监控和警报

Data Infrastructure Insights

NetApp
January 13, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/data-infrastructure-insights/task_create_monitor.html on January 13, 2026. Always check docs.netapp.com for the latest.

目录

监控和警报

使用监视器发出警报

配置监视器以跟踪基础设施资源的性能阈值、日志事件和异常。为节点写入延迟、存储容量或应用程序性能等指标创建自定义警报，并在满足这些条件时接收通知。

监视器允许您设置由“基础设施”对象（例如存储、VM、EC2 和端口）生成的指标的阈值，以及“集成”数据（例如为 Kubernetes、 ONTAP高级指标和 Telegraf 插件收集的数据）的阈值。当超过警告级别或临界级别阈值时，这些_metric_监视器会向您发出警报。

您还可以创建监视器，当检测到指定的日志事件时触发警告、严重或信息级别的警报。

Data Infrastructure Insights提供了许多"系统定义的监视器"也取决于您的环境。

安全最佳实践

Data Infrastructure Insights警报旨在突出显示租户的数据点和趋势，Data Infrastructure Insights允许您输入任何有效的电子邮件地址作为警报收件人。如果您在安全的环境中工作，请特别注意谁接收通知或以其他方式有权访问警报。

指标还是日志监控?

1. 从“Data Infrastructure Insights”菜单中，单击“警报”>“管理监视器”

   将显示监视器列表页面，其中显示当前配置的监视器。

2. 要修改现有监视器，请单击列表中的监视器名称。
3. 要添加监视器，请单击“+ 监视器”。

当您添加新的监视器时，系统会提示您创建指标监视器或日志监视器。

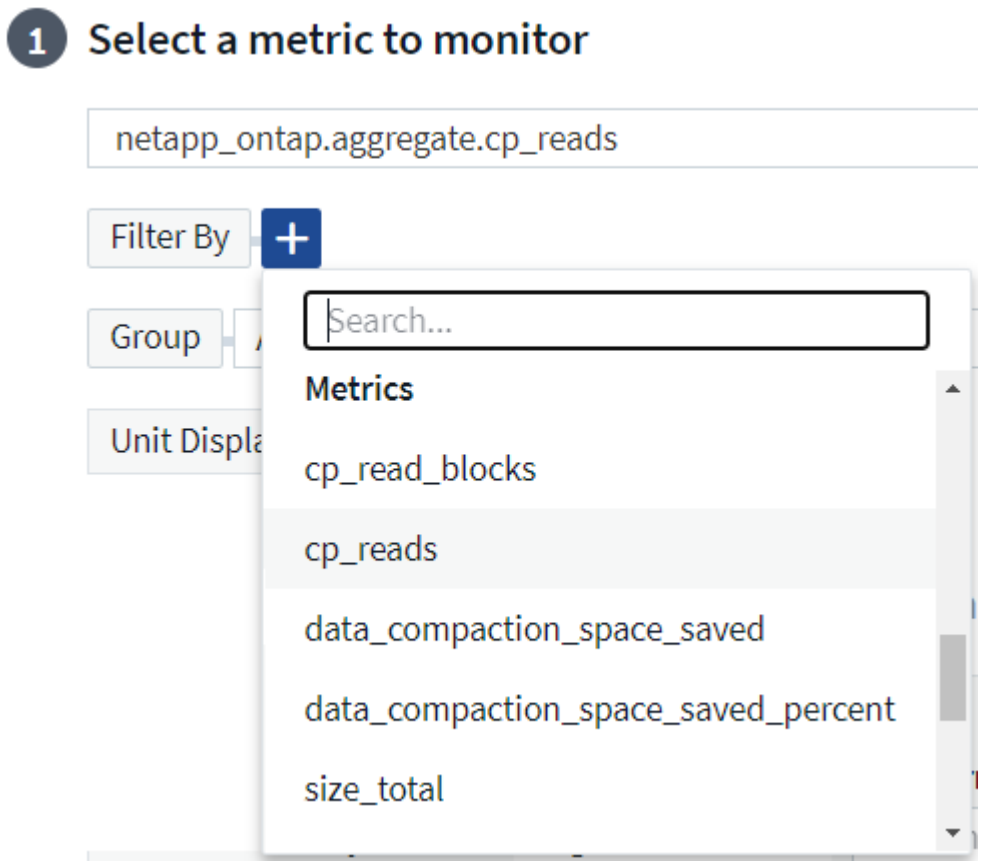
- *Metric* 监控与基础设施或性能相关的触发事件的警报
- *Log* 监控与日志相关的活动警报

选择监视器类型后，将显示“监视器配置”对话框。配置根据您创建的监视器类型而有所不同。

指标监控

1. 在下拉菜单中，搜索并选择要监控的对象类型和指标。

您可以设置过滤器来缩小要监控的对象属性或指标的范围。

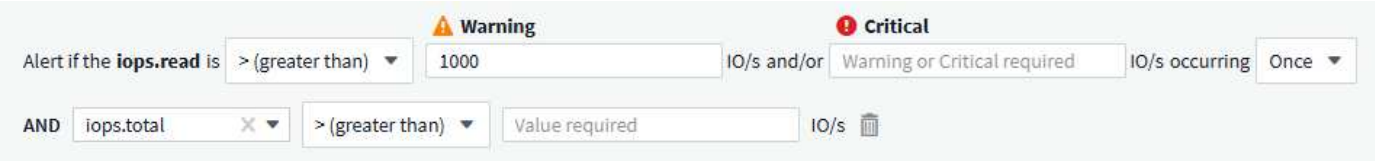


处理集成数据（Kubernetes、 ONTAP Advanced Data 等）时，指标过滤会从绘制的数据系列中删除单个/不匹配的数据点，这与基础设施数据（存储、VM、端口等）不同，其中过滤器会对数据系列的聚合值进行处理，并可能从图表中删除整个对象。

指标监视器适用于存储、交换机、主机、虚拟机等库存对象，以及ONTAP Advanced 或 Kubernetes 数据等集成指标。监控库存对象时，请注意不能选择“分组依据”方法。但是，监控集成数据时允许分组。

多条件监视器

您可以选择通过添加第二个条件来进一步优化您的指标监视器。只需展开“+添加次要指标条件”提示并配置附加条件。



如果两个条件都满足，监视器就会发出警报。

请注意，您只能“AND”第二个条件；您不能选择在一个条件“OR”另一个条件上发出警报。

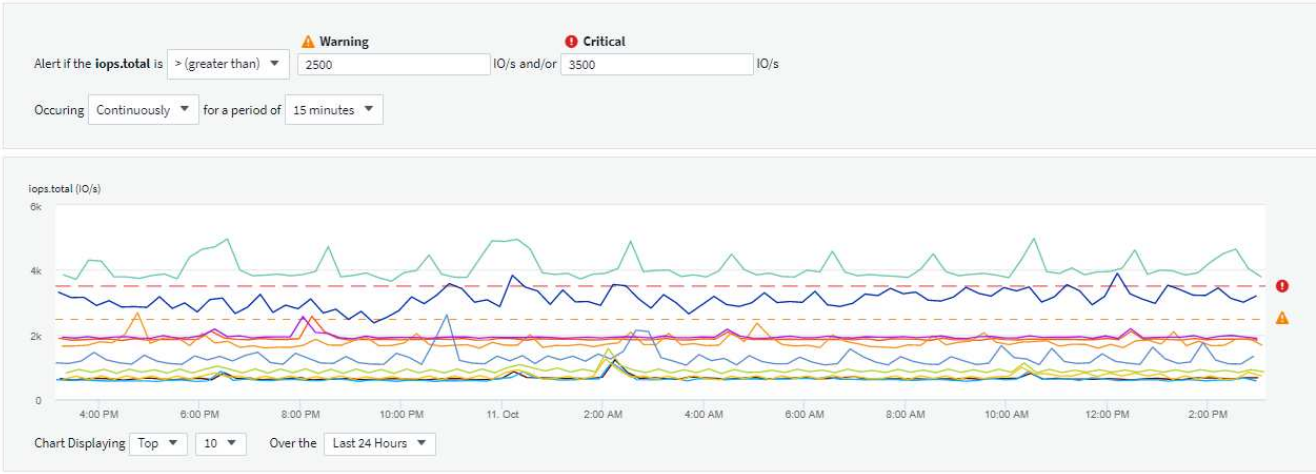
定义监视器的条件。

1. 选择要监控的对象和指标后，设置警告级别和/或临界级别阈值。
2. 对于“警告”级别，在我们的示例中输入 200。示例图中显示了表示此警告级别的虚线。
3. 对于“*Critical*”级别，输入 400。示例图中显示了表示此临界水平的虚线。

   该图表显示历史数据。图表上的警告和严重级别线是监视器的直观表示，因此您可以轻松看到监视器在每种情况下何时可能触发警报。

4. 对于发生间隔，选择“连续”且周期为“15 分钟”。

   您可以选择在超出阈值时立即触发警报，或者等到阈值持续超出一段时间后再触发警报。在我们的示例中，我们不希望每次总 IOPS 峰值超过警告或严重级别时都收到警报，而希望仅当监控对象连续超过其中一个级别至少 15 分钟时才收到警报。



