）：憑證 應用程式內支援票證：否。
提交推送失敗 （進階警示）	設定推送失敗。 Class（類別）：健康情況 Category（類別）：組態設定 應用程式內支援票證：否。
設定記憶體使用量接近最大限制 （進階警示）	防火牆的設定正在接近其最大記憶體使用量限制。在提交期間，防火牆的設定記憶體總計必須容納兩個副本：目前的「使用中」設定和新的「待使用」設定。如果每個設定配置的記憶體超過 50%，防火牆就會達到容量限制，導致提交失敗。

警示	說明
	Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：否。
DP 封包丟棄 （進階警示）	警示偵測到不同原因導致的異常資封包丟棄 Class（類別）：健康情況 Category（類別）：效能 應用程式內支援票證：否。
HA 連結狀態 （進階警示）	連線至防火牆的連結運作狀況。防火牆連線至各種系統以提供各種服務。此警示提供這些連線的運作狀況。 Class（類別）：健康情況 Category（類別）：高可用性 應用程式內支援票證：否。
高日誌擷取率 （進階警示）	日誌收集器正在接近其支援的最大擷取率。 Class（類別）：健康情況 Category（類別）：記錄 應用程式內支援票證：否。
高日誌查詢活動 （進階警示）	日誌收集器已接近其查詢作業或報告的容量。 Class（類別）：健康情況 Category（類別）：記錄 應用程式內支援票證：否。
流量延遲增加 - 封包緩衝區 （進階警示）	裝置上的封包緩衝區資源不足。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：是
流量延遲增加 - 封包描述元 （進階警示）	裝置上的封包描述元資源不足。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：是

警示	說明
流量延遲增加 - 未知 TCP 或 UDP （進階警示）	防火牆接收到大量的流量，其應用程式被分類為未知 tcp 或未知 udp。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：否。
遺失與日誌轉送目的地的連線 （進階警示）	裝置無法連接到其日誌轉送目的地。 Class（類別）：健康情況 Category（類別）：記錄 應用程式內支援票證：否。
超過最短日誌保留期限 （進階警示）	日誌收集器包含的日誌超過定義的最短保留期限。 Class（類別）：健康情況 Category（類別）：記錄 應用程式內支援票證：否。
NAT 配置失敗 （進階警示）	至少一條 NAT 規則無法配置足夠的資源以進行轉換。 Class（類別）：健康情況 Category（類別）：NAT 集區資源 應用程式內支援票證：是
NAT 集區使用情況 （進階警示）	一或多條 NAT 規則的資源使用率較高。 Class（類別）：健康情況 Category（類別）：NAT 集區資源 應用程式內支援票證：否。
NGFW SD-WAN 應用程式效能警示 （進階警示）	指出受連線效能不佳影響的應用程式清單。 Class（類別）：健康情況 Category（類別）：SD-WAN 效能 應用程式內支援票證：否。
NGFW SD-WAN 連結效能警示 （進階警示）	指出導致應用程式和服務或連結效能降級的原因。 Class（類別）：健康情況 Category（類別）：SD-WAN 效能 應用程式內支援票證：否。

警示	說明
非預設記錄層級 （進階警示）	當服務的記錄層級未設定為其預設設定時，將觸發此警示。此警示可確保服務始終維護其指定的記錄設定。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：否。
PAN-OS 整合式 User-ID 代理程式監控伺服器已中斷連線 （進階警示）	當 PAN-OS 整合式 User-ID 代理程式（無代理 User-ID）監控的伺服器失去與防火牆的連線時，會觸發此警示。此受監控伺服器是將使用者身分對應到網路活動的關鍵元件。 Class（類別）：健康情況 Category（類別）： 應用程式內支援票證：否。
政策設定記憶體使用量接近最大限制 （進階警示）	此警示會偵測政策設定記憶體使用量是否超過關鍵閾值。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：否。
流量延遲 - 封包描述元（晶片上） （進階警示）	裝置上的封包描述元（晶片上）資源不足。 Class（類別）：健康情況 Category（類別）：洪水/DoS 應用程式內支援票證：否。
通道關閉 （進階警示）	一或多個站台對站台 VPN 通道已關閉。 Class（類別）：健康情況 Category（類別）：站台對站台 VPN 應用程式內支援票證：是
區域保護設定檔 - 洪水偵測 （進階警示）	在區域上建立的連線數量或傳入封包的速率過高或異常。 Class（類別）：健康情況 Category（類別）：洪水/DoS 應用程式內支援票證：是
區域保護設定檔 - 閾值建議 （進階警示）	某個區域缺少區域保護設定檔，或區域保護設定檔中的閾值需要調整。 Class（類別）：健康情況

