paloalto TECHDOCS

NGFW 事件和警报

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

警报

在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 、 ❑ 或

为了帮助您维持设备的持续运行状况并避免业务中断事件，AIOps for NGFW 会根据其在防火墙部署中检测到的一个或多个问题生成警报。这些问题或事件是通过以下三种方式之一触发的：

- 当指标发生重大变化时
- 当先前生成的事件发生变化时
- 当用户或系统执行某项操作时，例如确认或关闭警报

警报表示需要解决的特定问题（防火墙功能降级或丧失）。也可以根据多个事件的关联或聚合来生成警报。通过将事件聚合到单个警报中，有助于分类警报、简化团队之间的警报移交流程、集中关键信息并减轻通知疲劳。

根据与警报关联的指标，将警报分为不同的类别。您可以使用警报类别来指定接收通知的警报种类。例如，硬件、配置限制、资源限制、动态内容以及 PAN-OS 和订阅。

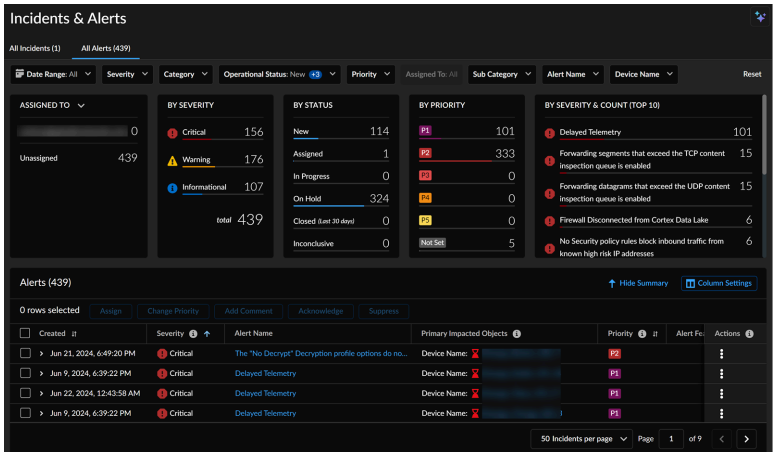
在 **Incidents & Alerts**（事件和警报） > **NGFW** > **All Alerts**（所有警报）中，您可以查看并管理为部署生成的所有警报。在 **Notification Rules**（通知规则）中，您可以配置通知规则，指定在事件触发警报时您希望何时以及如何收到通知。

- 管理 NGFW 警报
- 查看警报详细信息
- 查看可能的原因
- 预测和异常检测
- 管理 Capacity Analyzer 警报
- AIOps for NGFW 中的 CPU 使用率指标
- 创建通知规则
- 与 ServiceNow 集成

管理 NGFW 警报

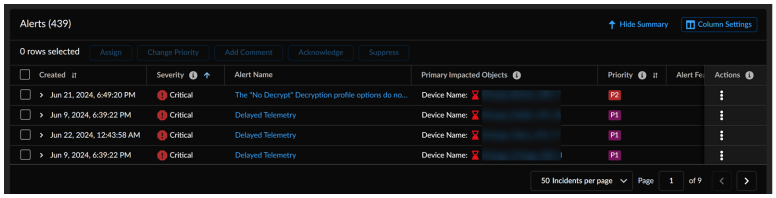
在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 、 ❑ 或

选择 **Incidents & Alerts**（事件和警报） > **NGFW** > **All Alerts**（所有警报），以获取 NGFW 警报的鸟瞰视图。浏览警报页面，帮助您维持设备和部署的持续运行状况，避免业务中断。您可以直接访问警报的详细列表以及关键的可视化摘要。您还可以 **Hide Summary**（隐藏摘要），以隐藏小部件并仅以表格格式查看警报。



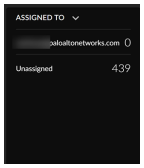
以下是 **All Alerts**（所有警报）下显示的数据。

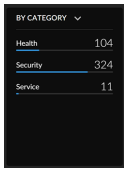
- 警报：显示所有警报。



  在此表中，您可以执行以下任务：

  - **Hide Summary**（隐藏摘要）以隐藏小部件并仅以表格格式查看警报。
  - 展开警报以查看其描述和影响。
  - 在“Actions（操作）”下，您可以执行以下操作：
    - 将警报分配给用户、自己，或者取消分配警报。
    - 更改警报的优先级或选择“Not Set（未设置）”以删除优先级。
    - 选择 **Yes**（是）以确认警报，确认您看到了该警报。
    - 当您不打算主动解决警报时，通过阻止将事件设置为"搁置"运行状态。
    - 为警报添加注释。
  - 单击警报以查看其详细信息。
  - 使用 **Column Settings**（列设置）查看或隐藏警报的特定列，并重新排列这些列的默认顺序。这些更改将在未来的会话中保留。
- 分配对象：显示分配给负责解决警报的个人或实体的警报数量。顶部显示分配给当前登录用户的警报和未分配的警报。您也可以在下拉列表中选择 **BY CATEGORY**（按类别）来查看警报数量。





- 按严重性和计数分类（前 **10** 个）：显示按严重性分类的警报，以及每个类别中的警报计数。严重警报的优先级最高，其次是警告警报，然后是信息警报。

- 按状态分类：按状态显示警报总数。
  - “New（新建）”表示未分配的事件。
  - “Assigned（已分配）”表示已分配给用户的事件。
  - “In Progress（进行中）”表示正在处理此事件。
  - “On Hold（搁置）”表示您不打算主动解决警报。
  - “Closed（已关闭）”表示最近 30 天内关闭的警报。
  - “Inconclusive（没有定论）”表示这些警报没有解决办法。

- 按严重性分类：显示归类为“严重”、“警告”和“信息”的警报总数。

- 按优先级分类：显示按照优先级分类的警报，其中 P1 表示程度最为严重。

查看警报详细信息

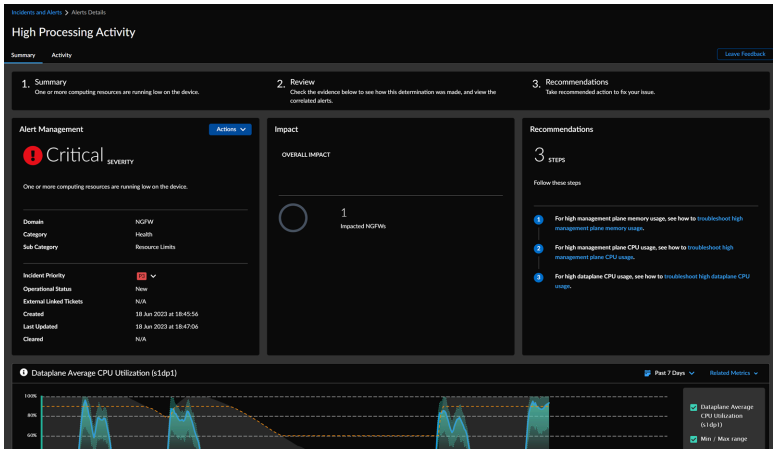
在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 、 ❑ 或

在 **All Alerts**（所有警报）中，您可以选择一个警报，然后会打开一个页面，其中包含有关该警报的详细信息。**Summary**（摘要）选项卡显示以下详细信息：

1. 包含详细信息的警报摘要。您可以更改警报的优先级或将其分配给用户。
2. 警报造成的影响，即受影响的 NGFW 数量。
3. 用于解决问题的补救措施建议和资源。

您还可以查看贡献事件的图表。

Activity（活动）选项卡显示警报的记录活动。



查看可能的原因

在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	❑ 或

使用高级 AI 功能时，AIOps for NGFW 会显示警报的可能原因，并提供有关如何解决潜在问题的建议。此功能通过减少中断并最大限度地提高网络安全解决方案的有效性来确保实现最佳网络性能。

以下是支持可能原因分析的警报：

- 大量处理活动
- 流量延迟增加 - 数据包缓冲区
- 流量延迟增加 - 数据包描述符（片上）
- 允许的威胁
- 流量延迟 - 数据包描述符（片上）
- 资源使用情况不利
- 不同步对等体 - 配置
- 潜在的凭据盗窃滥用
- 提交推送失败

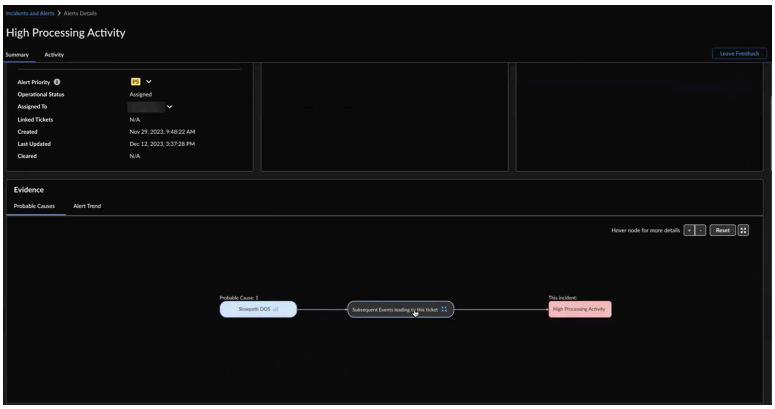
可能的原因分析得到增强，可使用 Strata Logging Service 日志并为导致创建警报或事件的可能原因提供其他元数据。此增强功能允许您精确定位可能导致警报的策略、应用程序、源区域、URL、源 IP 和区域。

您可以查看以下场景的可能原因：

- 大量处理活动（大量处理活动警报）：当数据平面 CPU 使用率较高时，可能会导致各种问题，例如防火墙不稳定、防火墙处于挂起或卡住状态，以及数据包丢失或延迟问题。这可能会对您的业务运营产生负面影响。如果数据平面 CPU 使用率至少为 60%，并且使用率大幅飙升，AIOps for NGFW 将在大量处理活动警报中显示可能的原因。但是，如果数据平面 CPU 使用率长时间保持在较高水平且没有任何变化，则原因将不明确且无法轻易确定，因此不会显示任何可能的原因。例如，如果数据平面 CPU 使用率在较长时间内始终保持在 70%，则 AIOps for NGFW 不会显示任何可能的原因。
- 单个或多个贪婪会话检测和修复（大量处理活动警报）：防火墙上的贪婪会话攻击是指攻击者快速创建大量连接，利用防火墙的内部资源，从而导致资源耗尽和拒绝服务 (DoS) 事件。AIOps for NGFW 可以检测这些问题并显示可能的原因。
- 会话耗尽与连接丢失（大量处理活动警报）：当防火墙接收流量时，它会为该流量建立会话以跟踪其状态并执行必要的安全检查。每个会话都会消耗系统资源，包括内存和 CPU 周期。如果防火墙达到并发会话数的最大容量，将导致会话耗尽。出现此问题的原因有多种，包括流量大、安全策略配置错误以及会话超时设置不正确。AIOps for NGFW 利用先进的 AI 功能主动检测网络设备中的会话耗尽问题。这样可以优化资源分配，提升网络性能并缓解连接问题，以确保不间断的服务可用性。