定义警报解决行为

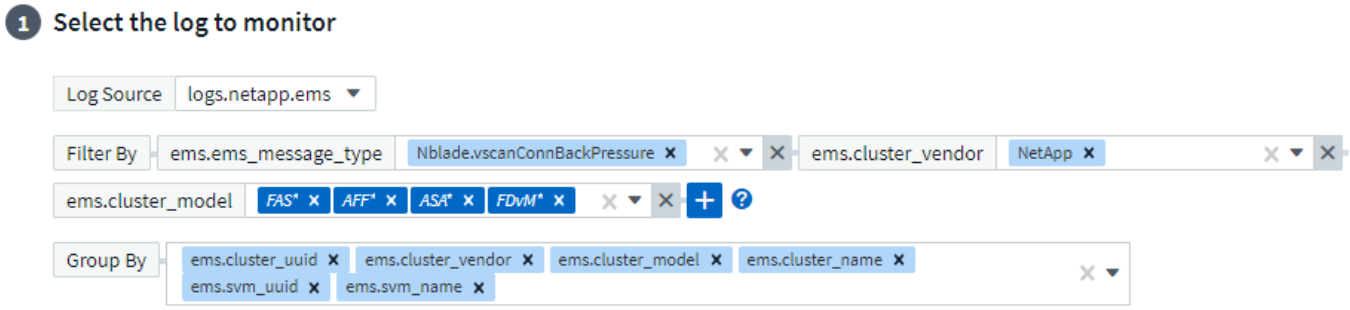
您可以选择如何解决指标监视器警报。您面临两个选择：

- 当指标恢复到可接受范围时进行解决。
- 当指标在指定时间范围内（从 1 分钟到 7 天）处于可接受范围内时进行解析。

日志监控

创建*日志监视器*时，首先从可用日志列表中选择要监视的日志。然后，您可以根据上述可用属性进行过滤。您还可以选择一个或多个“分组依据”属性。

日志监控过滤器不能为空。



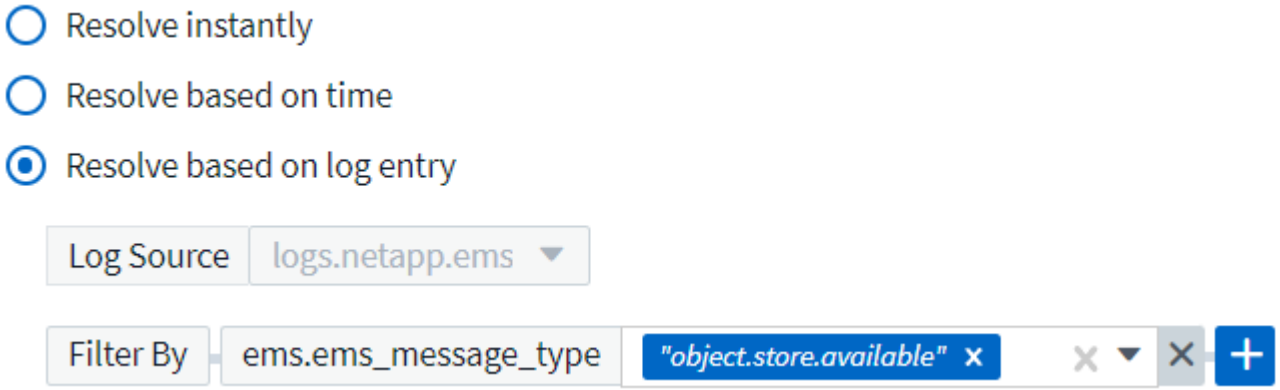
定义警报行为

您可以创建监视器，当您上面定义的条件发生一次（即立即）时，以严重级别_Critical_、_Warning_或_Informational_发出警报，或者等到条件发生 2 次或更多次时发出警报。

定义警报解决行为

您可以选择如何解决日志监视器警报。您面临三个选择：

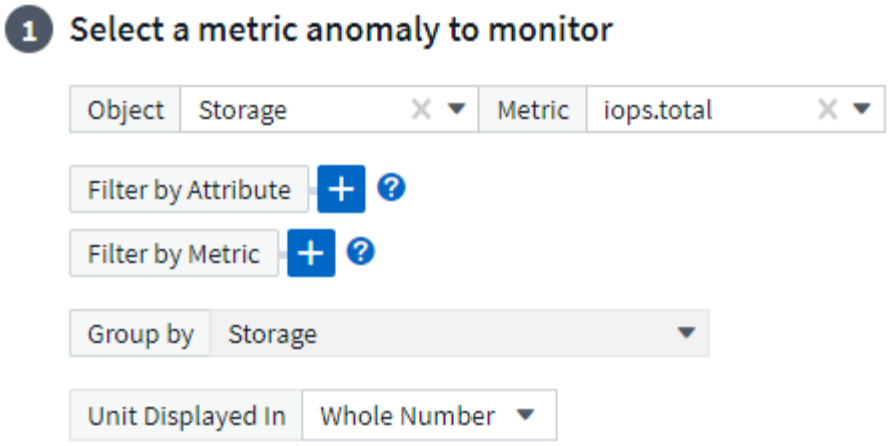
- 立即解决：警报立即解决，无需采取进一步行动
- 根据时间解决：指定时间过后，警报得到解决
- 根据日志条目解决：当发生后续日志活动时，警报得到解决。例如，当一个对象被记录为“可用”时。



异常检测监视器

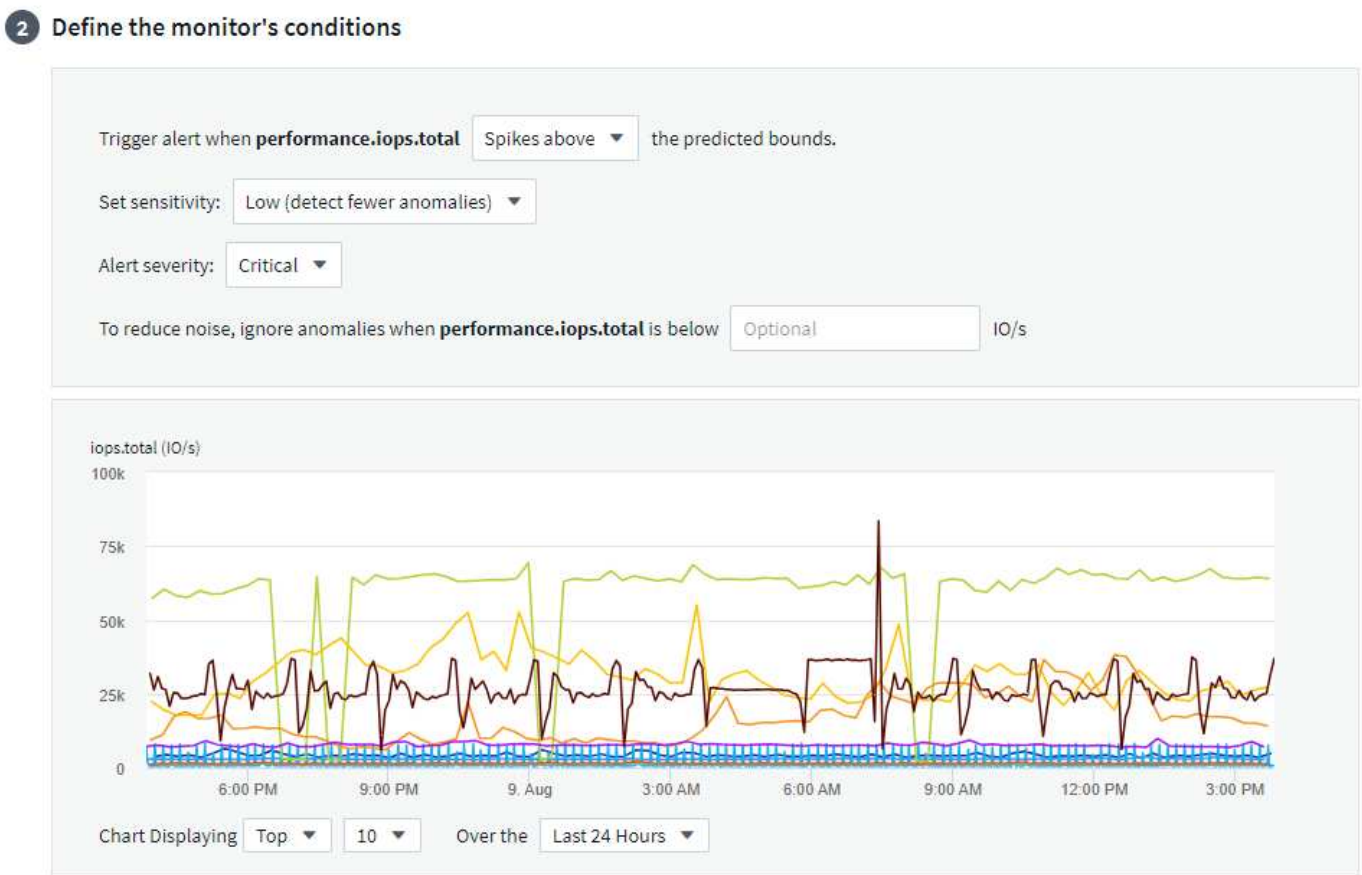
1. 在下拉菜单中，搜索并选择要监控的对象类型和指标。

您可以设置过滤器来缩小要监控的对象属性或指标的范围。



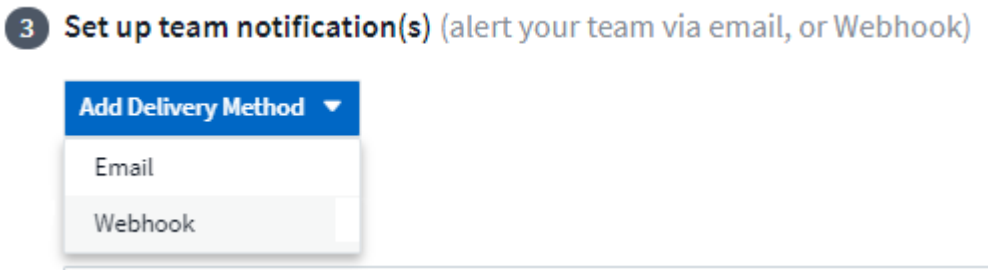
定义监视器的条件。

1. 选择要监控的对象和指标后，您需要设置检测异常的条件。
   - 当所选指标*飙升至*预测边界之上、*跌至*该边界之下，或*飙升至*边界之上或跌至*边界之下时，选择是否检测异常。
   - 设置检测的*灵敏度*。 低（检测到的异常较少）、中*或*高（检测到的异常较多）。
   - 将警报设置为*警告*或*严重*。
   - 如果需要，您可以选择减少噪音，当所选指标低于您设置的阈值时忽略异常。