警示	說明
	Category（類別）：洪水/DoS 應用程式內支援票證：否。

免費健康情況警示

下表識別了 AIOps for NGFW 可顯示與平台健康情況相關的免費警示。

AIOps for NGFW 不需要進階授權也能顯示這些警示。

警示	說明
卡片電源故障 （免費警示）	已偵測到卡片故障，表示該卡片或其在底座內的位置可能出現問題。 Class（類別）：健康情況 Category（類別）：硬體 應用程式內支援票證：否。
設定大小達到裝置容量限制 （免費警示）	此裝置的設定大小已達到其容量限制。 Class（類別）：健康情況 Category（類別）：組態設定 應用程式內支援票證：否。
降級的系統磁碟機 （免費警示）	透過監控其屬性值來識別降級的系統磁碟機。 Class（類別）：健康情況 Category（類別）：硬體 應用程式內支援票證：否。
延遲遙測 （免費警示）	分析引擎沒有來自此 NGFW/Panorama 的新遙測。 Class（類別）：健康情況 Category（類別）：遙測 應用程式內支援票證：是
FE100 失敗 （免費警示）	在防火牆中的 FE100 晶片上偵測到校正錯誤。此問題通常表示硬體故障。 Class（類別）：健康情況 Category（類別）：硬體 應用程式內支援票證：否。
風扇問題 （免費警示）	風扇或風扇托盤在裝置上觸發警報。 Class（類別）：健康情況 Category（類別）：硬體

警示	說明
	應用程式內支援票證：否。
嚴重機器檢查失敗 （免費警示）	偵測到嚴重機器檢查失敗。此問題通常表示 CPU 中有硬體故障。 Class（類別）：健康情況 Category（類別）：硬體 應用程式內支援票證：否。
防火牆與 Cortex 資料湖已中斷連接 （免費警示）	FW 與 Strata Logging Service 之間的連線已中斷。 Class（類別）：健康情況 Category（類別）：SLS 連線 應用程式內支援票證：否。
防火牆與 Panorama 已中斷連線 （免費警示）	防火牆與 Panorama 之間的連線已中斷。 Class（類別）：健康情況 Category（類別）：連線失敗 應用程式內支援票證：否。
HA 備份 （免費警示）	目前尚未設定 HA 備份連結。 Class（類別）：健康情況 Category（類別）：高可用性 應用程式內支援票證：否。
HA 對等連線狀態 （免費警示）	HA 配對中的其中一個防火牆處於非健康狀態。 Class（類別）：健康情況 Category（類別）：高可用性 應用程式內支援票證：是
高磁碟空間使用量 - Pancfg 分割區 （免費警示）	硬碟分割區接近或達到容量限制。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：是
高磁碟空間使用量 - Panlogs 分割區 （免費警示）	硬碟分割區接近或達到容量限制。 Class（類別）：健康情況 Category（類別）：資源使用情況