- 由于单个应用程序而导致的高数据包缓冲区利用率（流量延迟增加 - 数据包缓冲区）：AIOps for NGFW 检测到由于单个应用程序独占数据包缓冲区而导致的高数据包缓冲区利用率的可能根本原因。AIOps for NGFW 利用先进的 AI 功能，及时提醒资源分配不理想并防止性能下降，从而确保实现最佳网络性能。
- 由于单个应用程序而导致的高片上数据包描述符利用率 （流量延迟增加 - 数据包描述符（片上））：AIOps for NGFW 可检测片上数据包描述符利用率高的可能根本原因。这有助于主动识别和解决由单个应用程序独占片上数据包描述符而引起的网络拥塞。
- 慢速路径 **DoS** 攻击检测和修复（大量处理活动警报）：AIOps for NGFW 使用 AI 支持的技术来检测慢速路径 DoS 攻击，以确保网络安全和不间断的服务可用性。它执行大量数据平面处理活动警报、大量策略拒绝活动根本原因分析以及基于因果关系分析的修复建议。
- 大量 **URL** 缓存查找活动检测和修复（大量处理活动警报）：AIOps for NGFW 可检测并解决大量 URL 缓存查找活动，从而优化处理效率并保持系统稳定性。此功能将 URL 缓存查找活动与 DP CPU 利用率相关联，识别高 CPU 使用率，并提供修复建议以防止接近饱和的情况。
- 大量内容处理活动检测和修复（大量处理活动警报）：AIOps for NGFW 可检测大量内容处理活动。此功能可分析各个内容处理阶段与数据平面 CPU 利用率之间的相关性，识别 CPU 使用率高或接近饱和的情况，并提供可行的修复建议以提高系统稳定性。
- 证书过长 **RCA** 报告（提交推送失败警报）：AIOps for NGFW 可检测到提交失败并概述提交失败的潜在原因，特别是当证书长度超过缓冲区大小时。

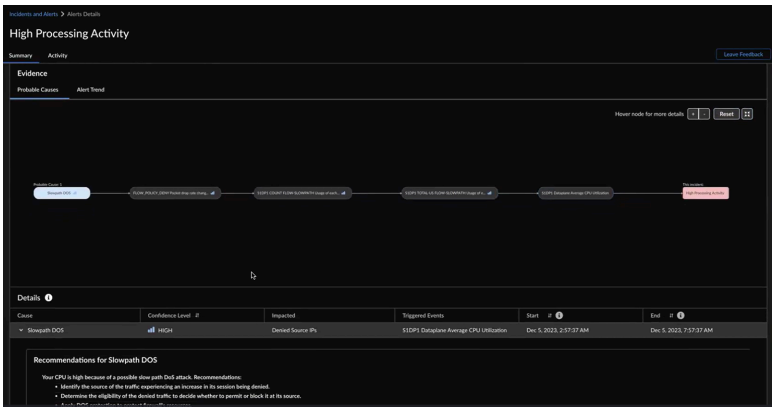
STEP 1 | 在 **Incidents & Alerts**（事件和警报）> **Alerts**（警报）中，您可以选择一个警报，然后会打开一个页面，其中包含有关该警报的详细信息。



流程图表示：

- 触发大量处理活动警报的事件
- 触发事件的可能原因

您还可以将光标悬停在节点上以查看更多详细信息，例如可能的原因、置信度、触发的事件和影响的持续时间。每当有三个或更多事件节点时，您可以单击并展开事件以查看详细信息。



AIOps for NFGW 也以表格格式显示相同的信息。您可以将光标悬停在表中的可能原因上，以查看流程图中突出显示的节点和路径。您还可以单击流程图中的可能原因，以表格格式查看其详细信息。

Confidence Level（置信度级别）表示 AIOps for NGFW 如何识别大量处理活动警报的原因。可能的原因按置信度级别降序排列。您可以先查看置信度级别较高的原因。

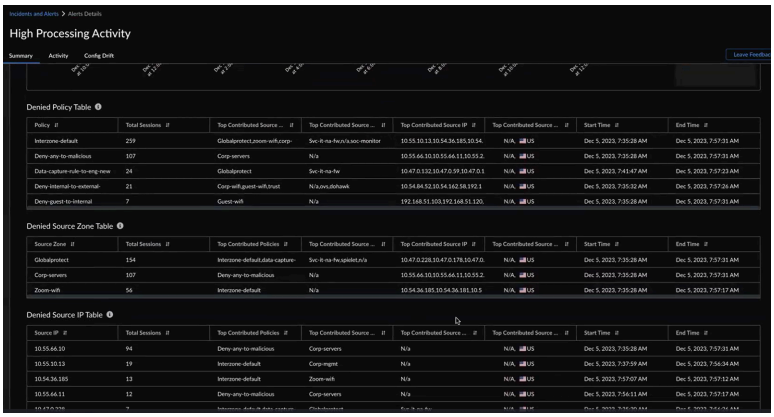
STEP 2 | 展开表中的可能原因，以查看您想要调查的触发警报的图表和受影响的指标。

STEP 3 | 使用图表工具检查图表。

因果关系期限使您能够直观地看到随着时间的推移警报的 **Cause**（原因）原因和 **Triggered Event**（触发时间）和触发事件之间的因果关系。

您可以在图表中查看影响前后 6 小时、24 小时或 48 小时的情况。

可能的原因分析功能已得到增强，可使用 SLS 日志并为导致创建警报或事件的可能原因提供额外的元数据。此增强功能允许您精确定位可能导致警报的策略、应用程序、源区域、URL、源 IP 和区域。例如，当高数据平面 CPU 使用率触发 **High Processing Activity**（大量处理活动）警报时，您可以利用可能的原因分析来确定触发警报的主要因素，并遵循修复建议。



预测和异常检测

在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 、 ❑ 或

通常情况下，AIOps for NGFW 通过将固定规则应用于部署中的指标来检测问题。例如，如果管理平面 CPU 使用率超过 85%，则该指标进入临界状态。

但是，为了提醒您固定规则可能遗漏的事件，AIOps for NGFW 可以使用机器学习来了解您的部署，并根据您的使用情况趋势为您提供额外的警报和事件。

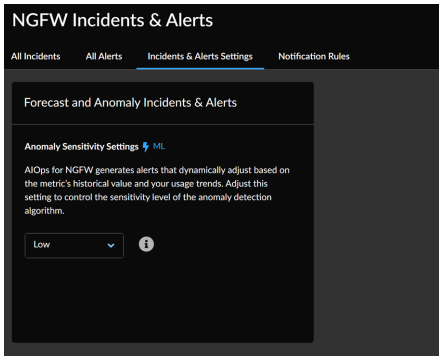
- **Forecast-Based Alerts**（基于预测的警报）通过预测设备指标可能如何变化并相应地向您发出警报，从而帮助您预测问题。
- **Anomaly-Based Alerts**（基于异常的警报）为设备指标建立基线行为，并在该指标超过您指定的 **Anomaly Sensitivity Settings**（异常敏感度设置）时向您发出警报。

预测和异常检测具有以下优势：

- 主动管理：通过预测潜在问题并尽早发现异常，管理员可以采取主动措施来预防问题，从而减少停机时间并提高整体网络性能。
- 增强的安全性：检测异常模式和行为有助于识别安全威胁和漏洞，从而及时采取干预和缓解措施。
- 优化的资源：预测有助于更好地规划和分配资源，确保网络基础设施做好充分的准备应对未来的需求。

导航到 **Incidents & Alerts**（事件和警报） > **Incident & Alert Settings**（事件和警报设置） > **Forecast and Anomaly Incidents & Alerts**（预测和异常事件和警报）。

AIOps for NGFW 会生成根据指标的历史值和使用情况趋势动态调整的警报和事件。偏离正常范围可能表示存在潜在问题。您可以调整此设置来控制异常检测算法的敏感度级别。



管理 Capacity Analyzer 警报

在何处可以使用？	需要提供什么？
•	❑ 或

Capacity Analyzer 使用机器学习模型来预测接近其最大容量的资源消耗并发出警报。系统会提前生成 Capacity Analyzer 警报，以识别潜在的容量瓶颈。

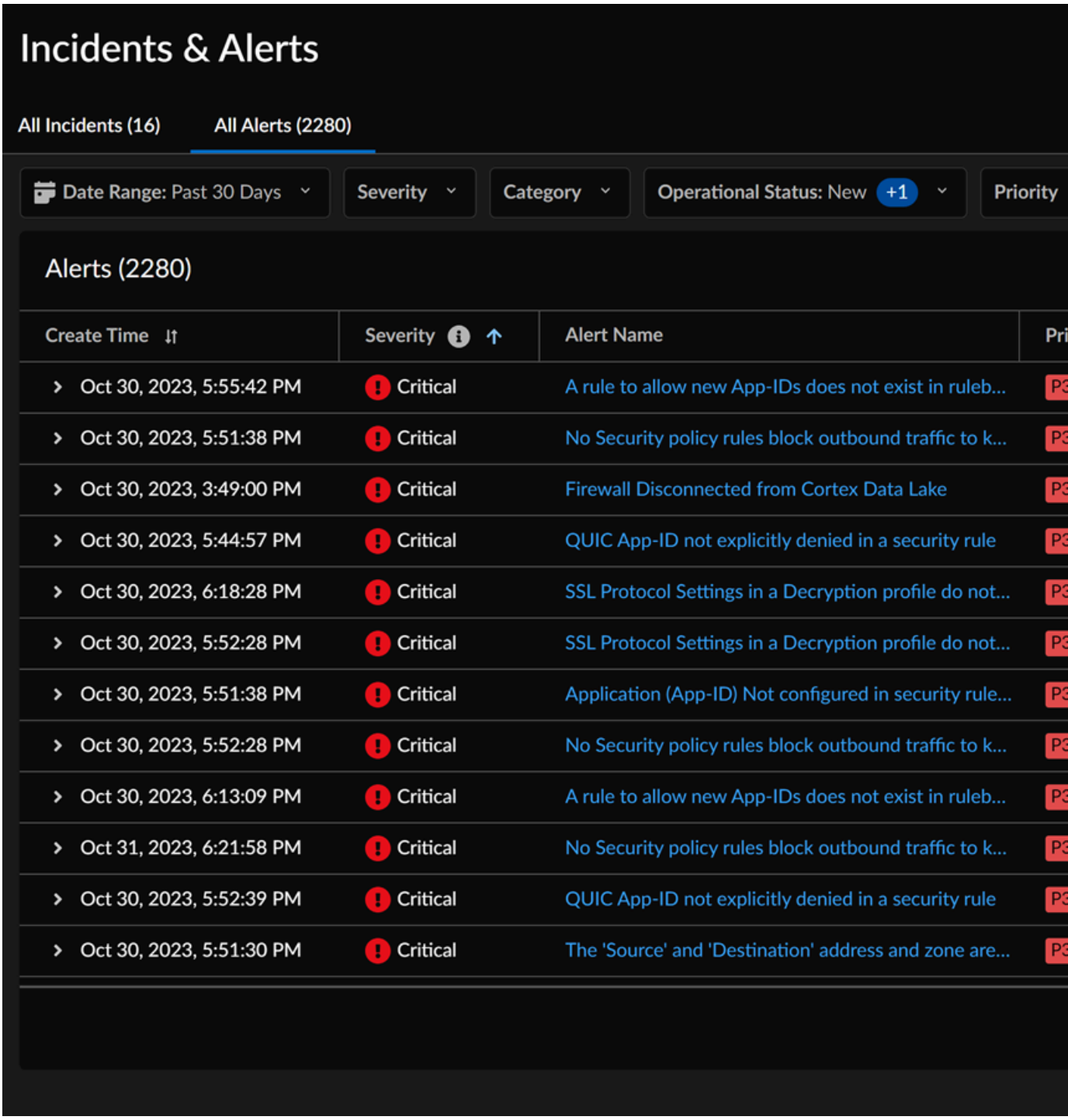
您还可以创建通知规则来触发 Capacity Analyzer 警报通知。

STEP 1 | 导航到 **Incidents & Alerts**（事件和警报）> **NGFW** > **All Alerts**（所有警报），然后单击 **List View**（列表视图）。