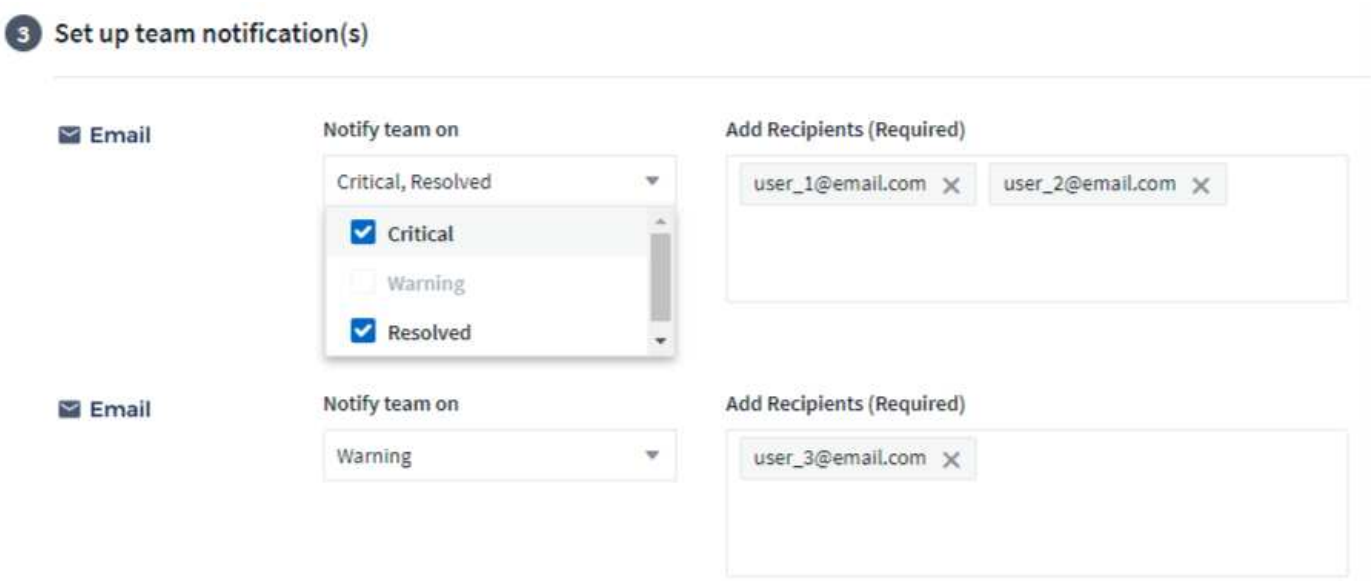
选择通知类型和收件人

在“设置团队通知”部分，您可以选择通过电子邮件还是 Webhook 提醒您的团队。



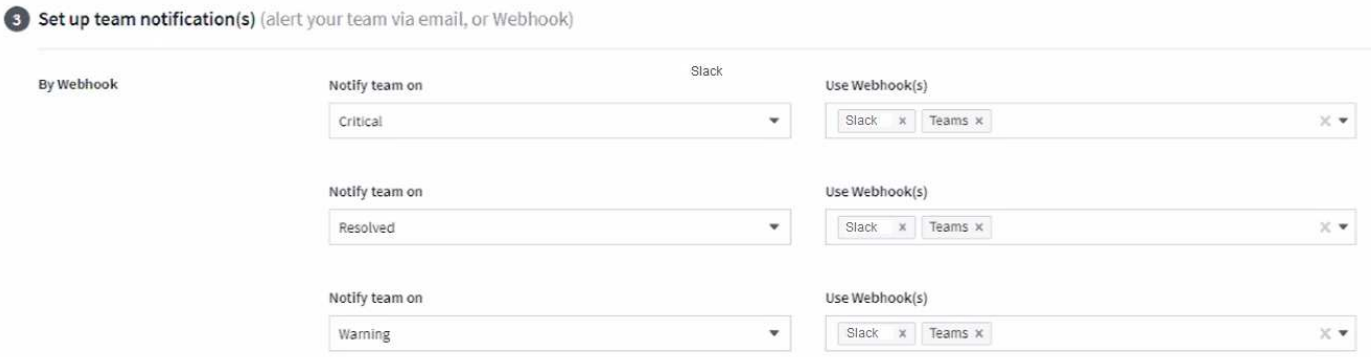
通过电子邮件发出警报：

指定警报通知的电子邮件收件人。如果需要，您可以为警告或严重警报选择不同的收件人。



通过 **Webhook** 发出警报：

指定警报通知的 webhook。如果需要，您可以选择不同的 webhook 来发出警告或严重警报。



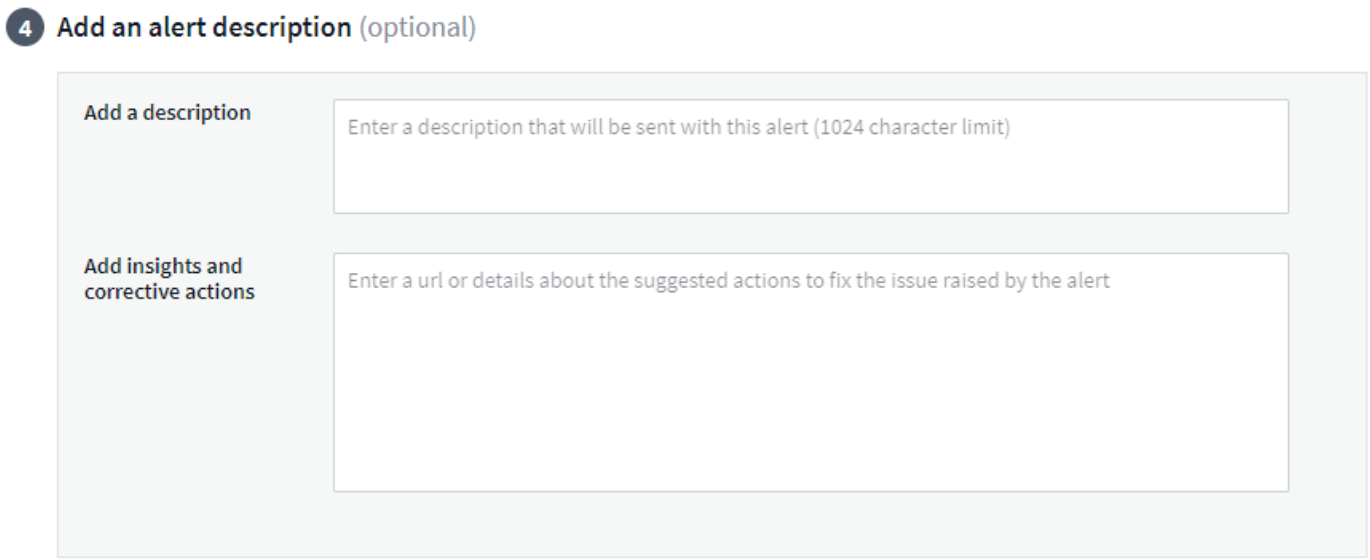
ONTAP数据收集器通知优先于与集群/数据收集器相关的任何特定监视器通知。您为数据收集器本身设置的收件人列表将接收数据收集器警报。如果没有活动的数据收集器警报，则监视器生成的警报将发送给特定的监视器接收者。

设置纠正措施或附加信息

您可以通过填写“添加警报描述”部分来添加可选描述以及其他见解和/或纠正措施。描述最多可以有 1024 个字符，并将与警报一起发送。见解/纠正措施字段最多可包含 67,000 个字符，并将显示在警报登陆页面的摘要部分。

在这些字段中，您可以提供注释、链接或纠正或处理警报所需的步骤。

您可以将任何对象属性（例如，存储名称）作为参数添加到警报描述中。例如，您可以在描述中设置卷名称和存储名称的参数，如：“卷的高延迟：*%%relatedObject.volume.name%%*，存储：*%%relatedObject.storage.name%%*”。



保存您的监视器

1. 如果需要，您可以添加监视器的描述。
2. 为监视器指定一个有意义的名称，然后单击“保存”。

   您的新监视器已添加到活动监视器列表中。

监控列表

监视器页面列出了当前配置的监视器，显示以下内容：

- 监视器名称
- 状态
- 被监控的对象/指标
- 监测条件

您可以选择暂时暂停某个对象类型的监控，方法是单击监视器右侧的菜单并选择“暂停”。当您准备好恢复监控时

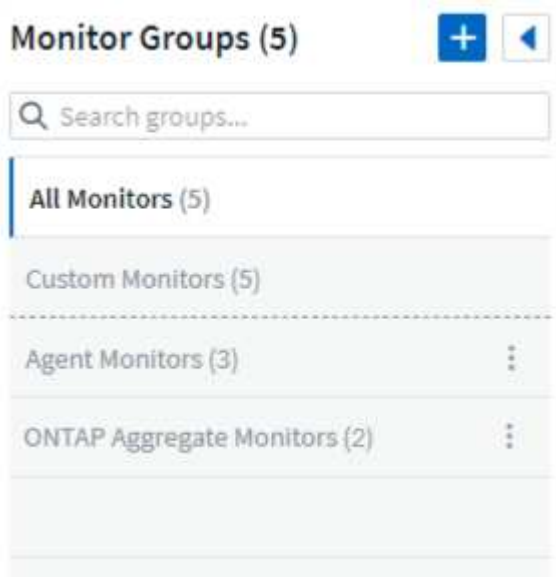
，单击*恢复*。

您可以通过从菜单中选择“复制”来复制监视器。然后，您可以修改新的监视器并更改对象/指标、过滤器、条件、电子邮件收件人等。

如果不再需要监视器，您可以通过从菜单中选择“删除”来删除它。

监控组

通过分组，您可以查看和管理相关的监视器。例如，您可以有一个专门负责租户存储的监视组，或者监视与特定收件人列表相关的监视组。



显示以下监视器组。组中包含的监视器数量显示在组名旁边。

- 所有监视器 列出所有监视器。
- *自定义监视器*列出了所有用户创建的监视器。
- 暂停的监视器 将列出所有已被Data Infrastructure Insights暂停的系统监视器。
- Data Infrastructure Insights还将显示多个*系统监控组*，其中将列出一个或多个组"系统定义的监视器"，包括ONTAP基础架构和工作负载监视器。

自定义监视器可以暂停、恢复、删除或移动到另一个组。系统定义的监视器可以暂停和恢复，但不能删除或移动。

悬挂式监视器

仅当Data Infrastructure Insights已暂停一个或多个监视器时，才会显示此组。如果监视器生成过多或连续的警报，则可能会被暂停。如果监视器是自定义监视器，请修改条件以防止持续警报，然后恢复监视器。当导致暂停的问题得到解决后，该监视器将从暂停监视器组中删除。

系统定义的监视器

只要您的环境包含监视器所需的设备和/或日志可用性，这些组就会显示Data Infrastructure Insights提供的监视器。

系统定义的监视器不能被修改、移动到另一个组或删除。但是，您可以复制系统监视器并修改或移动副本。

系统监视器可能包括ONTAP基础架构（存储、卷等）或工作负载（即日志监视器）或其他组的监视器。 NetApp不断评估客户需求和产品功能，并将根据需要更新或添加系统监视器和组。

自定义监控组

您可以根据需要创建自己的组来包含监视器。例如，您可能想要为所有与存储相关的监视器创建一个组。

要创建新的自定义监控组，请点击“+”创建新监控组按钮。输入组的名称，然后单击“创建组”。将以该名称创建一个空组。

要将监视器添加到组，请转到“所有监视器”组（推荐）并执行以下操作之一：

- 要添加单个监视器，请单击监视器右侧的菜单并选择“添加到组”。选择要添加监视器的组。
- 点击监视器名称打开监视器的编辑视图，并在_关联到监视器组_部分中选择一个组。

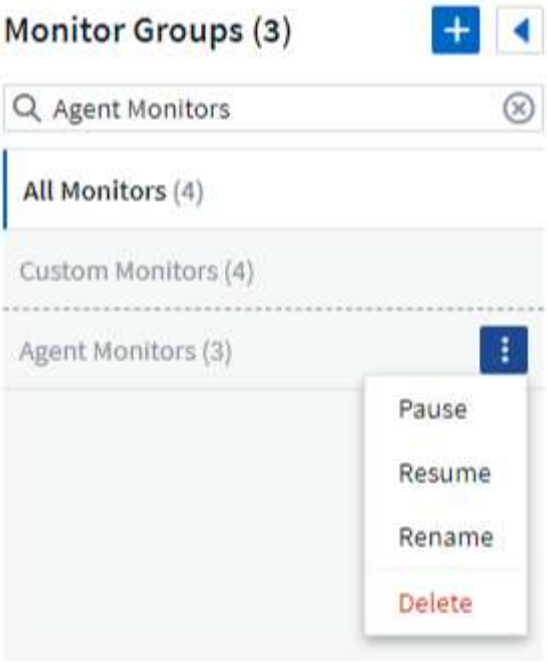
单击某个组并从菜单中选择“从组中删除”来删除监视器。您不能从“所有监视器”或“自定义监视器”组中删除监视器。要从这些组中删除监视器，您必须删除监视器本身。