警示	說明
	應用程式內支援票證：是
高磁碟空間使用量 - 根分割區 （免費警示）	硬碟分割區接近或達到容量限制。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：是
高處理活動 （免費警示）	裝置上的一或多個運算資源不足。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：否。
IPQ 錯誤 （免費警示）	在防火牆中的其中一個 FE100 晶片上偵測到 IPQ（進入封包佇列）錯誤。此錯誤通常表示需要重新裝設，或存在硬體錯誤。 Class（類別）：健康情況 Category（類別）：硬體 應用程式內支援票證：否。
不規則的輸入電源 （免費警示）	裝置的電源水平超出正常範圍。 Class（類別）：健康情況 Category（類別）：硬體 應用程式內支援票證：否。
授權到期 （免費警示）	您的一或多個授權已快要到期或已到期。 Class（類別）：健康情況 Category（類別）：PanOS 和訂閱 應用程式內支援票證：否。
記錄磁碟機失敗 （免費警示）	透過監控防火牆的磁碟狀態，已識別失敗的記錄磁碟機。 Class（類別）：健康情況 Category（類別）：硬體 應用程式內支援票證：否。
MPC 卡 - CPLD 失敗 （免費警示）	管理處理器卡 (MPC) 是 PA-5450 的重要元件，提供管理、記錄和高可用性功能。MPC 卡因其元件複雜可程式化邏輯裝置 (CPLD) 出現問題而發生故障。 Class（類別）：健康情況

警示	說明
	Category（類別）：硬體 應用程式內支援票證：否。
NGFW/Panorama 管理憑證到期 （免費警示）	此警示偵測到 NGFW/Panorama 管理憑證已過期。 Class（類別）：健康情況 Category（類別）：憑證 應用程式內支援票證：否。
NPC 卡 - FE100 故障 （免費警示）	網路處理卡 (NPC) 提供網路連線能力，並且對網路流量處理至關重要。NPC 卡已遭遇其 FE100 元件的問題，導致其發生故障。 Class（類別）：健康情況 Category（類別）：硬體 應用程式內支援票證：否。
不同步對等 - 設定 （免費警示）	高可用性對等上的系統設定不相符。 Class（類別）：健康情況 Category（類別）：高可用性 應用程式內支援票證：否。
不同步對等 - 動態內容 （免費警示）	動態內容（例如防毒軟體或應用程式與威脅）在高可用性對等之間不相符。 Class（類別）：健康情況 Category（類別）：高可用性 應用程式內支援票證：否。
不同步對等 - 工作階段 （免費警示）	高可用性對等之間的工作階段不相符或不是最新的。 Class（類別）：健康情況 Category（類別）：高可用性 應用程式內支援票證：否。
不同步對等 - 軟體 （免費警示）	高可用性對等的 PAN-OS 軟體版本不相符。 Class（類別）：健康情況 Category（類別）：高可用性 應用程式內支援票證：否。
過時的動態內容	與更新伺服器上可用的內容相比，裝置上安裝的動態內容已過時。

警示	說明
（免費警示）	Class（類別）：健康情況 Category（類別）：動態內容 應用程式內支援票證：否。
PAN-OS 生命週期結束 （免費警示）	不再支援目前版本的 PAN-OS。 Class（類別）：健康情況 Category（類別）：PanOS 和訂閱 應用程式內支援票證：否。
PAN-OS 已知弱點 （免費警示）	目前版本的 PAN-OS 具有已知弱點。 Class（類別）：健康情況 Category（類別）：動態內容 應用程式內支援票證：否。
PAN-OS 根和預設憑證到期 - 案例 1 （免費警示）	防火牆上的根憑證和預設憑證已過期。 Class（類別）：健康情況 Category（類別）：憑證 應用程式內支援票證：否。
PCI 錯誤 （免費警示）	周邊元件互連 (PCI) 負責將管理平面 (MP) 連線至控制平面 (CP)。與此元件相關的某些錯誤表示其功能出現故障。 Class（類別）：健康情況 Category（類別）：硬體 應用程式內支援票證：否。
路徑監控錯誤 - 卡片 （免費警示）	在位於防火牆插槽內的卡片上偵測到路徑監控失敗。 Class（類別）：健康情況 Category（類別）：硬體 應用程式內支援票證：否。
連接埠失敗 （免費警示）	已偵測到與管理實體連接埠或其中一個高可用性實體連接埠相關的故障。 Class（類別）：健康情況 Category（類別）：硬體 應用程式內支援票證：否。