STEP 2 | 在 **Alert Name**（警报名称）下，搜索 **approaching max alerts**（接近最大警报数）。

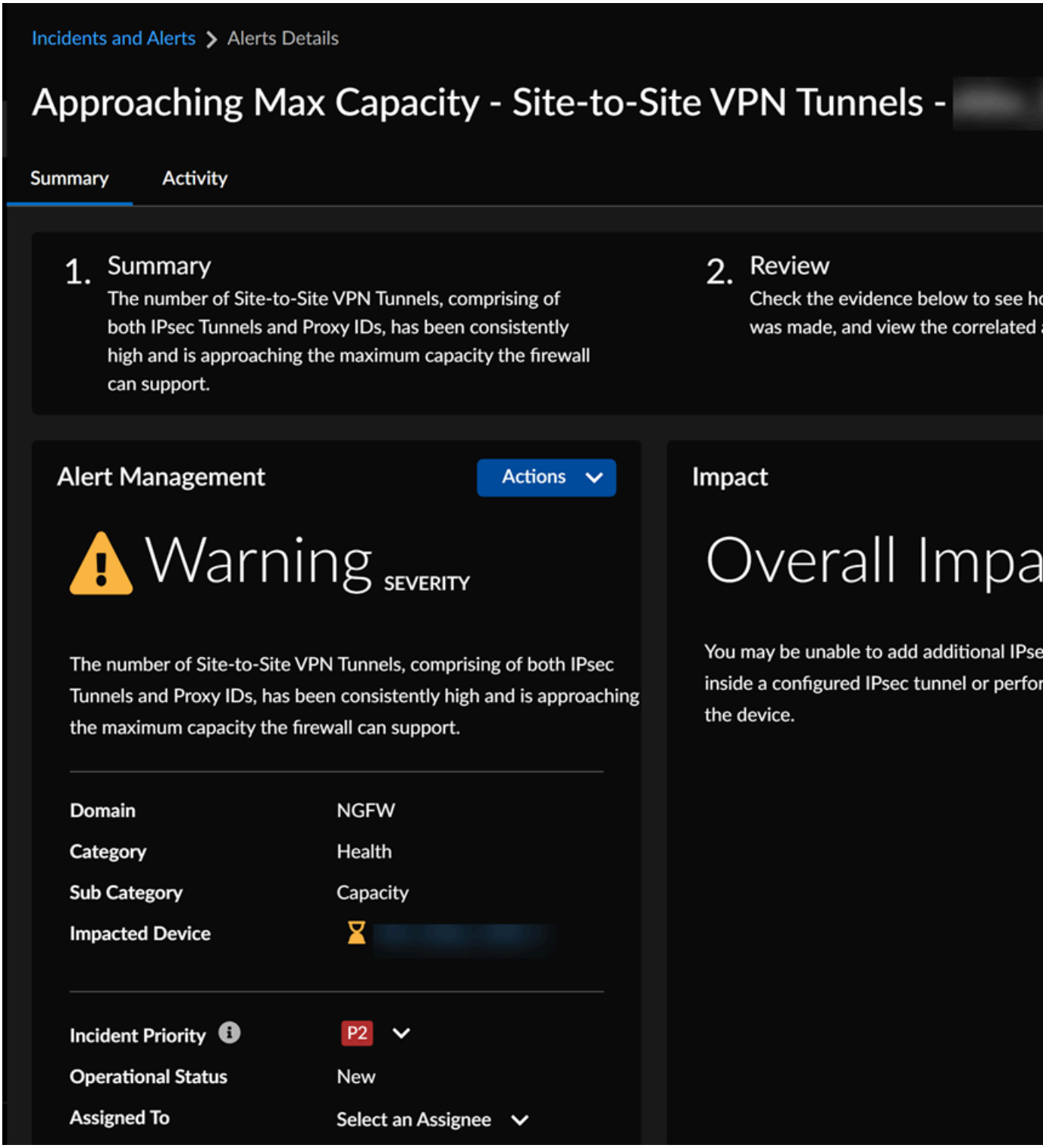
针对 Capacity Analyzer 功能发出的警报名称如下：

Approaching Max Capacity（接近最大容量）- <*Metric-Name*>。



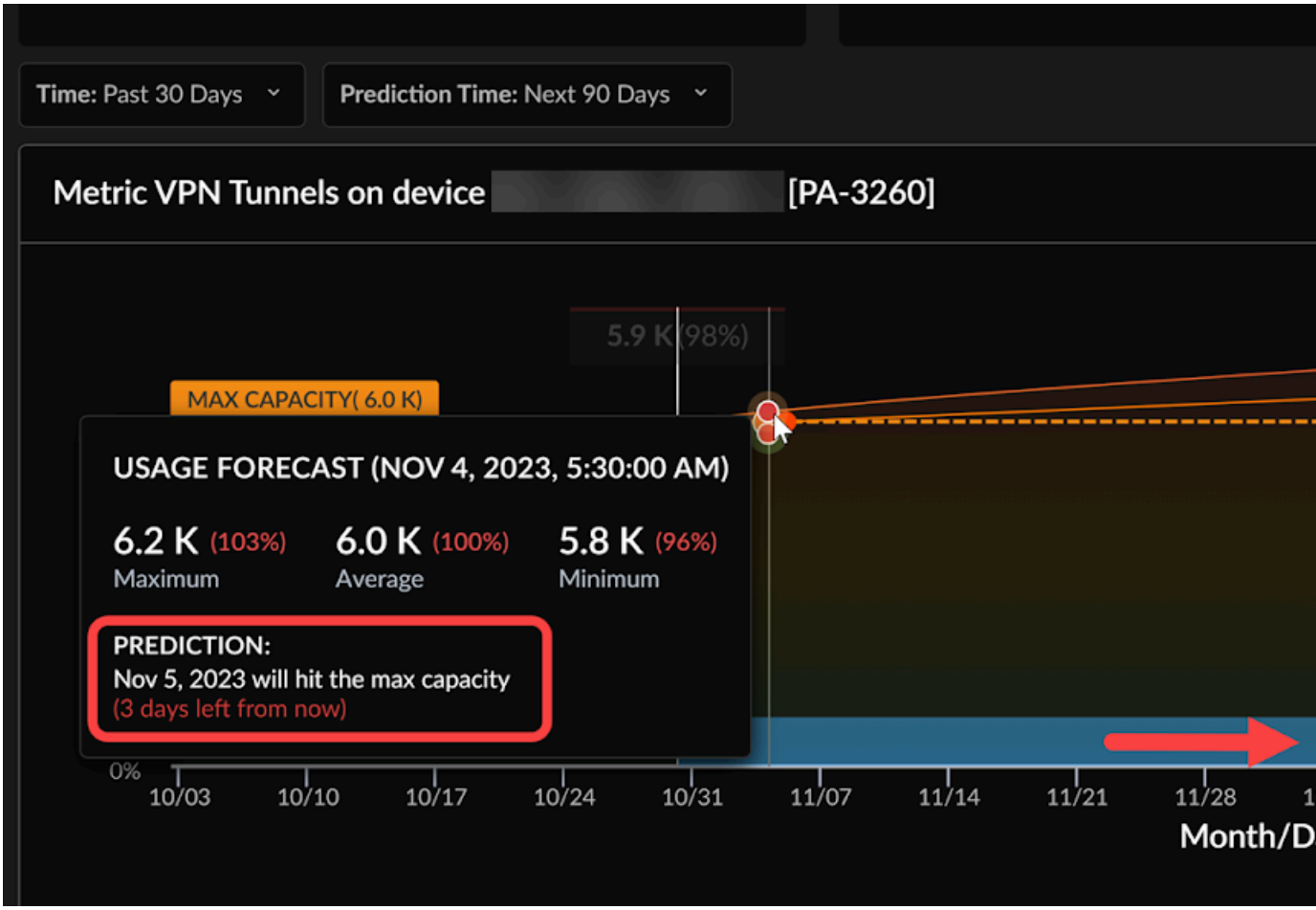
STEP 3 | 选择其中一个警报以查看其详细信息，包括：

- 包含详细信息的警报摘要。
- 警报造成的影响。
- 为了解决您的问题而建议采取的措施。

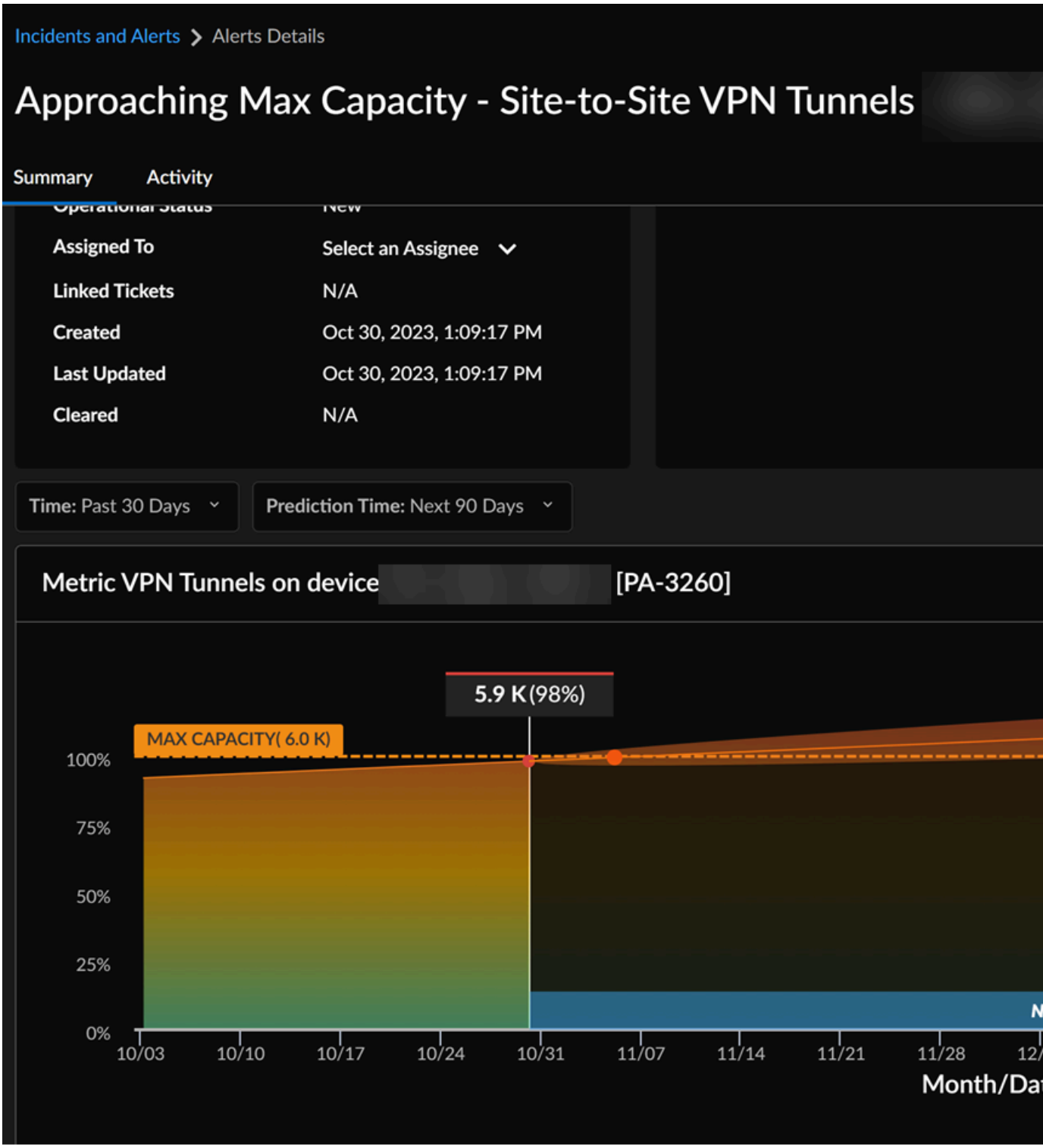


在警报详细信息中，您还可以查看显示指标趋势的图表。Strata Cloud Manager 预测指标达到最大容量的日期。您可以将光标悬停在图表上，以查看任何特定时间点的指标容量。您可以选择未来 30 天或 90 天的 **Prediction Time**（预测时间）。

在本示例中，您可以看到设备上的“VPN 隧道”指标将在 **Nov 5, 2023**（**2023** 年 **11** 月 **5** 日）达到最大容量。



STEP 4 | 在 **Alerts**（警报）页面中，您可以 **Go to Capacity Analyzer Page**（转至 **Capacity Analyzer** 页面）来查看 Capacity Analyzer 热图。



有关如何利用 Capacity Analyzer 热图和查看容量警报的信息，请参阅分析指标容量。

AIOps for NGFW 中的 CPU 使用率指标

在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 、 ❑ 或

使用以下指标跟踪 AIOps for NGFW 中的 CPU 使用率：

- **mp_system_resources.mp_cpu**：指示总 CPU 使用率。
- **mp_system_resources_daemon.cpu_usage_sum**：指示在管理平面 CPU (MP-CPU) 中运行的管理平面任务所产生的 CPU 使用率。该指标相当于 SNMP 中的 CPU 使用率。
- **mp_system_resources_daemon.pan_task_cpu_usage**：指示在 MP-CPU 中运行的 PAN 任务在执行数据平面类型的操作时所产生的 CPU 使用率。该数据并非 SNMP 和 **mp_system_resources_daemon.pan_task_cpu_usage** 指标的一部分。

总 CPU 使用率计算如下：

mp_system_resources.mp_cpu = mp_system_resources_daemon.cpu_usage_sum + mp_system_resources_daemon.pan_task_cpu_usage

创建通知规则

在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 、 ❑ 或

将 Strata Cloud Manager 集成到现有运营中时需要设置主动警报，以便您在潜在问题升级为严重问题之前就能检测并管理它们。可以根据您的运营团队的案例管理协议（例如常用的 P1 或 P2）来定制这些警报。

例如，您可以设置一个警报系统，在该系统中代表最严重问题的严重警报会立即上报至您的安全团队，以便立即引起注意。另一方面，可以安排对紧急程度较低但仍然重要的警告警报进行每日审查。这样的安排既能确保有效的事件管理，同时又能保证运营工作的顺利进行。