从组中删除监视器并不会从Data Infrastructure Insights中删除该监视器。要完全删除监视器，请选择该监视器并单击“删除”。这也会将其从其所属的组中删除，并且任何用户都无法再使用它。

您还可以以相同的方式将监视器移动到不同的组，选择“移动到组”。

要一次暂停或恢复组中的所有监视器，请选择该组的菜单，然后单击“暂停”或“恢复”。

使用相同的菜单重命名或删除组。删除组并不会从Data Infrastructure Insights中删除监视器；它们仍然在“所有监视器”中可用。



系统定义的监视器

Data Infrastructure Insights包括许多系统定义的指标和日志监视器。可用的系统监视器取决于租户上的数据收集器。因此，随着数据收集器的添加或其配置的改变，Data Infrastructure Insights中可用的监视器可能会发生变化。

查看"系统定义的监视器"页面，了解Data Infrastructure Insights中包含的监视器的描述。

更多信息

- "查看和关闭警报"

查看和管理监视器的警报

Data Infrastructure Insights在以下情况下显示警报"监控阈值"超出了。

监控和警报功能在Data Infrastructure Insights标准版及更高版本中可用。

查看和管理警报

要查看和管理警报，请执行以下操作。

1. 导航到*警报 > 所有警报*页面。
2. 显示最多最近 1,000 条警报的列表。您可以通过单击字段的列标题来按任何字段对该列表进行排序。该列表显示以下信息。请注意，默认情况下并非所有这些列都会显示。您可以通过单击“齿轮”图标来选择要显示的列：
   - 警报 **ID**：系统生成的唯一警报 ID
   - 触发时间：相关监视器触发警报的时间

- 当前严重程度（活动警报选项卡）：活动警报的当前严重程度
- 最高严重程度（已解决警报选项卡）；警报在解决之前的最高严重程度
- 监视器：配置为触发警报的监视器
- 触发条件：超出监控阈值的对象
- 状态：当前警报状态，新_或_处理中
- 活动状态：活动_或_已解决
- 条件：触发警报的阈值条件
- 指标：超出监控阈值的对象指标
- 监视器状态：触发警报的监视器的当前状态
- 有纠正措施：警报已建议采取纠正措施。打开警报页面即可查看这些内容。

您可以通过单击警报右侧的菜单并选择以下选项之一来管理警报：

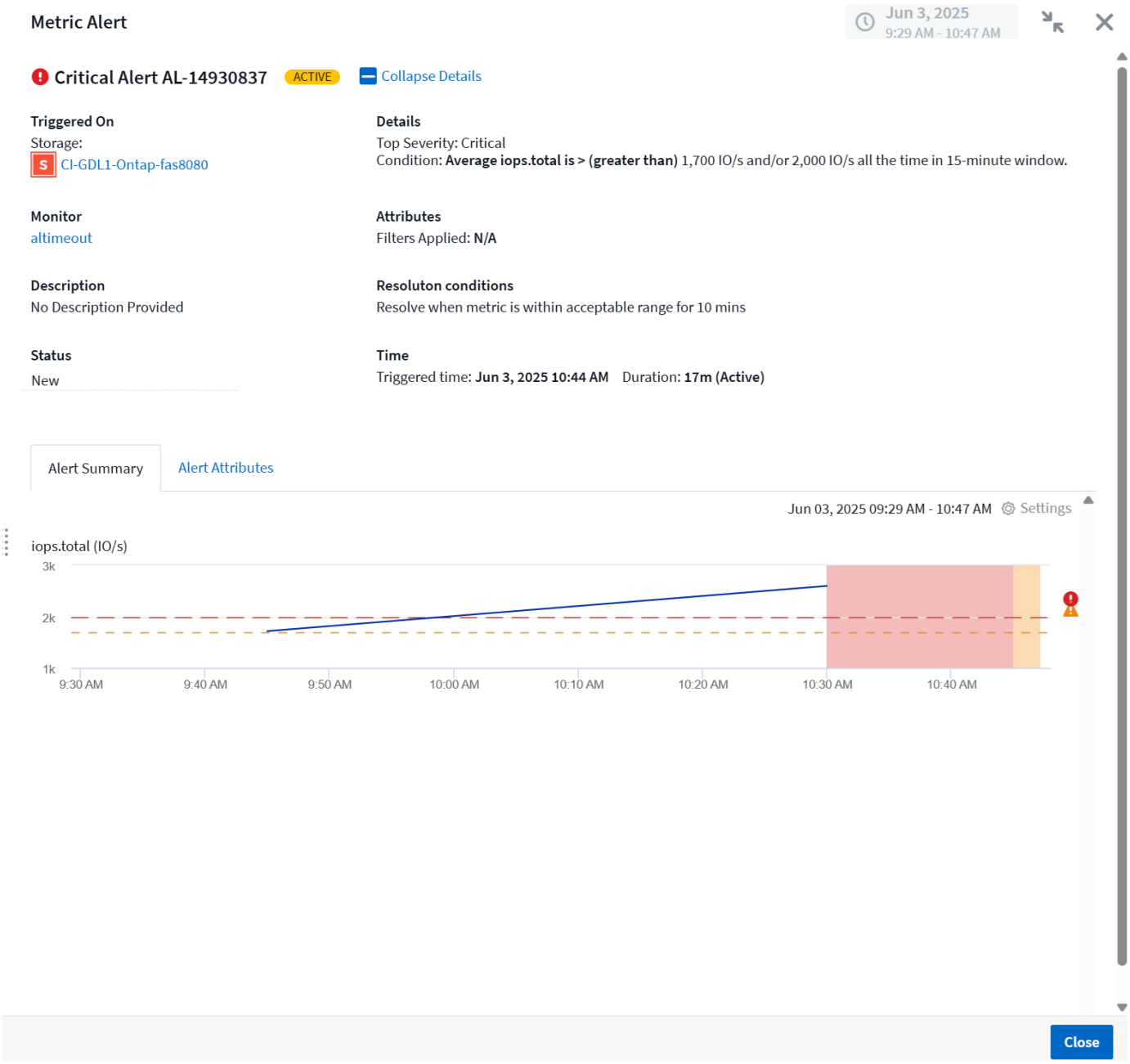
- 处理中 表示警报正在调查中或需要保持打开状态
- 关闭 从活动警报列表中删除警报。

您可以通过选中每个警报左侧的复选框并单击“更改选定警报状态”来管理多个警报。

单击警报 ID 将打开警报详细信息页面。

警报详细信息面板

选择任意警报行以打开警报的详细信息面板。警报详细信息面板提供有关警报的更多详细信息，包括_摘要_、显示与对象数据相关的图表的_性能_部分、任何_相关资产_以及警报调查员输入的_评论_。



数据丢失时发出警报

在诸如Data Infrastructure Insights之类的实时系统中，为了触发监视器的分析以决定是否应生成警报，我们依赖于以下两件事之一：

- 下一个到达的数据点
- 当没有数据点并且您已经等待了足够长的时间时触发的计时器

与数据到达缓慢或无数据到达的情况一样，计时器机制需要接管，因为数据到达率不足以“实时”触发警报。因此问题通常变成“我要等多久才能关闭分析窗口并查看我所拥有的内容？”如果等待的时间太长，则生成的警报速度不够快，无法发挥作用。

如果您有一个 30 分钟窗口的监视器，它注意到长期数据丢失之前的最后一个数据点违反了某个条件，则会生成警报，因为监视器没有收到其他信息来确认指标的恢复或注意到该条件持续存在。

“永久活动”警报

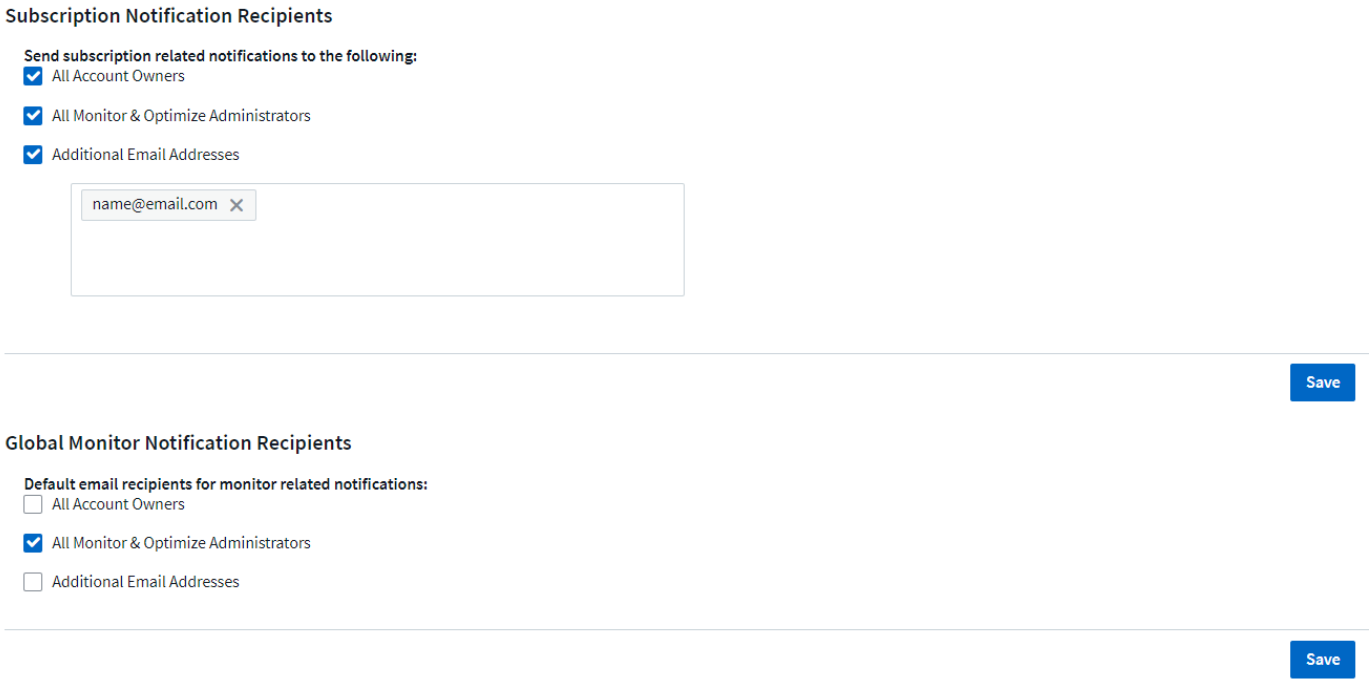
可以以这样的方式配置监视器，使条件*始终*存在于监视对象上 - 例如，IOPS > 1 或延迟 > 0。这些通常被创建为“测试”监视器，然后就被遗忘了。此类监视器会在组成对象上创建永久打开的警报，随着时间的推移，这可能会导致系统压力和稳定性问题。