警示	說明
處理程序記憶體耗盡 - 設定 （免費警示）	裝置的管理平面處理程序正在耗盡其可用的記憶體。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：是
程序記憶體耗盡 - 裝置伺服器 （免費警示）	裝置的管理平面處理程序正在耗盡其可用的記憶體。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：是
處理記憶體耗盡 - 記錄接收器 （免費警示）	裝置的管理平面處理程序正在耗盡其可用的記憶體。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：是
處理記憶體耗盡 - 管理伺服器 （免費警示）	裝置的管理平面處理程序正在耗盡其可用的記憶體。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：是
程序記憶體耗盡 - 使用者 ID （免費警示）	裝置的管理平面處理程序正在耗盡其可用的記憶體。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：是
備援電源供應器故障 （免費警示）	由於未插入電源、電源供應器發生故障，或未完成完整備援，因此無法實現電源供應器備援。 Class（類別）：健康情況 Category（類別）：硬體 應用程式內支援票證：是
Strata Logging Service 日誌轉送延遲 （免費警示）	Strata Logging Service 的轉送延遲超出可接受的值。 Class（類別）：健康情況 Category（類別）：SLS 健康情況 應用程式內支援票證：否。

警示	說明
Strata Logging Service 日誌離線轉送 （免費警示）	Strata Logging Service 日誌轉送服務無法正常運作 Class（類別）：健康情況 Category（類別）：SLS 健康情況 應用程式內支援票證：否。
Strata Logging Service 日誌擷取延遲 （免費警示）	Strata Logging Service 的擷取延遲超出可接受的值。 Class（類別）：健康情況 Category（類別）：SLS 健康情況 應用程式內支援票證：否。
Strata Logging Service 日誌離線擷取 （免費警示）	Strata Logging Service 擷取服務無法正常運作。 Class（類別）：健康情況 Category（類別）：SLS 健康情況 應用程式內支援票證：否。
Strata Logging Service 日誌儲存空間接近限制 （免費警示）	記錄類型接近設定的最大儲存空間限制。 Class（類別）：健康情況 Category（類別）：記錄 應用程式內支援票證：否。
過熱問題 （免費警示）	裝置溫度超出正常範圍。 Class（類別）：健康情況 Category（類別）：硬體 應用程式內支援票證：否。

服務警示

下表識別了 AIOps for NGFW 可顯示的與其服務連線相關的警示。

警示	說明
防火牆與 Strata Logging Service 已中斷連線 （免費警示）	FW 與 SLS 之間已連線中斷超過 5 分鐘。 Category（類別）：SLS 連線 應用程式內支援票證：否。
Strata Logging Service 日誌離線擷取 （免費警示）	SLS 擷取服務無法運作的時間超過 5 分鐘。 Category（類別）：SLS 健康情況 應用程式內支援票證：否。
Strata Logging Service 日誌離線轉送 （免費警示）	SLS 日誌轉送服務無法運作的時間超過 5 分鐘。 Category（類別）：SLS 健康情況 應用程式內支援票證：否。
Strata Logging Service 日誌擷取延遲 （免費警示）	過去 15 分鐘內 SLS 的擷取延遲超過 10 分鐘。 Category（類別）：SLS 健康情況 應用程式內支援票證：否。
Strata Logging Service 日誌轉送延遲 （免費警示）	過去 15 分鐘內 SLS 的轉送延遲超過 10 分鐘。 Category（類別）：SLS 健康情況 應用程式內支援票證：否。
Strata Logging Service 日誌儲存空間接近限制 （免費警示）	記錄類型接近設定的最大儲存空間限制。 Category（類別）：記錄 應用程式內支援票證：否。

透過利用機器學習顯示警示

下表列出了 AIOps for NGFW 可以透過利用機器學習顯示的警示。

警示	說明
逆向加密流量資源使用 （進階警示）	加密流量資源不足。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：否。 偵測類型：異常
不良資源使用 （進階警示）	防火牆的每秒連線數 (CPS)、吞吐量或工作階段數量存在異常值。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：否。 偵測類型：異常
接近最大設定限制 （進階警示）	規則、群組和安全性設定檔等防火牆物件已接近裝置限制。 Class（類別）：健康情況 Category（類別）：設定限制 應用程式內支援票證：否。 偵測類型：異常
高處理活動 （免費警示）	裝置上的一或多個運算資源不足。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：否。
流量延遲增加 - 封包緩衝區 （進階警示）	裝置上的封包緩衝區資源不足。 Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：是 偵測類型：異常
流量延遲增加 - 封包描述元	裝置上的封包描述元資源不足。