另一种选择是根据团队来路由警报；某些类别的警报，甚至是特定警报，都可以路由至最有能力处理它们的不同团队。您可以定义通知首选项，例如哪些警报会触发通知、如何接收通知以及接收通知的频率，从而创建通知规则。

以下视频演示了如何创建通知规则。

STEP 1 | 选择 **Incidents & Alerts**（事件和警报） > **Incident & Alert Settings**（事件和警报设置） > **Notification Rules**（通知规则） > **+ Add Notification Rule**（添加通知规则）

STEP 2 | 输入 `Name`（名称）和 `Description`（说明）。

STEP 3 | 选择 **Add New Condition**（添加新条件）以指定将触发通知的规则条件。

例如，要创建硬件警报通知，请选择 **subCategory**（子类别）、**Equals**（等于）和 **Hardware**（硬件）。

STEP 4 | 选择该通知的通知类型和接收者。

1. 如果选择 **Email**（电子邮件），请选择电子邮件组，即将会收到电子邮件通知的一组用户，或 **Create a New Email Group**（创建新的电子邮件组）。
   1. 如果创建新的电子邮件组，请输入电子邮件组名称，然后开始键入要添加到该组的人员的电子邮件地址。填写所有电子邮件地址后，按回车键。
   2. 选择 **Next**（下一步）。
   3. 选择发送这些通知的频率：
      - 立即
      - 分组并每隔 4 小时发送一次
      - 分组并每天发送一次
2. 如果选择 **ServiceNow**，请输入 `ServiceNow URL`、客户端凭据、ServiceNow 凭据和 `ServiceNow API` 版本。
   1. **Test**（测试）您的连接，以确保集成正常工作。
   2. 选择 **Next**（下一步）。

STEP 5 | **Save Rule**（保存规则）。

与 ServiceNow 集成

在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	❑ 或

在 AIOps for NGFW 通知规则中配置 ServiceNow 集成时，您需要以下信息：

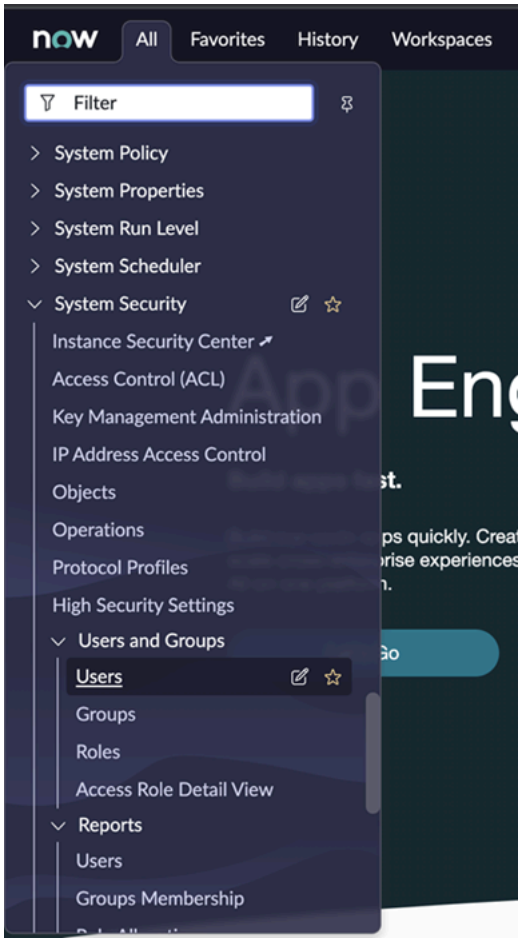
- 配置了管理权限的 ServiceNow 实例
- 具有 Web 访问权限和特定角色的 ServiceNow 用户名和密码，用于创建事件或查询各种表
- 在应用程序注册表下创建的客户端 ID 和密码，以授权 AIOps 访问您的 ServiceNow 实例
- ServiceNow 实例的 URL

您的 ServiceNow 实例还应具有 **Incident**（事件）表，以便 AIOps 向其发送警报，以及包含 **Assignees**（分配对象）的 **Assignment Groups**（分配组），以便向特定人员发出这些警报。

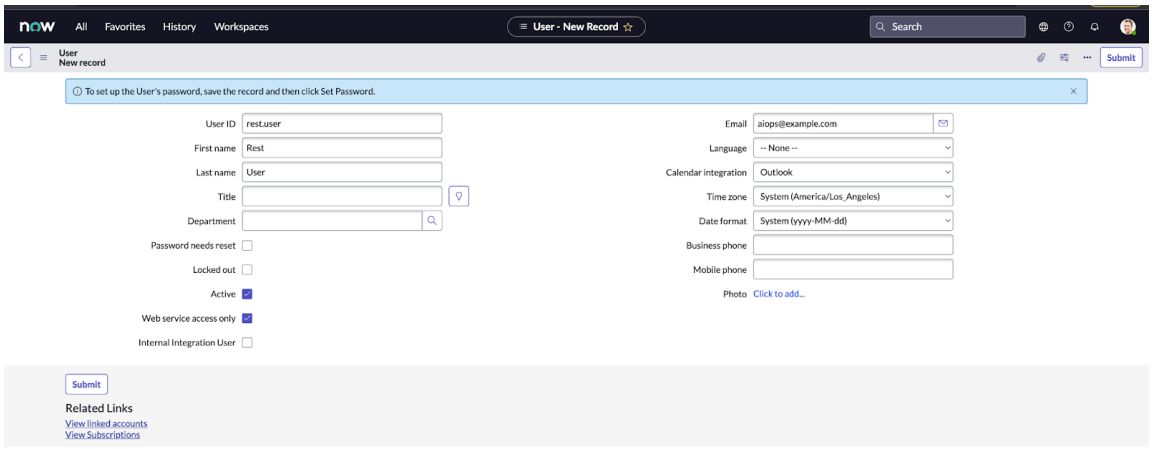
STEP 1 | 创建 ServiceNow Rest 用户。

创建一个具有特定角色的 ServiceNow 新用户，以读取和写入集成所需的各种表（事件、分配组和分配对象）。

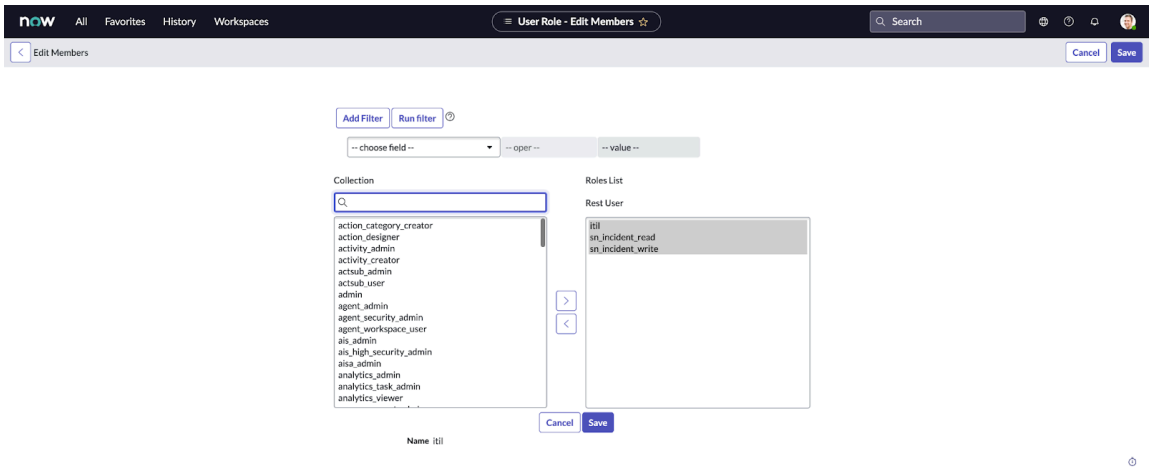
1. 要在 ServiceNow 中创建用户，请导航到 **Security**（安全）**> Users and Groups**（用户和用户组）下的 **Users**（用户）。