为防止这种情况，Data Infrastructure Insights将在 7 天后自动关闭任何“永久活动”警报。请注意，底层监控条件可能（很可能会）继续存在，导致几乎立即发出新的警报，但关闭“始终活动”警报可以减轻可能发生的一些系统压力。

配置电子邮件通知

您可以配置与订阅相关的通知的电子邮件列表，以及用于通知性能策略阈值违规的收件人的全局电子邮件列表。

要配置通知电子邮件收件人设置，请转到*管理>通知*页面并选择_电子邮件_选项卡。



订阅通知收件人

要配置订阅相关事件通知的收件人，请转到“订阅通知收件人”部分。您可以选择将订阅相关事件的电子邮件通知发送给以下任何或所有收件人：

- 所有账户所有者
- 所有_监控和优化_管理员
- 您指定的其他电子邮件地址

以下是可能发送的通知类型以及您可以采取的用户操作的示例。

通知：	用户操作：

试用版或订阅版已更新	查看订阅详情"订阅"页
订阅将在 90 天后到期 订阅将在 30 天后到期	如果启用了“自动续订”，则无需采取任何行动，请联系NetApp销售人员续订
试用期将于 2 天后结束	续订试用版"订阅"页。您可以续订一次试用版。联系NetApp销售人员购买订阅
试用或订阅已过期 帐户将在 48 小时后停止收集数据 帐户将在 48 小时后被删除	联系NetApp销售人员购买订阅

为了确保您的收件人收到来自Data Infrastructure Insights的通知，请将以下电子邮件地址添加到任何“允许”列表中：

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

警报的全局收件人列表

对于针对警报采取的每个操作，都会向警报收件人列表发送警报的电子邮件通知。您可以选择向全球收件人列表发送警报通知。

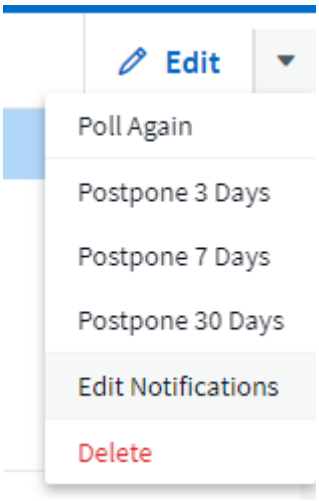
要配置全局警报收件人，请在“全局监控通知收件人”部分中选择所需的收件人。

在创建或修改监视器时，您始终可以覆盖单个监视器的全局收件人列表。

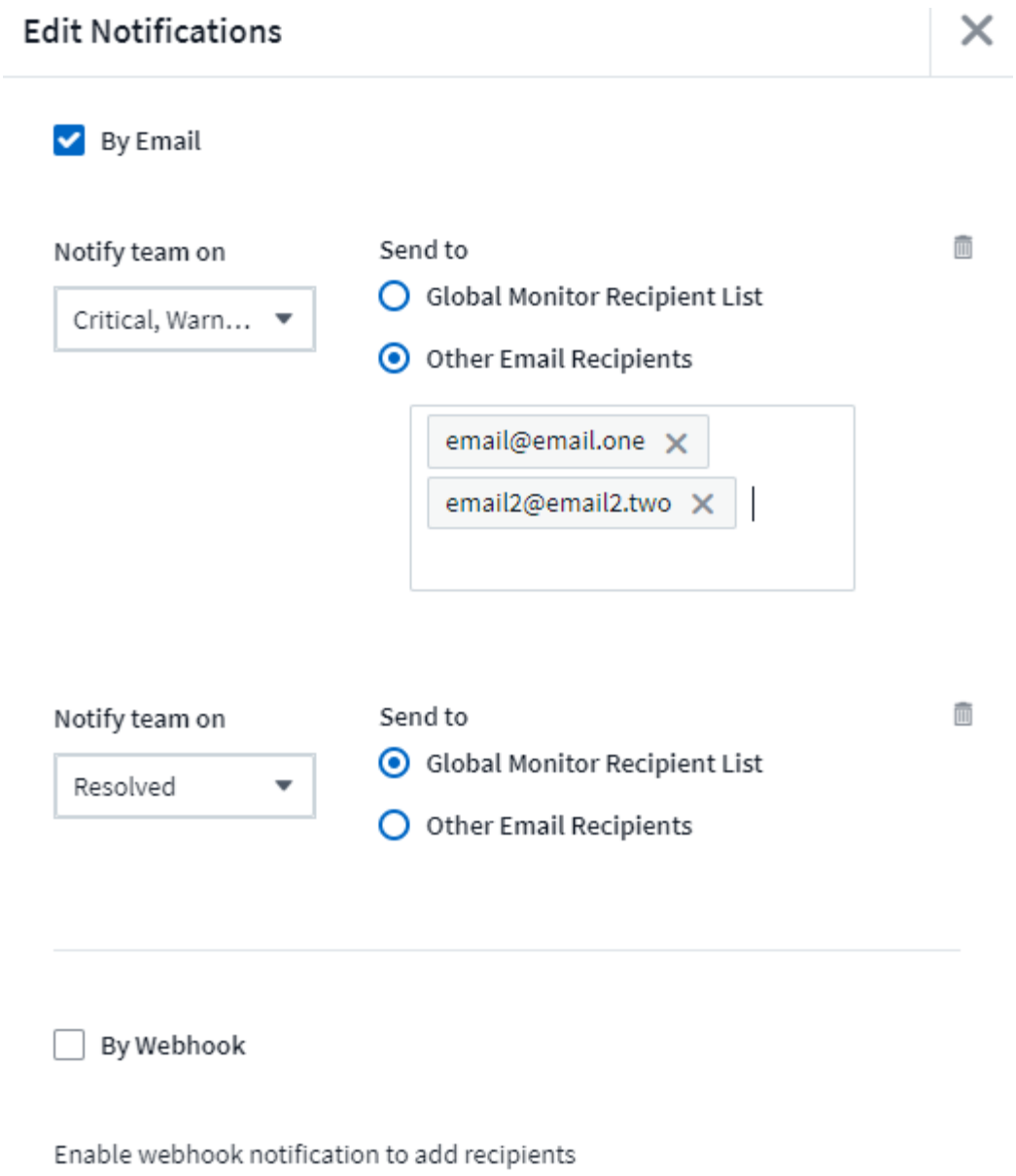
ONTAP数据收集器通知优先于与集群/数据收集器相关的任何特定监视器通知。您为数据收集器本身设置的收件人列表将接收数据收集器警报。如果没有活动的数据收集器警报，则监视器生成的警报将发送给特定的监视器接收者。

编辑ONTAP的通知

您可以通过从存储登录页面右上角的下拉菜单中选择“编辑通知”来修改ONTAP集群的通知。



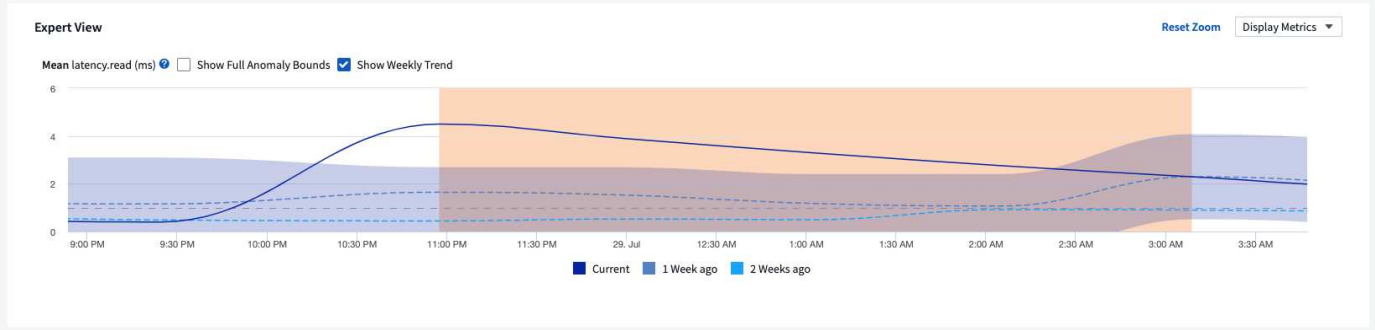
从这里，您可以设置严重、警告、信息和/或已解决警报的通知。每个场景都可以通知全局收件人列表或您选择的其他收件人。



异常检测监视器

异常检测可以洞察租户数据模式的意外变化。当对象的行为模式发生变化时，就会出现异常，例如，如果某个对象在星期三的某个时间经历了一定程度的延迟，但在接下来的星期三的那个时间延迟峰值超过了该水平，则该峰值将被视为异常。Data Infrastructure Insights允许创建监视器，以便在发生此类异常时发出警报。

异常检测适用于表现出重复、可预测模式的对象指标。当这些对象指标飙升至预期水平以上或以下时，Data Infrastructure Insights可以生成警报以提示调查。



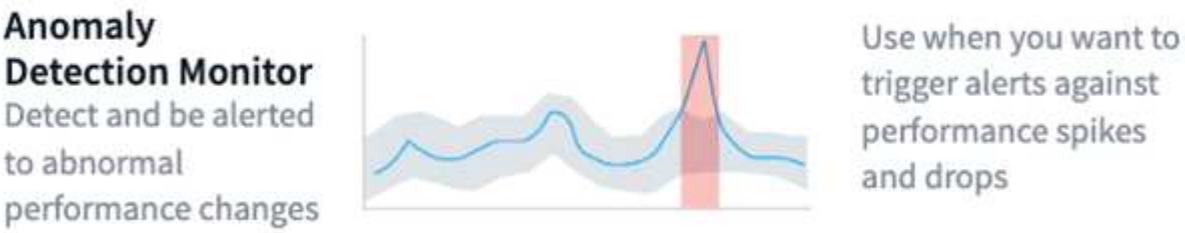
什么是异常检测?

当某个指标的平均值与前几周该指标的加权平均值相差若干个标准差，且最近几周的权重大于前几周时，就会出现异常。Data Infrastructure Insights提供监控数据并在检测到异常时发出警报的能力。您可以选择设置检测的“灵敏度”级别。例如，当平均值与平均值的标准差较小时，灵敏度会更高，从而导致生成更多警报。相反，敏感度越低 = 平均值的标准差越大 = 警报越少。

异常检测监控不同于阈值监控。

- 当您对特定指标有预定义阈值时，*基于阈值的监控*就会起作用。换句话说，当您清楚地了解预期结果（即在正常范围内）时。

- *异常检测监控*使用机器学习算法来识别偏离常态的异常值，用于“正常”的定义不明确的情况。



我什么时候需要异常检测?