警示	說明
（進階警示）	Class（類別）：健康情況 Category（類別）：資源使用情況 應用程式內支援票證：是 偵測類型：異常
流量延遲 - 封包描述元（晶片上） （進階警示）	裝置上的封包描述元（晶片上）資源不足。 Class（類別）：健康情況 Category（類別）：洪水/DoS 應用程式內支援票證：否。 偵測類型：異常
接近最大容量 - ARP 表 （進階警示）	資料預測分析顯示 ARP 表項目即將達到防火牆的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 地址群組 （進階警示）	地址群組物件的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 位址物件 （進階警示）	位址物件的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 資料平面 CPU （進階警示）	資料平面 (DP) CPU 的使用率長時間持續較高，並且已接近裝置可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 解密使用情況	資料預測分析顯示 SSL 解密工作階段即將達到防火牆的最大容量。

警示	說明
（進階警示）	Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - FQDN 位址 （進階警示）	FQDN 位址物件的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - GlobalProtect 通道（無用戶端） （進階警示）	無用戶端 GlobalProtect VPN 通道的數量正在接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - IKE 對等 （進階警示）	IKE 對等的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 管理平面 CPU （進階警示）	管理平面 (MP) CPU 使用率持續較高，並且已接近裝置可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 管理平面記憶體 （進階警示）	管理平面 (MP) 記憶體使用量持續較高，並且已接近裝置可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - NAT 政策 （進階警示）	NAT 政策規則的數量隨著時間持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況

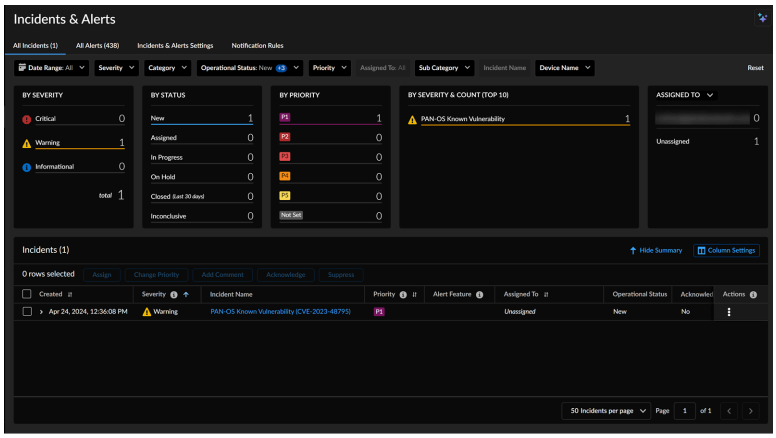
警示	說明
	Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 安全政策 （進階警示）	安全性政策規則的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 服務群組 （進階警示）	服務群組物件的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 服務物件 （進階警示）	服務物件的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 工作階段表使用率 （進階警示）	工作階段表的使用率 (%) 隨著時間持續較高，並且已接近防火牆或 VM 授權可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 虛擬系統 （進階警示）	資料預測分析顯示虛擬系統設定即將達到防火牆授權支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能 應用程式內支援票證：否。
接近最大容量 - 站台對站台 VPN 通道 （進階警示）	由 IPsec 通道和 Proxy ID 組成的站台對站台 VPN 通道的數量持續較高，並且已接近防火牆可以支援的最大容量。 Class（類別）：健康情況 Category（類別）：功能

警示	說明
	應用程式內支援票證：否。
NGFW SD-WAN 應用程式效能警示 （進階警示）	指出受連線效能不佳影響的應用程式清單。 Class（類別）：健康情況 Category（類別）：SD-WAN 效能 應用程式內支援票證：否。 偵測類型：異常
NGFW SD-WAN 連結效能警示 （進階警示）	指出導致應用程式和服務或連結效能降級的原因。 Class（類別）：健康情況 Category（類別）：SD-WAN 效能 應用程式內支援票證：否。 偵測類型：異常