2. 选中 **Web service access only**（仅限访问 **Web** 服务）复选框并提交您的更改。

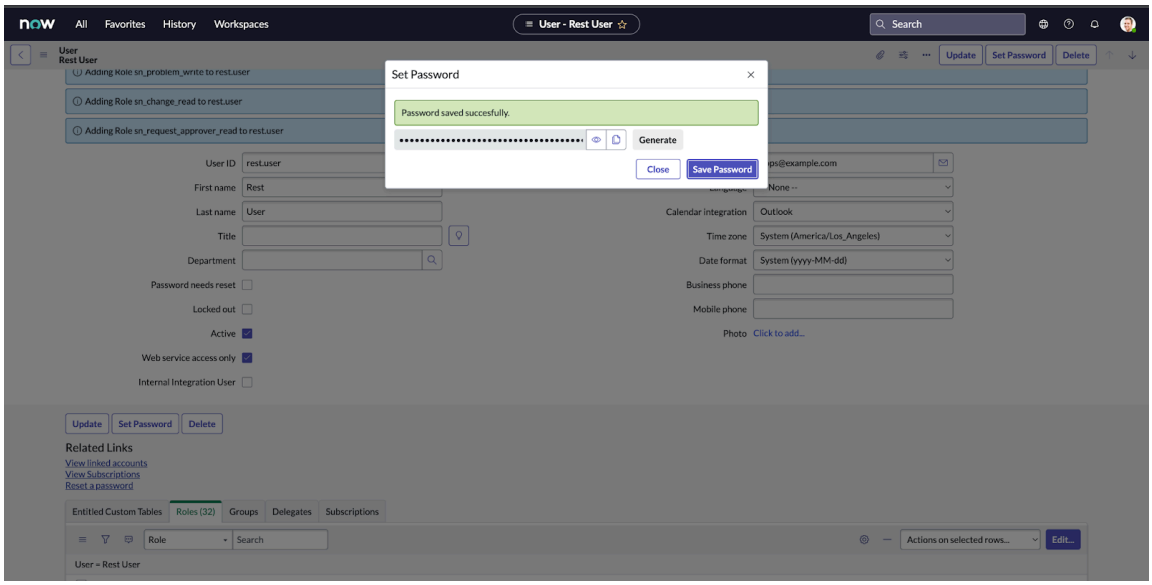


3. 搜索新建用户。在页面底部的表中选择 **Roles**（角色）选项卡，然后单击 **Edit**（编辑）。您需要向用户提供以下三个角色的权限：**itil**、**sn_incident_read** 和 **sn_incident_write**。保存更改。



4. 在“User（用户）”页面上单击 **Set Password**（设置密码）。在弹出窗口中，单击 **Generate**（生成）和 **Save Password**（保存密码）。确保将该密码与用户 ID 一起

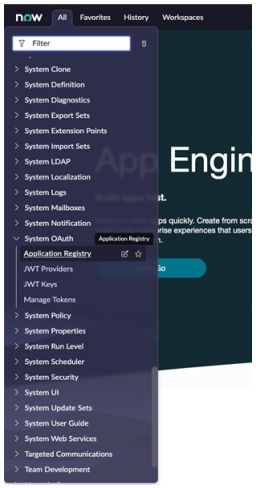
复制到安全位置。这些信息将用于填充 AIOps for NGFW 中的 **ServiceNow User Credentials**（**ServiceNow** 用户凭据）。



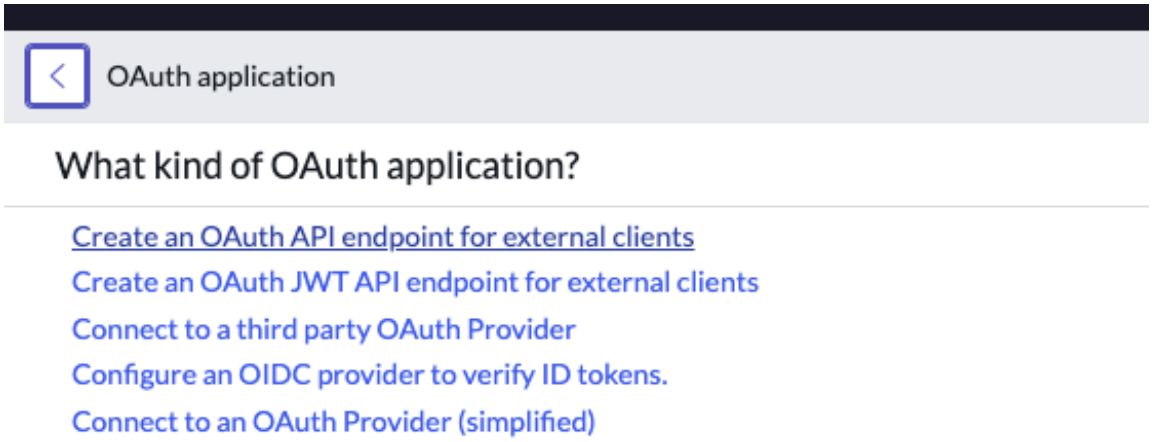
STEP 2 | 创建 Web OAuth 客户端。

AIOps for NGFW 需要 OAuth 客户端才能对您的 ServiceNow 实例进行身份验证。

1. 导航到 **System OAuth**（系统 **OAuth**）**> Application Registry**（应用程序注册表）。

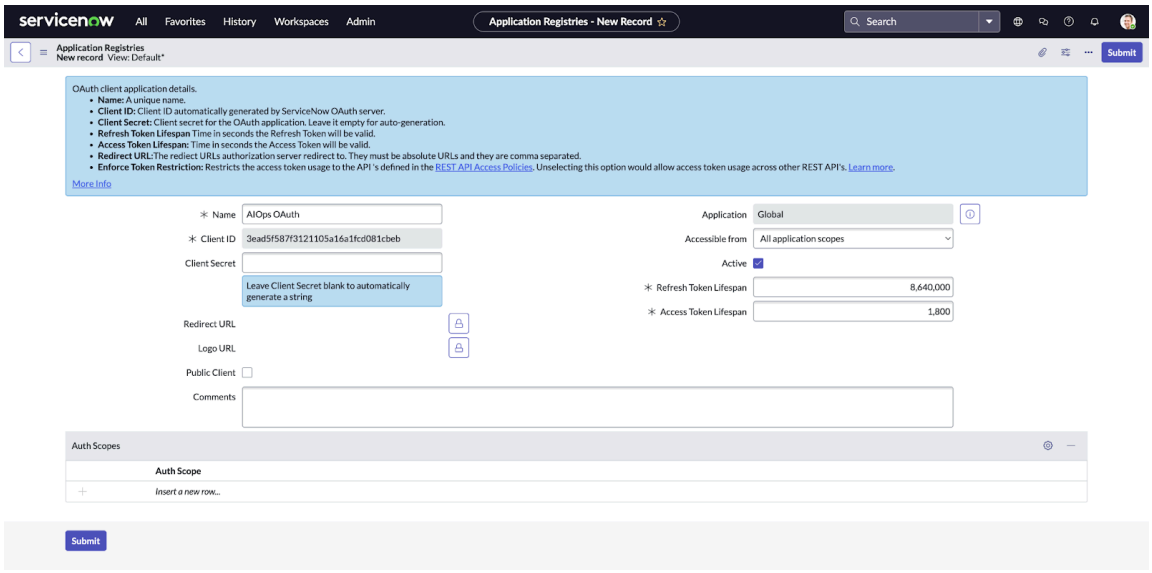


2. 创建一个新条目，然后在下一页中选择 **Create an OAuth API endpoint for external clients**（为外部客户端创建 **OAuth API** 端点）。



3. 为 OAuth 添加名称并创建 **Client Secret**（客户端机密）。如果需要自动生成的机密，也可以将 **Client Secret**（客户端机密）留空。单击 **Submit**（提交），然后导航回应用程序

注册表条目，并将 **Client ID**（客户端 **ID**）和 **Client Secret**（客户端机密）保存在安全的地方。将在 AIOps for NGFW 中的 **Client credential**（客户端凭据）表下使用这些信息。



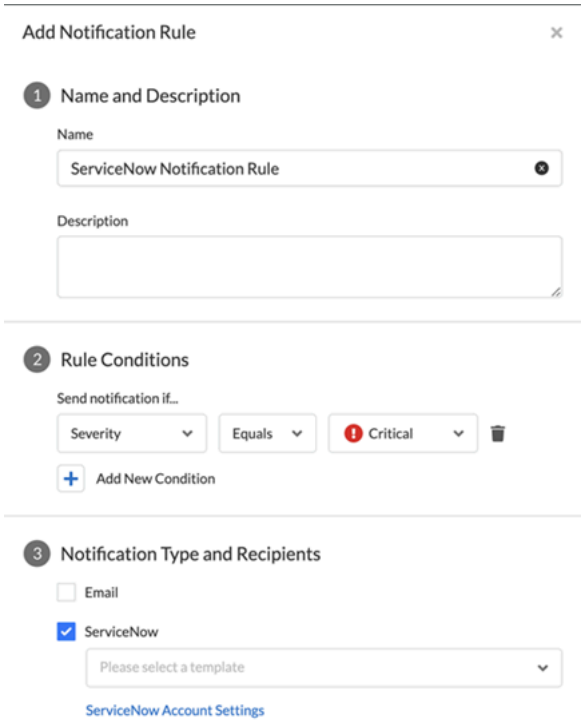
STEP 3 | 在 AIOps for NGFW 中添加 ServiceNow 账户设置信息。

在 AIOps for NGFW 中添加前面步骤中的信息，以完成 ServiceNow 与 AIOps for NGFW 之间的集成。

您需要以下信息：

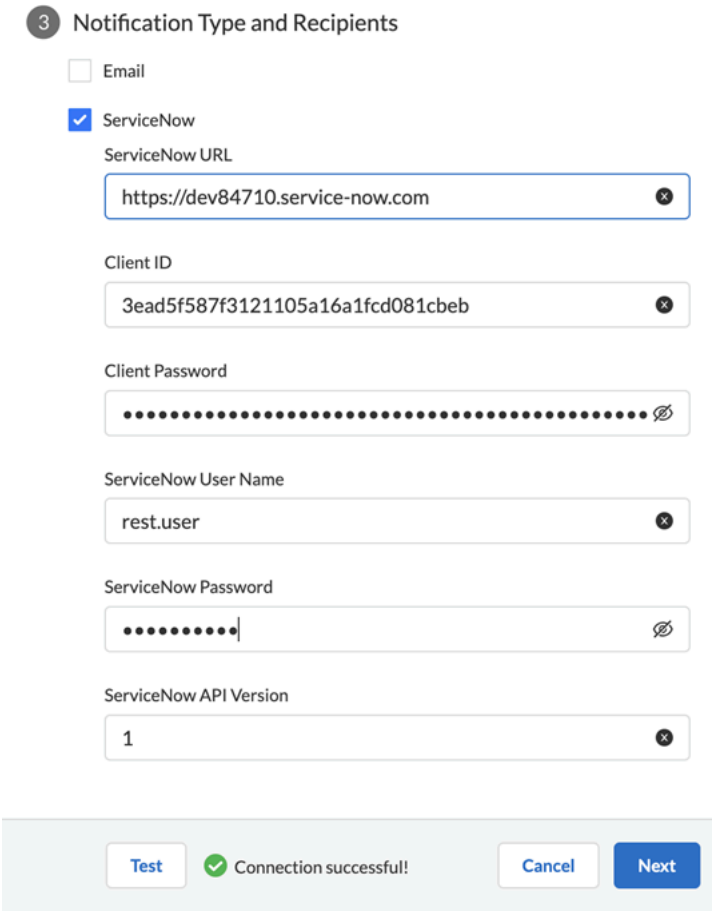
- 您的 **ServiceNow** 实例 **URL**
- 步骤 1 中的 **ServiceNow** 用户和密码
- 步骤 2 中的客户端 **ID** 和客户端机密