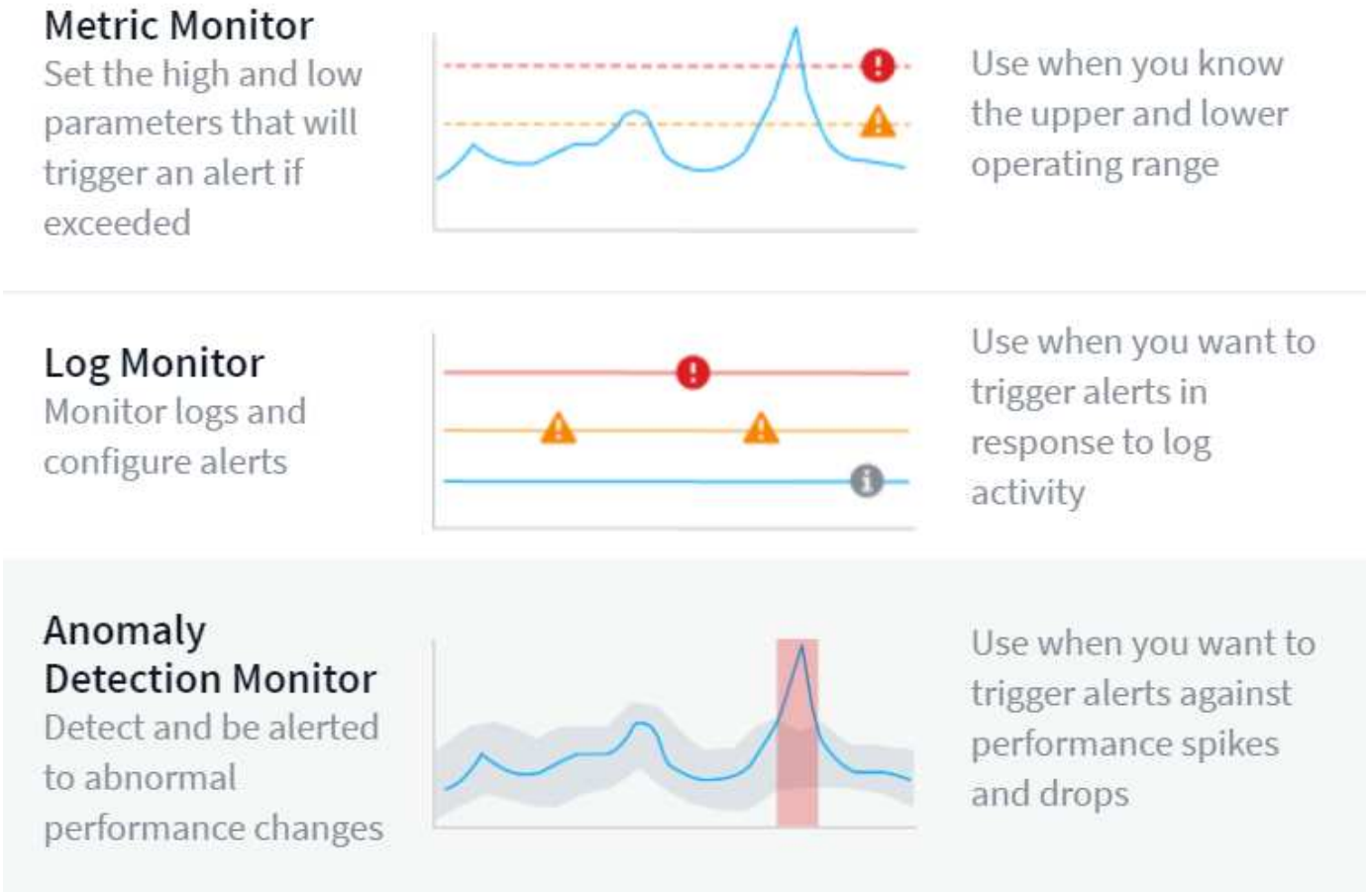
异常检测监控可以为许多情况提供有用的警报，包括以下情况：

- 当_正常_的定义不明确时。例如，SAN 错误率可能会根据端口的不同而有所不同。对一个错误发出警报是嘈杂且不必要的，但突然或显着的增加可能表明存在普遍的问题。
- 随着时间的推移，那里也发生了变化。表现出季节性的工作负载（即在某些时间繁忙或安静）。这可能包括可能表明批量停顿的意外安静期。

- 处理大量数据时，手动定义和调整阈值是不切实际的。例如，具有大量主机和/或具有不同工作负载的卷的租户。每个可能都有不同的 SLA，因此了解超出标准的 SLA 非常重要。

创建异常检测监视器

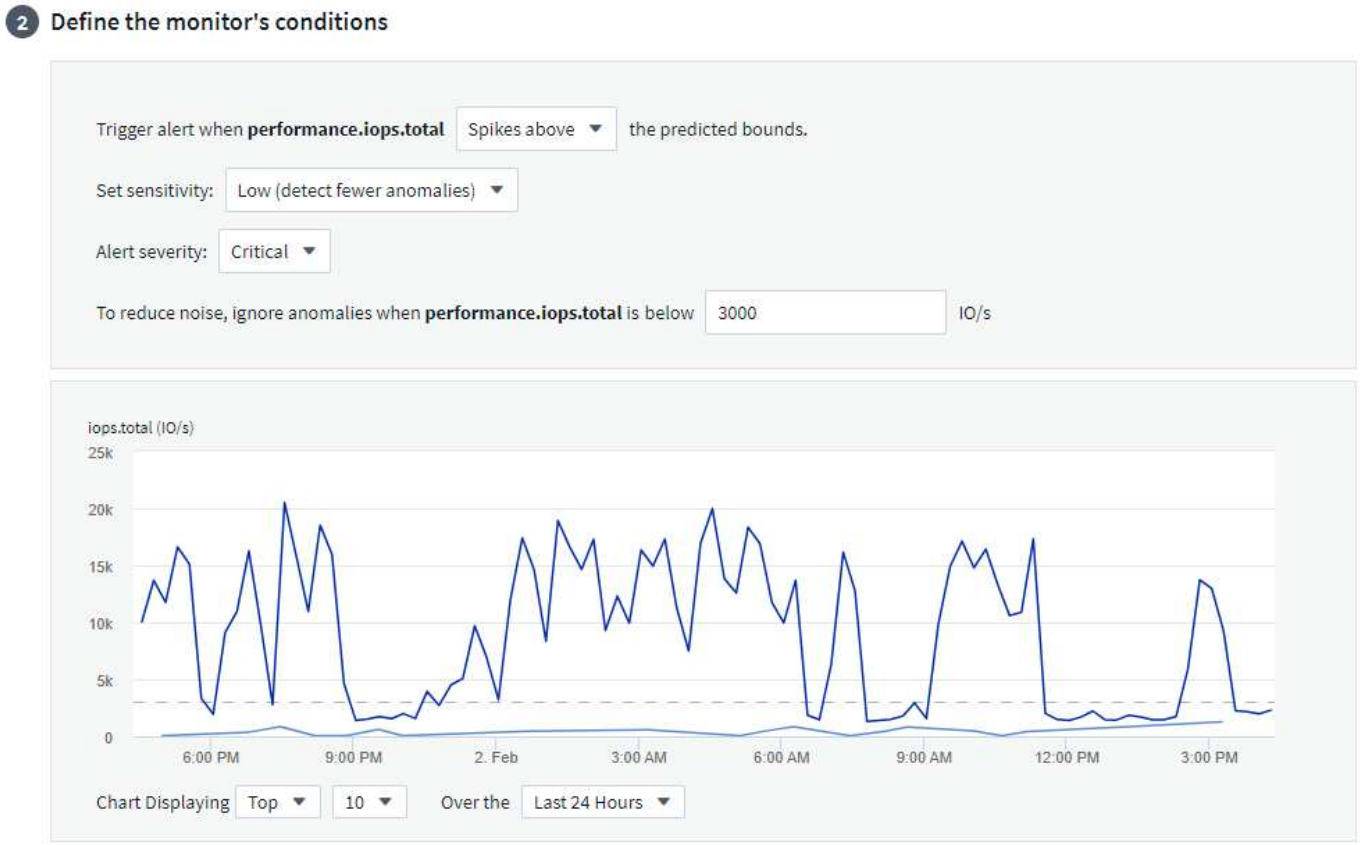
要对异常发出警报，请通过导航至 可观察性 **>** 警报 **>** **+**监控 来创建监控器。选择“异常检测监视器”作为监视器类型。



选择您想要监控的对象和指标。您可以像其他类型的监视器一样设置过滤器和分组。

接下来，设置监视器的条件。

- 当选定指标超出预测界限、低于该界限或两者兼而有之时，触发警报。
- 将敏感度设置为_中_、低（检测到较少异常）或_高_（检测到较多异常）。
- 确定警报级别是_严重_还是_警告_。
- 或者，设置一个值，低于该值时异常将被_忽略_。这有助于减少噪音。该值在示例图上显示为虚线。



最后，您可以配置警报的传送方式（电子邮件、Webhook 或两者），为监视器提供可选描述或纠正措施，并根据需要将监视器添加到自定义组。

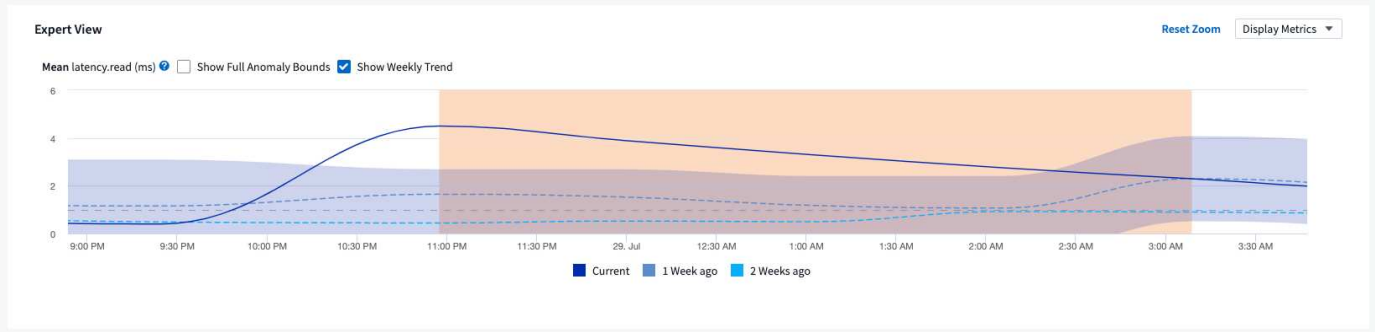
用一个有意义的名字保存监视器，就完成了。

创建后，监视器会分析前一周的数据以建立初始基线。随着时间的推移和更多历史记录的出现，异常检测变得更加准确。

> 创建监视器时，DII 会查看前一周的任何现有数据，以发现明显的数据峰值或下降；这些都被视为异常。在监视器创建后的第一周（“学习”阶段），警报中的“噪音”可能会增加。为了减轻这种噪音，只有持续时间超过 30 分钟的峰值或下降才会被视为异常并产生警报。在接下来的一周里，随着更多数据的分析，噪音通常会减少，并且持续一段时间的显著峰值或下降都将被视为异常。