管理 NGFW 事件

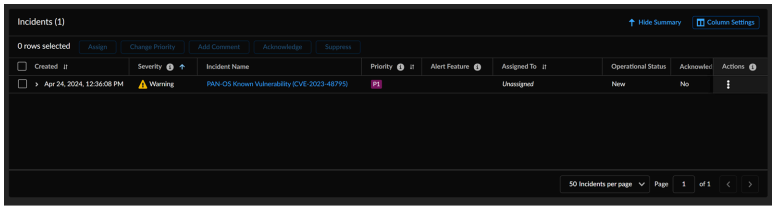
我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或者 ❑ 或者

透過選取 **Incidents & Alerts**（事件和警示） > **NGFW** > **All Incidents**（所有事件）來取得 NGFW 事件的鳥瞰圖。瀏覽事件頁面，讓您隨時了解部署中的變更，讓您可以調查這些變更並在必要時採取預防措施。您可以直接存取詳細的事件清單以及關鍵的視覺化摘要。您還可以 **Hide Summary**（隱藏摘要）以隱藏 Widget並僅以表格格式查看事件。



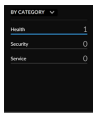
以下是 **All Incidents**（所有事件）下顯示的資料。

- **Incidents**（事件）：顯示所有事件。



  在此表中，您可以執行下列任務：

  - 隱藏摘要以隱藏 Widget並僅以表格格式查看事件。
  - 展開事件以查看其說明和影響。
  - 在 [Actions（動作）] 下方，您可以執行以下動作：
    - 指派事件給使用者、您自己，或取消指派事件。
    - 變更事件的優先順序或選取 [Not Set（未設定）] 以移除優先順序。
    - 透過選取 [Yes（是）] 來確認事件，確認您已看到該事件。
    - 當您不打算主動解決事件時，抑制功能會將事件設為「保留」作業狀態。
    - 為事件新增註解。
  - 按一下事件以檢視其詳細資訊。
  - 使用欄設定檢視或隱藏事件的特定欄，並重新排列欄的預設順序。這些變化會在未來的工作階段中持續存在。
- 指派給：顯示按負責解決事件的個人或實體劃分的事件數。在頂部，它顯示指派給目前登入使用者的事件和未指派的事件。您也可以透過在下拉式清單中選取 [BY CATEGORY（依類別）]來檢視事件數量。



- 依嚴重性和計數（前 **10** 名）：顯示依嚴重性分類的事件，以及每個類別中的事件計數。首先優先考慮嚴重事件，其次是警告事件，最後是資訊事件。

- 依狀態：依狀態顯示事件總數。
  - 「新增」表示尚未指派的事件。
  - 「已指派」表示已指派至使用者的事件。
  - 「進行中」表示該事件正在處理中。
  - 「保留」表示您不打算主動解決該事件。
  - 「已關閉」表示過去 30 天內已關閉的事件。
  - 「不明」表示這些事件沒有解決方案。

- 依嚴重性：顯示分類為「嚴重」、「警告」和「資訊」的事件總數。

- 依優先順序：根據事件的優先順序顯示事件，其中 P1 是最嚴重的事件。

檢視事件詳細資訊

我可以在哪裡使用這個？	我需要哪些內容？
• ，包括由軟體 NGFW 積分資助的項目	其中一個： ❑ 或者 ❑ 或者

從 **All Incidents**（所有事件）中，您可以選取一個事件來開啟包含其詳細資訊的頁面。**Summary**（摘要）標籤顯示以下詳細資訊：

1. 事件摘要及詳細資訊。您可以變更事件的優先順序或將其指派給使用者。
2. 事件造成的影響，亦即受影響的 NGFW 數量。
3. 建議採取的動作來解決您的問題。

您也可以按一下 CVE 以檢視 Palo Alto Networks 安全公告中的詳細資訊以及 PAN-OS 版本中的弱點。

Correlated Alerts & Activity（相關警示和活動）標籤顯示以下詳細資訊：

- 所選事件的相關警示
- 事件的記錄活動