1. 在 AIOps for NGFW 中，导航到 **Alert Notification Rules**（警报通知规则），然后单击 **Add Notification Rule**（添加通知规则）。

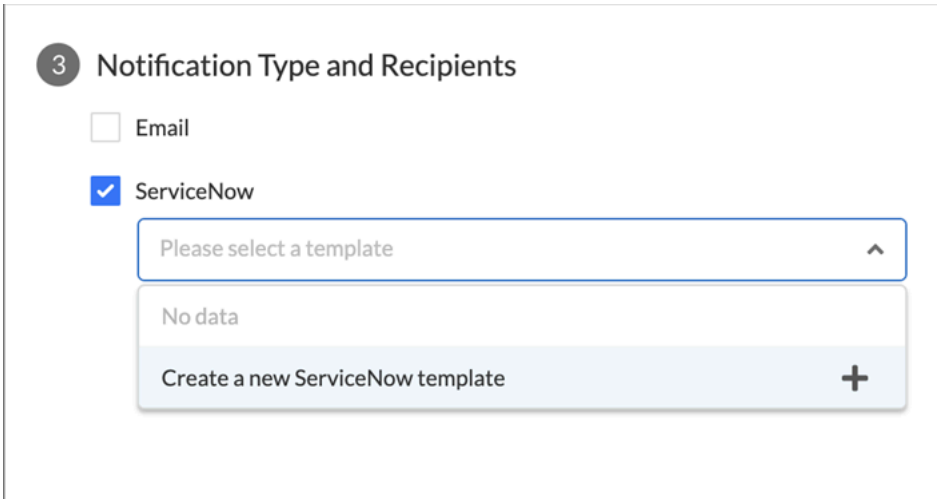


2. 填充 **Rule Name**（规则名称）和 **Alert Condition**（警报条件）等字段，然后单击 **Notification Type and Recipients**（通知类型和接收者）下的 **ServiceNow** 复选框。
3. 点击侧边栏底部的 **ServiceNow Account Settings**（**ServiceNow** 账户设置）。使用之前保存的信息填写以下表单。步骤 1 中的 **ServiceNow** 用户和 **ServiceNow** 密码，在该步骤中您可以设置 Rest 用户。步骤 2 中的客户端 **ID** 和客户端机密，在该步骤中您可以设

置应用程序注册。保持版本不变。单击 **Test**（测试）保存配置并将测试事件发布到您的 ServiceNow 实例。此操作必须成功才能继续。单击 **Next**（下一步）。



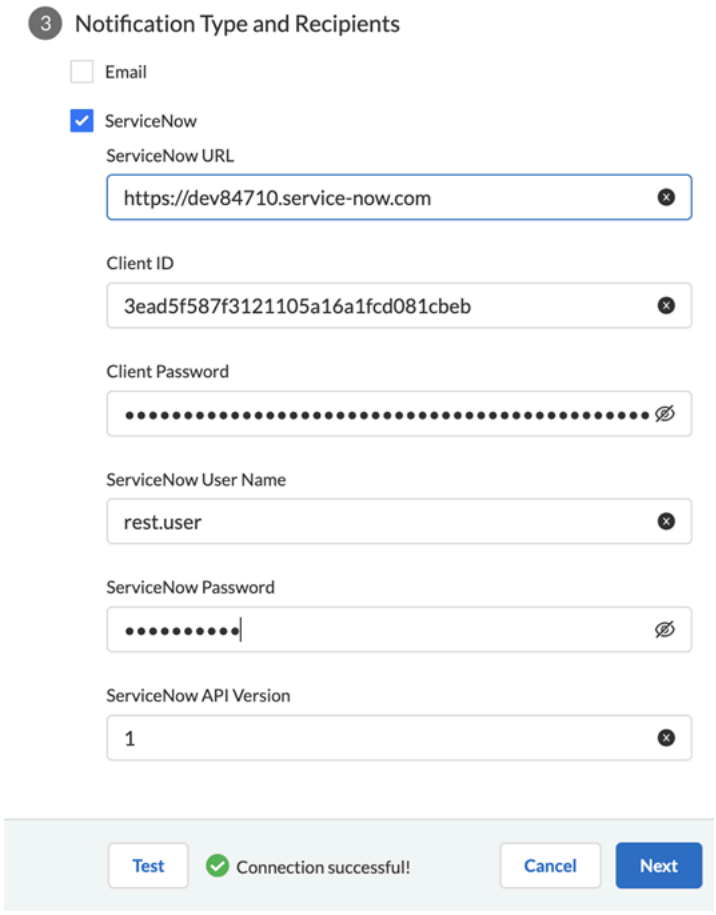
4. 展开 **Please select a template**（请选择一个模板）下拉列表，然后单击 **Create a new ServiceNow Template**（创建新的 **ServiceNow** 模板）。



5. 输入 **eServiceNow** 模板名称，然后从 **Assignment Group**（分配组）下拉列表中选择一个组。从 **Assignee**（分配对象）下拉列表中选择一个分配对象。请注意，这些下拉列表是通过从 ServiceNow 实例调用以下表格来填充的：

   - **System Security**（系统安全）**> Users and Groups**（用户和用户组）**> Users**（用户）
   - **System Security**（系统安全）**> Users and Groups**（用户和用户组）**> Groups**（用户组）

   如果未定义用户组，则不会填充 **Assignment Group**（分配组）下拉列表。如果没有向特定用户组分配任何用户，则不会填充 **Assignees**（分配对象）下拉列表。单击 **Next**（下一步），然后单击 **Save Rule**（保存规则）。



AIOps for NGFW 警报参考

欢迎来到 AIOps for NGFW 警报参考。运行状况警报会实时主动地监控平台的运行状况和性能。这种方法有助于发现问题、预测潜在问题并实施补救措施，确保您的设备以最佳方式运行。以下是一些关键方面：

- 监控指标：持续监控 NGFW 的各种指标，包括 CPU 利用率、内存使用率、磁盘空间、网络吞吐量以及其他相关的性能指标。这种持续监控可以确保快速识别任何偏离正常性能的情况。
- 异常检测：生成根据指标的历史值和使用情况趋势动态调整的警报。通过利用历史数据，系统可以检测到表明存在潜在问题的异常，从而实现主动管理。
- 预测分析：通过分析历史数据和模式，预测何时超出特定阈值或何时发生特定事件。这样有助于在潜在问题升级之前预测问题。

以下页面标识了 AIOps for NGFW 可以发出的警报。

- 高级运行状况警报：查看 Strata Cloud Manager 可以发出的与您的平台运行状况相关的高级警报。
- 免费运行状况警报：查看 AIOps for NGFW 可以发出的与您的平台运行状况相关的免费警报。
- 服务警报：查看 AIOps for NGFW 可以发出的与连接服务相关的警报。
- 利用机器学习发出的警报：查看 Strata Cloud Manager 可以利用机器学习发出的警报。

有关 AIOps for NGFW 可以发出的安全状况检查的相关信息，请导航至 **Manage**（管理）> **Security Posture**（安全状况）> **Settings**（设置）> **Security Checks**（安全检查）表来查看检查。

高级运行状况警报

下表列出了 Strata Cloud Manager 可能发出的与您的平台运行状况相关的高级警报。

Strata Cloud Manager 需要 AIOps for NGFW 高级许可证才能发出这些警报。

警报	说明
ACC 查询失败 （高级警报）	此警报检测应用程序命令中心 (ACC) 查询是否失败。 类：运行状况 类别：报告 应用内支持票证：否
加密流量资源的使用情况不利 （高级警报）	加密流量资源不足。 类：运行状况 类别：资源使用情况 应用内支持票证：否
资源使用情况不利 （高级警报）	防火墙的每秒连接数 (CPS)、吞吐量或会话数量出现异常值。 类：运行状况 类别：资源使用情况 应用内支持票证：否
接近最大容量 - ARP 表 （高级警报）	数据预测分析表明，ARP 表条目很快就会达到防火墙的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 地址组 （高级警报）	地址组对象的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 地址对象 （高级警报）	地址对象的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况

警报	说明
	类别：容量 应用内支持票证：否
接近最大容量 - 数据平面 CPU （高级警报）	数据平面 (DP) CPU 使用率一直居高不下，接近设备所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 解密使用情况 （高级警报）	数据预测分析表明，SSL 解密会话数量很快就会达到防火墙的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - FQDN 地址 （高级警报）	FQDN 地址对象的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - GlobalProtect 隧道（无客户端） （高级警报）	无客户端 GlobalProtect VPN 隧道的数量接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - IKE 对等体 （高级警报）	IKE 对等体的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 管理平面 CPU （高级警报）	管理平面 (MP) CPU 使用率一直居高不下，接近设备所能支持的最大容量。 类：运行状况 类别：容量

警报	说明
	应用内支持票证：否
接近最大容量 - 管理平面内存 （高级警报）	管理平面 (MP) 内存使用率一直居高不下，接近设备所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - NAT 策略 （高级警报）	NAT 策略规则的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 安全策略 （高级警报）	安全策略规则的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 服务组 （高级警报）	服务组对象的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 服务对象 （高级警报）	服务对象的数量一直居高不下，接近防火墙能够支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 会话表利用率 （高级警报）	会话表的使用率 (%) 一直居高不下，接近防火墙或 VM 许可证所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否

警报	说明
接近最大容量 - 站点到站点 VPN 隧道 （高级警报）	站点到站点 VPN 隧道的数量（包括 IPsec 隧道和代理 ID）一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - EDL 内的 URL 或 IP （高级警报）	此防火墙上的策略中使用的已配置 EDL 中的 URL、IP 或域的数量接近防火墙所能支持的最大容量。 类：运行状况 类别：资源使用情况 应用内支持票证：否
接近最大容量 - 虚拟系统 （高级警报）	数据预测分析表明，虚拟系统配置很快就会达到防火墙许可证支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大配置限制 （高级警报）	规则、组和安全配置文件等防火墙对象接近设备限制。 类：运行状况 类别：配置限制 应用内支持票证：否
证书过期 （高级警报）	防火墙上的一个或多个证书已吊销或即将过期。 类：运行状况 类别：证书 应用内支持票证：否
提交推送失败 （高级警报）	配置推送失败。 类：运行状况 类别：配置 应用内支持票证：否
配置内存使用率接近最大限制 （高级警报）	防火墙的配置接近其最大内存使用率限制。在提交期间，防火墙的总配置内存必须容纳两个副本：当前“正在使用”的配置和新的“即将使用”的配置。如果每个配置分配的内存超出 50%，则防火墙达到容量限制，从而导致提交失败。