查看异常

在警报登陆页面上，检测到异常时触发的警报将在图表中显示一个突出显示的带，从指标超出预测范围的时间到移回该范围之内的时间。



在警报登录页面上查看异常图表时，您可以选择以下选项：

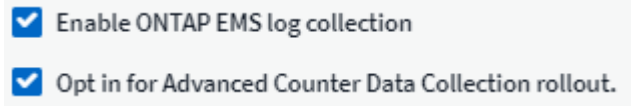
- 每周趋势：将值与前几周的同一时间、同一天进行比较，最多可比较前 5 周的值。
- 完整异常边界：默认情况下，图表关注指标值，以便您可以更好地分析指标行为。选择显示完整的异常边界（最大值等）

您还可以通过选择登录页面的性能部分中的对象来查看导致异常的对象。图表将显示所选对象的行为。

系统监视器

Data Infrastructure Insights包括许多系统定义的指标和日志监视器。可用的系统监视器取决于租户上的数据收集器。因此，随着数据收集器的添加或其配置的改变，Data Infrastructure Insights中可用的监视器可能会发生变化。

许多系统监视器默认处于_暂停_状态。您可以通过选择监视器的“*Resume*”选项来启用系统监视器。确保在数据收集器中启用了_高级计数器数据收集_和_启用ONTAP EMS 日志收集_。这些选项可以在ONTAP数据收集器的“高级配置”下找到



：

目录：[]

监视器描述

系统定义的监视器由预定义的指标和条件以及默认描述和纠正措施组成，这些都无法修改。您可以修改系统定义的监视器的通知收件人列表。要查看指标、条件、描述和纠正措施，或修改收件人列表，请打开系统定义的监视器组并点击列表中的监视器名称。

系统定义的监控组不能被修改或删除。

下列系统定义的监视器在注明的组中可用。

- * ONTAP基础架构* 包括对ONTAP集群中基础架构相关问题的监视器。
- * ONTAP工作负载示例* 包括工作负载相关问题的监视器。
- 两个组中的监视器默认处于_暂停_状态。

以下是Data Infrastructure Insights当前包含的系统监视器：

指标监视器

监视器名称	严重性	监视器描述	更正操作
光纤通道端口利用率高	严重	光纤通道协议端口用于接收和传输客户主机系统和ONTAP LUN 之间的 SAN 流量。如果端口利用率很高，那么它就会成为瓶颈，并最终影响光纤通道协议工作负载的敏感性能。…警告警报表明应采取计划措施来平衡网络流量。…严重警报表明服务中断即将发生，应采取紧急措施来平衡网络流量，以确保服务连续性。	如果突破了关键阈值，请考虑立即采取行动以尽量减少服务中断：1.将工作负载转移到另一个利用率较低的 FCP 端口。2.通过ONTAP中的 QoS 策略或主机端配置将某些 LUN 的流量限制在必要的工作范围内，以减轻 FCP 端口的利用率。…如果超出警告阈值，计划采取以下措施：1.配置更多 FCP 端口来处理数据流量，以便端口利用率分布在更多端口上。2.将工作负载转移到另一个利用率较低的 FCP 端口。3.通过ONTAP中的 QoS 策略或主机端配置将某些 LUN 的流量限制在必要的工作范围内，以减轻 FCP 端口的利用率。

Lun 延迟高	严重	LUN 是服务于 I/O 流量的对象，通常由性能敏感的应用程序（例如数据库）驱动。高 LUN 延迟意味着应用程序本身可能会受到影响并且无法完成其任务。…警告警报表示应采取计划的操作将 LUN 移动到适当的节点或聚合。…严重警报表示服务中断即将发生，应采取紧急措施以确保服务连续性。以下是基于介质类型的预期延迟 - SSD 最多 1-2 毫秒；SAS 最多 8-10 毫秒，SATA HDD 最多 17-20 毫秒	如果突破了关键阈值，请考虑采取以下措施以最大限度地减少服务中断：如果 LUN 或其卷具有与其关联的 QoS 策略，则评估其阈值限制并验证它们是否导致 LUN 工作负载受到限制。…如果超出警告阈值，计划采取以下措施：1.如果聚合也经历高利用率，则将 LUN 移动到另一个聚合。2.如果该节点也遇到高利用率，请将卷移动到另一个节点或减少该节点的总工作负载。3.如果 LUN 或其卷具有关联的 QoS 策略，请评估其阈值限制并验证它们是否导致 LUN 工作负载受到限制。
网络端口利用率高	严重	网络端口用于接收和传输客户主机系统和ONTAP卷之间的 NFS、CIFS 和 iSCSI 协议流量。如果端口利用率很高，那么它就会成为瓶颈，最终会影响 NFS、CIFS 和 iSCSI 工作负载的性能。…警告警报表明应采取计划措施来平衡网络流量。…严重警报表明服务中断即将发生，应采取紧急措施来平衡网络流量，以确保服务连续性。	如果突破了关键阈值，请考虑立即采取以下措施以尽量减少服务中断：1.通过ONTAP中的 QoS 策略或主机端分析将某些卷的流量限制在必要的工作范围内，以降低网络端口的利用率。2.配置一个或多个卷以使用另一个利用率较低的网络端口。…如果超出警告阈值，请考虑采取以下紧急措施：1.配置更多网络端口来处理数据流量，以便端口利用率分布在更多端口上。2.配置一个或多个卷以使用另一个利用率较低的网络端口。

NVMe 命名空间延迟高	严重	NVMe 命名空间是服务于由性能敏感型应用程序（例如数据库）驱动的 I/O 流量的对象。高 NVMe 命名空间延迟意味着应用程序本身可能会受到影响并且无法完成其任务。…警告警报表示应采取计划措施将 LUN 移动到适当的节点或聚合。…严重警报表示服务中断即将发生，应采取紧急措施以确保服务连续性。	如果突破了关键阈值，请考虑立即采取措施以尽量减少服务中断：如果 NVMe 命名空间或其卷分配了 QoS 策略，则评估其限制阈值，以防它们导致 NVMe 命名空间工作负载受到限制。…如果超出警告阈值，请考虑采取以下措施：1.如果聚合也经历高利用率，则将 LUN 移动到另一个聚合。2.如果该节点也遇到高利用率，请将卷移动到另一个节点或减少该节点的总工作负载。3.如果 NVMe 命名空间或其卷分配了 QoS 策略，请评估其限制阈值，以防它们导致 NVMe 命名空间工作负载受到限制。
QTree 容量已满	严重	qtree 是一种逻辑定义的文件系统，可以作为卷内根目录的特殊子目录存在。每个 qtree 都有一个默认空间配额或由配额策略定义的配额，以限制在卷容量范围内存储在树中的数据量。…警告警报表示应采取计划措施来增加空间。…严重警报表示服务中断即将发生，应采取紧急措施释放空间以确保服务连续性。	如果突破了关键阈值，请考虑立即采取行动以尽量减少服务中断：1.增加 qtree 的空间以适应增长。2.删除不需要的数据以释放空间。…如果超出警告阈值，计划立即采取以下措施：1.增加 qtree 的空间以适应增长。2.删除不需要的数据以释放空间。
QTree 容量硬限制	严重	qtree 是一种逻辑定义的文件系统，可以作为卷内根目录的特殊子目录存在。每个 qtree 都有一个以 KB 为单位的空间配额，用于存储数据，以控制用户数据量的增长，不超出其总容量。…qtree 维护一个软存储容量配额，在达到 qtree 中的总容量配额限制并且无法再存储数据之前主动向用户发出警报。监控 qtree 内存储的数据量可确保用户接收不间断的数据服务。	如果突破了关键阈值，请考虑立即采取以下措施以尽量减少服务中断：1.增加树木空间配额以适应增长2。指导用户删除树中不需要的数据以释放空间

QTree 容量软限制	警告	qtree 是一种逻辑定义的文件系统，可以作为卷内根目录的特殊子目录存在。每个 qtree 都有一个以 KB 为单位的空间配额，可用于存储数据，以控制用户数据量的增长，并且不超过其总容量。…qtree 维护一个软存储容量配额，在达到 qtree 中的总容量配额限制并且无法再存储数据之前主动向用户发出警报。监控 qtree 内存储的数据量可确保用户接收不间断的数据服务。	如果超出警告阈值，请考虑采取以下紧急措施：1.增加树木空间配额以适应生长。2.指导用户删除树中不需要的数据以释放空间。
QTree 文件硬限制	严重	qtree 是一种逻辑定义的文件系统，可以作为卷内根目录的特殊子目录存在。每个 qtree 都有一个可包含的文件数量配额，以维持卷内可管理的文件系统大小。…qtree 维护一个硬文件数量配额，超过该配额，树中的新文件将被拒绝。监控 qtree 内的文件数量可确保用户接收不间断的数据服务。	如果突破了关键阈值，请考虑立即采取行动以尽量减少服务中断：1.增加 qtree 的文件数配额。2.从 qtree 文件系统中删除不需要的文件。
QTree 文件软限制	警告	qtree 是一种逻辑定义的文件系统，可以作为卷内根目录的特殊子目录存在。每个 qtree 都有一个可包含的文件数量配额，以便在卷内维持可管理的文件系统大小。…qtree 维护一个软文件数配额，以便在达到 qtree 中的文件限制并且无法存储任何其他文件之前主动向用户发出警报。监控 qtree 内的文件数量可确保用户接收不间断的数据服务。	如果超出警告阈值，计划立即采取以下措施：1.增加 qtree 的文件数配额。2.从 qtree 文件系统中删除不需要的文件。

快照保留空间已满	严重	卷的存储容量对于存储应用程序和客户数据是必要的。该空间的一部分称为快照保留空间，用于存储允许在本地保护数据的快照。 ONTAP卷中存储的新数据和更新数据越多，使用的快照容量就越多，而可用于未来新数据或更新数据的快照存储容量就越少。如果卷内的快照数据容量达到总快照预留空间，则可能导致客户无法存储新的快照数据，并降低卷中数据的保护级别。监控卷使用的快照容量，确保数据服务的连续性。	如果突破了关键阈值，请考虑立即采取行动以尽量减少服务中断：1.配置快照以在快照保留已满时使用卷中的数据空间。2.删除一些不需要的旧快照以释放空间。…如果超出警告阈值，计划立即采取以下措施：1.增加卷内的快照保留空间以适应增长。2.配置快照以在快照保留已满时使用卷中的数据空间。
存储容量限制	严重	当存储池（聚合）填满时，I/O 操作会减慢并最终停止，从而导致存储中断事件。警告警报表明应尽快采取计划措施来恢复最小可用空间。严重警报表示服务即将中断，应采取紧急措施释放空间以确保服务连续性。	如果突破临界阈值，请立即考虑采取以下措施以尽量减少服务中断：1.删除非关键卷上的快照。2.删除非必要工作负载且可从存储副本中恢复的卷或LUN。……如果超过警告阈值，请计划立即采取以下措施：1.将一个或多个卷移动到其他存储位置。2.添加更多存储容量。3.更改存储效率设置或将非活动数据分层到云存储。
存储性能限制	严重	当存储系统达到其性能极限时，操作速度会变慢，延迟会增加，工作负载和应用程序可能会开始出现故障。 ONTAP评估工作负载的存储池利用率，并估计已消耗的性能百分比。…警告警报表示应采取计划措施来减少存储池负载，以确保有足够的存储池性能来满足工作负载峰值。…严重警报表示即将发生性能下降，应采取紧急措施来减少存储池负载，以确保服务连续性。	如果突破了关键阈值，请考虑立即采取以下措施以尽量减少服务中断：1.暂停快照或SnapMirror复制等计划任务。2.闲置非必要的工作负载。…如果超出警告阈值，请立即采取以下措施：1.将一个或多个工作负载移动到不同的存储位置。2.添加更多存储节点（AFF）或磁盘架（FAS）并重新分配工作负载3。改变工作负载特征（块大小、应用程序缓存）。