警报	说明
	类：运行状况 类别：资源使用情况 应用内支持票证：否
DP 数据包丢弃 （高级警报）	警报检测到因不同原因导致的异常丢包 类：运行状况 类别：性能 应用内支持票证：否
HA 链接状态 （高级警报）	连接到防火墙的链接的运行状况。防火墙连接到各种系统以提供各种服务。此警报提供这些连接的运行状况。 类：运行状况 类别：高可用性 应用内支持票证：否
高日志提取率 （高级警报）	日志收集器接近其支持的最大提取率。 类：运行状况 类别：记录 应用内支持票证：否
大量日志查询活动 （高级警报）	日志收集器接近其查询作业或报告的容量。 类：运行状况 类别：记录 应用内支持票证：否
流量延迟增加 - 数据包缓冲区 （高级警报）	设备上的数据包缓冲区资源不足。 类：运行状况 类别：资源使用情况 应用内支持票证：是
流量延迟增加 - 数据包描述符 （高级警报）	设备上的数据包描述符资源不足。 类：运行状况 类别：资源使用情况 应用内支持票证：是

警报	说明
流量延迟增加 - 未知 TCP 或 UDP （高级警报）	防火墙收到应用程序分类为未知 TCP 或未知 UDP 的大量流量。 类：运行状况 类别：资源使用情况 应用内支持票证：否
与日志转发目的地的连接丢失 （高级警报）	该设备无法连接到其日志转发目的地。 类：运行状况 类别：记录 应用内支持票证：否
超出日志的最短保留期限 （高级警报）	日志收集器包含早于定义的最短保留期限的日志。 类：运行状况 类别：记录 应用内支持票证：否
NAT 分配失败 （高级警报）	至少有一条 NAT 规则无法分配足够的资源进行转换。 类：运行状况 类别：NAT 池资源 应用内支持票证：是
NAT 池使用情况 （高级警报）	一个或多个 NAT 规则的资源使用率较高。 类：运行状况 类别：NAT 池资源 应用内支持票证：否
NGFW SD-WAN 应用程序性能警报 （高级警报）	表示受到不良链路性能影响的应用程序列表。 类：运行状况 类别：SD-WAN 性能 应用内支持票证：否
NGFW SD-WAN 链路性能警报 （高级警报）	表示导致应用程序和服务或链路的性能下降的原因。 类：运行状况 类别：SD-WAN 性能 应用内支持票证：否

警报	说明
非默认日志记录级别 （高级警报）	当服务的日志记录级别未设置为其默认配置时，会触发此警报。此警报可确保服务始终维持其指定的日志记录设置。 类：运行状况 类别：资源使用情况 应用内支持票证：否
受 PAN-OS 集成 User-ID 代理监控的服务器已断开连接 （高级警报）	受 PAN-OS 集成 User-ID 代理（无代理 User-ID）监控的服务器与防火墙断开连接时，会触发此警报。该受监控的服务器是将用户身份映射到网络活动的关键组件。 类：运行状况 类别： 应用内支持票证：否
策略配置内存使用率接近最大限制 （高级警报）	此警报检测策略配置内存使用率是否超出临界阈值。 类：运行状况 类别：资源使用情况 应用内支持票证：否
流量延迟 - 数据包描述符（片上） （高级警报）	设备上的数据包描述符（片上）资源不足。 类：运行状况 类别：泛滥/DoS 应用内支持票证：否
隧道关闭 （高级警报）	一个或多个站点到站点 VPN 隧道已关闭。 类：运行状况 类别：站点到站点 VPN 应用内支持票证：是
区域保护配置文件 - 泛滥检测 （高级警报）	在该区域中建立的连接过多或异常，或者传入数据包速率过高或异常。 类：运行状况 类别：泛滥/DoS 应用内支持票证：是
区域保护配置文件 - 阈值建议	区域缺少区域保护配置文件或区域保护配置文件中的阈值需要调整。

警报	说明
（高级警报）	类：运行状况 类别：泛滥/DoS 应用内支持票证：否

免费运行状况警报

下表列出了 AIOps for NGFW 可能发出的与您的平台运行状况相关的免费警报。

AIOps for NGFW 无需高级许可证即可发出这些警报。

警报	说明
卡电源故障 （免费警报）	检测到卡故障，表明该卡或其在机箱中的位置可能存在问题。 类：运行状况 类别：硬件 应用内支持票证：否
配置大小达到设备容量限制 （免费警报）	该设备的配置大小已达到其容量限制。 类：运行状况 类别：配置 应用内支持票证：否
系统驱动器降级 （免费警报）	通过监控其属性值发现系统驱动器降级。 类：运行状况 类别：硬件 应用内支持票证：否
遥测延迟 （免费警报）	分析引擎没有来自此 NGFW/Panorama 的新遥测数据。 类：运行状况 类别：遥测 应用内支持票证：是
FE100 故障 （免费警报）	在防火墙的 FE100 芯片上检测到校准错误。此问题通常表示出现硬件故障。 类：运行状况 类别：硬件 应用内支持票证：否
风扇问题 （免费警报）	风扇或风扇托架触发了设备警报。 类：运行状况 类别：硬件

警报	说明
	应用内支持票证：否
致命机器检查故障 （免费警报）	检测到致命机器检查故障。此问题通常表示 CPU 出现硬件故障。 类：运行状况 类别：硬件 应用内支持票证：否
防火墙与 Cortex 数据湖断开连接 （免费警报）	FW 和 Strata 日志记录服务之间的连接已断开。 类：运行状况 类别：SLS 连接 应用内支持票证：否
防火墙与 Panorama 断开连接 （免费警报）	防火墙和 Panorama 之间的连接已断开。 类：运行状况 类别：connection-failure 应用内支持票证：否
HA 备份 （免费警报）	当前未配置 HA 备份链路。 类：运行状况 类别：高可用性 应用内支持票证：否
HA 对等连接状态 （免费警报）	HA 对中的一个防火墙处于非正常运行状态。 类：运行状况 类别：高可用性 应用内支持票证：是
磁盘空间使用率高 - Pancfg 分区 （免费警报）	硬盘分区接近或达到容量限制。 类：运行状况 类别：资源使用情况 应用内支持票证：是
磁盘空间使用率高 - Panlogs 分区 （免费警报）	硬盘分区接近或达到容量限制。 类：运行状况 类别：资源使用情况

警报	说明
	应用内支持票证：是
磁盘空间使用率高 - 根分区 （免费警报）	硬盘分区接近或达到容量限制。 类：运行状况 类别：资源使用情况 应用内支持票证：是
大量处理活动 （免费警报）	设备上的一个或多个计算资源不足。 类：运行状况 类别：资源使用情况 应用内支持票证：否
IPQ 错误 （免费警报）	在防火墙中的一个 FE100 芯片上检测到 IPQ（入口数据包队列）错误。此错误通常表示需要重新安装或出现硬件故障。 类：运行状况 类别：硬件 应用内支持票证：否
输入功率异常 （免费警报）	设备功率等级超出正常范围。 类：运行状况 类别：硬件 应用内支持票证：否
许可证到期 （免费警报）	您的一个或多个许可证即将过期或已过期。 类：运行状况 类别：PanOS 和订阅 应用内支持票证：否
日志记录驱动器故障 （免费警报）	通过监控防火墙的磁盘状态，发现日志记录驱动器出现故障。 类：运行状况 类别：硬件 应用内支持票证：否
MPC 卡 - CPLD 故障 （免费警报）	管理处理器卡 (MPC) 是 PA-5450 的重要组件，可提供管理、日志记录和高可用性功能。由于其组件，即复杂可编程逻辑器件 (CPLD) 出现问题，MPC 卡发生故障。 类：运行状况

警报	说明
	类别：硬件 应用内支持票证：否
NGFW/Panorama 管理证书过期 （免费警报）	此警报检测到 NGFW/Panorama 管理证书已过期。 类：运行状况 类别：证书 应用内支持票证：否
NPC 卡 - FE100 故障 （免费警报）	网络处理卡 (NPC) 提供网络连接，对于网络流量处理至关重要。一张 NPC 卡的 FE100 组件出现问题，导致其发生故障。 类：运行状况 类别：硬件 应用内支持票证：否
不同步对等体 - 配置 （免费警报）	高可用性对等体上的系统配置不匹配。 类：运行状况 类别：高可用性 应用内支持票证：否
不同步对等体 - 动态内容 （免费警报）	高可用性对等体之间的动态内容（例如防病毒或应用程序和威胁）不匹配。 类：运行状况 类别：高可用性 应用内支持票证：否
不同步对等体 - 会话 （免费警报）	高可用性对等体之间的会话不匹配或不是最新的。 类：运行状况 类别：高可用性 应用内支持票证：否
不同步对等体 - 软件 （免费警报）	高可用性对等体上的 PAN-OS 软件版本不匹配。 类：运行状况 类别：高可用性 应用内支持票证：否
动态内容过时	与更新服务器上可用的内容相比，该设备上安装的动态内容已过时。

警报	说明
（免费警报）	类：运行状况 类别：动态内容 应用内支持票证：否
PAN-OS 生命周期结束 （免费警报）	您当前的 PAN-OS 版本不再受支持。 类：运行状况 类别：PanOS 和订阅 应用内支持票证：否
PAN-OS 已知漏洞 （免费警报）	您当前的 PAN-OS 版本存在已知漏洞。 类：运行状况 类别：动态内容 应用内支持票证：否
PAN-OS 根证书和默认证书过期 - 场景 1 （免费警报）	防火墙上的根证书和默认证书已过期。 类：运行状况 类别：证书 应用内支持票证：否
PCI 错误 （免费警报）	外围组件互连 (PCI) 负责将管理平面 (MP) 连接到控制平面 (CP)。与该组件相关的某个错误表示其功能出现故障。 类：运行状况 类别：硬件 应用内支持票证：否
路径监视器故障 - 卡 （免费警报）	在防火墙插槽内的卡上检测到路径监视故障。 类：运行状况 类别：硬件 应用内支持票证：否
端口故障 （免费警报）	检测到与管理物理端口或其中一个高可用性物理端口相关的故障。 类：运行状况 类别：硬件 应用内支持票证：否

警报	说明
进程内存耗尽 - Configd （免费警报）	该设备的管理平面进程将会耗尽其可用内存。 类：运行状况 类别：资源使用情况 应用内支持票证：是
进程内存耗尽 - 设备服务器 （免费警报）	该设备的管理平面进程将会耗尽其可用内存。 类：运行状况 类别：资源使用情况 应用内支持票证：是
进程内存耗尽 - 日志接收器 （免费警报）	该设备的管理平面进程将会耗尽其可用内存。 类：运行状况 类别：资源使用情况 应用内支持票证：是
进程内存耗尽 - 管理服务器 （免费警报）	该设备的管理平面进程将会耗尽其可用内存。 类：运行状况 类别：资源使用情况 应用内支持票证：是
进程内存耗尽 - 用户 ID （免费警报）	该设备的管理平面进程将会耗尽其可用内存。 类：运行状况 类别：资源使用情况 应用内支持票证：是
冗余电源故障 （免费警报）	无法实现电源冗余，原因可能是电源尚未插入、电源出现故障或者尚未实现完全冗余。 类：运行状况 类别：硬件 应用内支持票证：是
Strata 日志记录服务的日志转发延迟 （免费警报）	Strata 日志记录服务上的转发延迟超出了可接受值。 类：运行状况 类别：SLS 运行状况 应用内支持票证：否

警报	说明
Strata 日志记录服务的日志转发离线 （免费警报）	Strata 日志记录服务的日志转发服务无法正常运行 类：运行状况 类别：SLS 运行状况 应用内支持票证：否
Strata 日志记录服务的日志提取延迟 （免费警报）	Strata 日志记录服务的提取延迟超出了可接受值。 类：运行状况 类别：SLS 运行状况 应用内支持票证：否
Strata 日志记录服务的日志提取离线 （免费警报）	Strata 日志记录服务的提取服务无法正常运行。 类：运行状况 类别：SLS 运行状况 应用内支持票证：否
Strata 日志记录服务的日志存储空间接近限制 （免费警报）	日志类型接近配置的最大存储限制。 类：运行状况 类别：记录 应用内支持票证：否
散热问题 （免费警报）	设备温度超出正常范围。 类：运行状况 类别：硬件 应用内支持票证：否

服务警报

下表列出了 AIOps for NGFW 可以发出的与连接服务相关的警报。

警报	说明
防火墙与 Strata Logging Service断开连接 （免费警报）	FW 与 SLS 之间的连接已丢失超过 5 分钟。 类别：SLS 连接 应用内支持票证：否
Strata 日志记录服务的日志提取离线 （免费警报）	SLS 提取服务已停止运行超过 5 分钟。 类别：SLS 运行状况 应用内支持票证：否
Strata 日志记录服务的日志转发离线 （免费警报）	SLS 日志转发服务已停止运行超过 5 分钟。 类别：SLS 运行状况 应用内支持票证：否
Strata 日志记录服务的日志提取延迟 （免费警报）	在过去 15 分钟内，SLS 的提取延迟超出 10 分钟。 类别：SLS 运行状况 应用内支持票证：否
Strata 日志记录服务的日志转发延迟 （免费警报）	过去 15 分钟内，SLS 的转发延迟超出 10 分钟。 类别：SLS 运行状况 应用内支持票证：否
Strata 日志记录服务的日志存储空间接近限制 （免费警报）	日志类型接近配置的最大存储限制。 类别：记录 应用内支持票证：否

利用机器学习发出的警报

下表列出了 AIOps for NGFW 可以利用机器学习发出的警报。

警报	说明
加密流量资源的使用情况不利 （高级警报）	加密流量资源不足。 类：运行状况 类别：资源使用情况 应用内支持票证：否 检测类型：异常
资源使用情况不利 （高级警报）	防火墙的每秒连接数 (CPS)、吞吐量或会话数量出现异常值。 类：运行状况 类别：资源使用情况 应用内支持票证：否 检测类型：异常
接近最大配置限制 （高级警报）	规则、组和安全配置文件等防火墙对象接近设备限制。 类：运行状况 类别：配置限制 应用内支持票证：否 检测类型：异常
大量处理活动 （免费警报）	设备上的一个或多个计算资源不足。 类：运行状况 类别：资源使用情况 应用内支持票证：否
流量延迟增加 - 数据包缓冲区 （高级警报）	设备上的数据包缓冲区资源不足。 类：运行状况 类别：资源使用情况 应用内支持票证：是 检测类型：异常
流量延迟增加 - 数据包描述符	设备上的数据包描述符资源不足。

警报	说明
（高级警报）	类：运行状况 类别：资源使用情况 应用内支持票证：是 检测类型：异常
流量延迟 - 数据包描述符（片上） （高级警报）	设备上的数据包描述符（片上）资源不足。 类：运行状况 类别：泛滥/DoS 应用内支持票证：否 检测类型：异常
接近最大容量 - ARP 表 （高级警报）	数据预测分析表明，ARP 表条目很快就会达到防火墙的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 地址组 （高级警报）	地址组对象的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 地址对象 （高级警报）	地址对象的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 数据平面 CPU （高级警报）	数据平面 (DP) CPU 使用率一直居高不下，接近设备所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 解密使用情况	数据预测分析表明，SSL 解密会话数量很快就会达到防火墙的最大容量。

警报	说明
（高级警报）	类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - FQDN 地址 （高级警报）	FQDN 地址对象的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - GlobalProtect 隧道（无客户端） （高级警报）	无客户端 GlobalProtect VPN 隧道的数量接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - IKE 对等体 （高级警报）	IKE 对等体的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 管理平面 CPU （高级警报）	管理平面 (MP) CPU 使用率一直居高不下，接近设备所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 管理平面内存 （高级警报）	管理平面 (MP) 内存使用率一直居高不下，接近设备所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - NAT 策略 （高级警报）	NAT 策略规则的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况

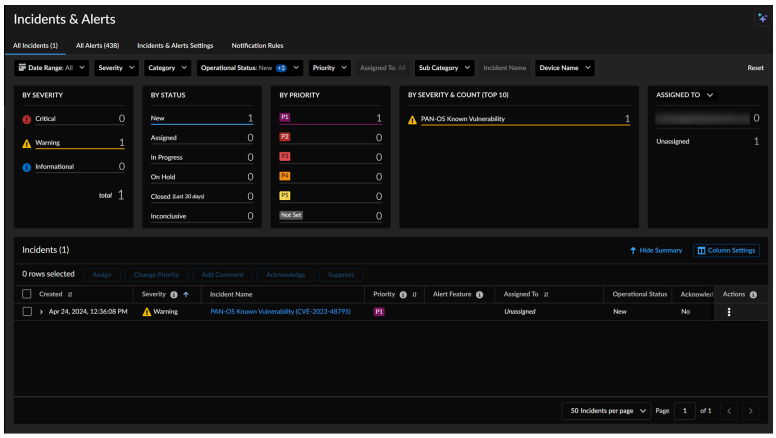
警报	说明
	类别：容量 应用内支持票证：否
接近最大容量 - 安全策略（高级警报）	安全策略规则的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 服务组（高级警报）	服务组对象的数量一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 服务对象（高级警报）	服务对象的数量一直居高不下，接近防火墙能够支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 会话表利用率（高级警报）	会话表的使用率 (%) 一直居高不下，接近防火墙或 VM 许可证所能支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 虚拟系统（高级警报）	数据预测分析表明，虚拟系统配置很快就会达到防火墙许可证支持的最大容量。 类：运行状况 类别：容量 应用内支持票证：否
接近最大容量 - 站点到站点 VPN 隧道（高级警报）	站点到站点 VPN 隧道的数量（包括 IPsec 隧道和代理 ID）一直居高不下，接近防火墙所能支持的最大容量。 类：运行状况 类别：容量

警报	说明
	应用内支持票证：否
NGFW SD-WAN 应用程序性能警报 （高级警报）	表示受到不良链路性能影响的应用程序列表。 类：运行状况 类别：SD-WAN 性能 应用内支持票证：否 检测类型：异常
NGFW SD-WAN 链路性能警报 （高级警报）	表示导致应用程序和服务或链路的性能下降的原因。 类：运行状况 类别：SD-WAN 性能 应用内支持票证：否 检测类型：异常

管理 NGFW 事件

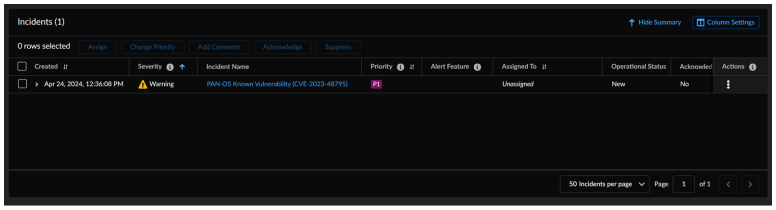
在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 、 ❑ 或

选择 **Incidents & Alerts**（事件和警报） > **NGFW** > **All Incidents**（所有事件），以获取 NGFW 事件的鸟瞰视图。浏览事件页面，随时了解部署中的变化，以便您可以对其进行调查并在必要时采取预防措施。您可以直接访问事件的详细列表以及关键的可视化摘要。您还可以 **Hide Summary**（隐藏摘要），以隐藏小部件并仅以表格格式查看事件。



以下是 **All Incidents**（所有事件）下显示的数据。

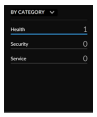
- 事件：显示所有事件。



在此表中，您可以执行以下任务：

- **Hide Summary**（隐藏摘要）以隐藏小部件并仅以表格格式查看事件。
- 展开事件以查看其描述和影响。
- 在“Actions（操作）”下，您可以执行以下操作：
  - 将事件分配给用户、自己，或者取消分配事件。
  - 更改事件的优先级或选择“Not Set（未设置）”以删除优先级。
  - 选择 **Yes**（是）以确认事件，确认您看到了该事件。
  - 当您不打算主动解决事件时，通过阻止将事件设置为"搁置"运行状态。
  - 为事件添加注释。
- 单击事件以查看其详细信息。
- 使用 **Column Settings**（列设置）查看或隐藏事件的特定列，并重新排列这些列的默认顺序。这些更改将在未来的会话中保留。

- 分配对象：显示分配给负责解决事件的个人或实体的事件数量。顶部显示分配给当前登录用户的事件和未分配的事件。您也可以在下拉列表中选择 **BY CATEGORY**（按类别）来查看事件数量。



- 按严重性和计数分类（前 **10** 个）：显示按严重性分类的事件，以及每个类别中的事件计数。严重事件的优先级最高，其次是警告事件，然后是信息事件。

- 按状态分类：按状态显示事件总数。
  - “New（新建）”表示未分配的事件。
  - “Assigned（已分配）”表示已分配给用户的事件。
  - “In Progress（进行中）”表示正在处理此事件。
  - “On Hold（搁置）”表示您不打算主动解决事件。
  - “Closed（已关闭）”表示最近 30 天内关闭的事件。
  - “Inconclusive（没有定论）”表示这些事件没有解决办法。

- 按严重性分类：显示归类为“严重”、“警告”和“信息”的事件总数。

- 按优先级分类：显示按照优先级分类的事件，其中 P1 表示程度最为严重。

查看事件详细信息

在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 、 ❑ 或

在 **All Incidents**（所有事件）中，您可以选择一个事件，然后会打开一个页面，其中包含有关该事件的详细信息。**Summary**（摘要）选项卡显示以下详细信息：

1. 包含详细信息的事件摘要。您可以更改事件的优先级或将其分配给用户。
2. 事件造成的影响，即受影响的 NGFW 数量。
3. 为了解决您的问题而建议采取的措施。

您还可以单击 CVE，以查看其在 Palo Alto Networks 安全公告中的详细信息以及 PAN-OS 版本中的漏洞。

Correlated Alerts & Activity（相关警报和活动）选项卡显示以下详细信息：

- 所选事件的相关警报
- 事件的记录活动