用户配额容量硬限制	严重	ONTAP可识别有权访问卷、卷内的文件或目录的 Unix 或 Windows 系统用户。因此， ONTAP允许客户为其 Linux 或 Windows 系统的用户或用户组配置存储容量。用户或组策略配额限制了用户可以用于其自身数据的空间量……此配额的硬限制允许在卷中使用的容量即将达到总容量配额时通知用户。监控用户或组配额内存储的数据量可确保用户获得不间断的数据服务。	如果突破了关键阈值，请考虑立即采取以下措施以尽量减少服务中断：1.增加用户或组配额的空间以适应增长。2.指示用户或组删除不需要的数据以释放空间。
用户配额容量软限制	警告	ONTAP可识别有权访问卷、卷内的文件或目录的 Unix 或 Windows 系统用户。因此， ONTAP允许客户为其 Linux 或 Windows 系统的用户或用户组配置存储容量。用户或组策略配额限制了用户可以用于其自身数据的空间量……当卷中使用的容量量达到总容量配额时，此配额的软限制允许主动通知用户。监控用户或组配额内存储的数据量可确保用户获得不间断的数据服务。	如果超出警告阈值，计划立即采取以下措施：1.增加用户或组配额的空间以适应增长。2.删除不需要的数据以释放空间。
卷容量已满	严重	卷的存储容量对于存储应用程序和客户数据是必要的。 ONTAP卷中存储的数据越多，未来数据的可用存储空间就越少。如果卷内的数据存储容量达到总存储容量，可能会导致客户因存储容量不足而无法存储数据。监控已用存储容量可确保数据服务的连续性。	如果突破了关键阈值，请考虑立即采取以下措施以尽量减少服务中断：1.增加卷的空间以适应增长。2.删除不需要的数据以释放空间。3.如果快照副本占用的空间超过快照保留空间，请删除旧快照或启用卷快照自动删除。…如果超过警告阈值，请计划立即采取以下措施：1.增加体积的空间以适应增长2。如果快照副本占用的空间超过快照保留空间，请删除旧快照或启用卷快照自动删除。……

卷 Inode 限制	严重	存储文件的卷使用索引节点（inode）来存储文件元数据。当卷耗尽其 inode 分配时，将无法再向其中添加文件。…警告警报表示应采取计划措施来增加可用的 inode 数量。…严重警报表示文件限制即将耗尽，应采取紧急措施释放 inode 以确保服务连续性。	如果突破了关键阈值，请考虑立即采取以下措施以尽量减少服务中断：1.增加卷的 inode 值。如果 inode 值已经达到最大值，则将卷拆分为两个或多个卷，因为文件系统已超出最大大小。2.使用FlexGroup因为它有助于容纳大型文件系统。…如果超出警告阈值，计划立即采取以下措施：1.增加卷的 inode 值。如果 inode 值已经达到最大值，则将卷拆分为两个或多个卷，因为文件系统已超出最大大小。2.使用FlexGroup ，因为它有助于容纳大型文件系统
卷延迟高	严重	卷是服务于 I/O 流量的对象，这些流量通常由性能敏感的应用程序（包括 devOps 应用程序、主目录和数据库）驱动。高容量延迟意味着应用程序本身可能会受到影响并且无法完成其任务。监控卷延迟对于维持应用程序的一致性能至关重要。以下是基于媒体类型的预期延迟 - SSD 最多 1-2 毫秒；SAS 最多 8-10 毫秒，SATA HDD 最多 17-20 毫秒。	如果突破了关键阈值，请考虑立即采取以下措施以尽量减少服务中断：如果卷分配了 QoS 策略，请评估其限制阈值，以防它们导致卷工作负载受到限制。…如果超出警告阈值，请考虑采取以下紧急措施：1.如果聚合体的利用率也很高，则将卷移动到另一个聚合体。2.如果卷分配了 QoS 策略，请评估其限制阈值，以防它们导致卷工作负载受到限制。3.如果该节点也遇到高利用率，请将卷移动到另一个节点或减少该节点的总工作负载。
监视器名称	严重性	监视器描述	更正操作

节点高延迟	警告/严重	节点延迟已达到可能影响节点上应用程序性能的水平。较低的节点延迟确保应用程序的一致性能。基于媒体类型的预期延迟为：SSD 最多 1-2 毫秒；SAS 最多 8-10 毫秒，SATA HDD 最多 17-20 毫秒。	如果突破了关键阈值，则应立即采取措施以尽量减少服务中断：1.暂停计划任务、快照或SnapMirror复制 2.通过 QoS 限制 3 降低低优先级工作负载的需求。停止非必要的工作负载 当警告阈值被突破时考虑立即采取行动：1.将一个或多个工作负载移动到不同的存储位置2.通过 QoS 限制 3 降低低优先级工作负载的需求。添加更多存储节点（AFF）或磁盘架（FAS）并重新分配工作负载4.改变工作负载特征（块大小、应用程序缓存等）
节点性能限制	警告/严重	节点性能利用率已达到可能影响 IO 和节点支持的应用程序的性能的水平。低节点性能利用率确保应用程序的一致性能。	如果突破临界阈值，应立即采取措施尽量减少服务中断：1.暂停计划任务、快照或SnapMirror复制 2.通过 QoS 限制 3 降低低优先级工作负载的需求。停用非必要工作负载如果超出警告阈值，请考虑采取以下措施：1.将一个或多个工作负载移动到不同的存储位置2.通过 QoS 限制 3 降低低优先级工作负载的需求。添加更多存储节点（AFF）或磁盘架（FAS）并重新分配工作负载4.改变工作负载特征（块大小、应用程序缓存等）
存储虚拟机高延迟	警告/严重	存储虚拟机 (SVM) 延迟已达到可能影响存储虚拟机上应用程序性能的水平。较低的存储虚拟机延迟可确保应用程序的一致性能。基于媒体类型的预期延迟为：SSD 最多 1-2 毫秒；SAS 最多 8-10 毫秒，SATA HDD 最多 17-20 毫秒。	如果超过临界阈值，则立即评估分配了 QoS 策略的存储虚拟机卷的阈值限制，以验证它们是否导致卷工作负载受到限制。当超过警告阈值时，请考虑立即采取以下措施：1.如果聚合也经历高利用率，请将存储虚拟机的某些卷移动到另一个聚合。2.对于分配了 QoS 策略的存储虚拟机的卷，评估阈值限制是否导致卷工作负载受到限制 3。如果节点利用率过高，请将存储虚拟机的某些卷移动到另一个节点或减少节点的总工作负载

用户配额文件硬限制	严重	卷内创建的文件数量已达到临界限制，无法创建更多文件。监控存储的文件数量可确保用户获得不间断的数据服务。	如果突破临界阈值，则需要立即采取行动，尽量减少服务中断……考虑采取以下行动：1.增加特定用户的文件数配额2。删除不需要的文件以减少特定用户的文件配额压力
用户配额文件软限制	警告	卷内创建的文件数量已达到配额的阈值限制，并且接近临界限制。如果配额达到临界限制，则无法创建其他文件。监控用户存储的文件数量可确保用户获得不间断的数据服务。	如果超出警告阈值，请考虑立即采取行动：1.增加特定用户配额2的文件数配额。删除不需要的文件以减少特定用户的文件配额压力
卷缓存未命中率	警告/严重	卷缓存未命中率是来自客户端应用程序的读取请求中从磁盘返回而不是从缓存返回的百分比。这意味着音量已经达到设定的阈值。	如果突破了关键阈值，则应立即采取措施以尽量减少服务中断：1.将一些工作负载移出卷的节点以减少 IO 负载 2.如果卷节点上尚未安装 Flash Cache 3，请通过购买和添加 Flash Cache 3 来增加WAFL缓存。通过 QoS 限制降低同一节点上较低优先级工作负载的需求 当警告阈值被突破时考虑立即采取行动：1.将一些工作负载移出卷的节点以减少 IO 负载 2.如果卷节点上尚未安装 Flash Cache 3，请通过购买和添加 Flash Cache 3 来增加WAFL缓存。通过QoS限制4降低同一节点上低优先级工作负载的需求。改变工作负载特征（块大小、应用程序缓存等）
卷 Qtree 配额过量使用	警告/严重	卷 Qtree 配额过载指定卷被视为被 qtree 配额过载的百分比。已达到卷的 qtree 配额设置的阈值。监控卷 qtree 配额过量提交可确保用户获得不间断的数据服务。	如果突破了关键阈值，则应立即采取措施以尽量减少服务中断：1.增加卷 2 的空间。删除不需要的数据当超过警告阈值时，考虑增加卷的空间。

返回顶部

日志监视器

监视器名称	严重性	描述	更正操作

AWS 凭证未初始化	INFO	当模块在初始化之前尝试从云凭证线程访问 Amazon Web Services (AWS) 身份和访问管理 (IAM) 基于角色的凭证时，会发生此事件。	等待云凭证线程以及系统完成初始化。
无法访问云层	严重	存储节点无法连接到 Cloud Tier 对象存储 API。某些数据将无法访问。	如果您使用本地产品，请执行以下纠正措施：…使用“network interface show”命令验证集群间 LIF 是否在线且正常运行。…通过目标节点集群间 LIF 使用“ping”命令检查与对象存储服务器的网络连接。…确保以下事项：…对象存储的配置未更改。…登录和连接信息仍然有效。…如果问题仍然存在，请联系NetApp技术支持。如果您使用Cloud Volumes ONTAP，请执行以下纠正措施：…确保对象存储的配置没有更改。…确保登录和连接信息仍然有效。…如果问题仍然存在，请联系NetApp技术支持。
磁盘停止服务	INFO	当磁盘因被标记为故障、正在被清理或已进入维护中心而被从服务中移除时，会发生此事件。	无。
FlexGroup完整组成部分	严重	FlexGroup卷内的某个组成部分已满，这可能会导致服务中断。您仍然可以在FlexGroup卷上创建或扩展文件。但是，存储在组件上的任何文件都不能被修改。因此，当您尝试在FlexGroup卷上执行写入操作时，可能会看到随机的空间不足错误。	建议您使用“volume modify -files +X”命令为FlexGroup卷添加容量。…或者，从FlexGroup卷中删除文件。然而，很难确定哪些文件已经落入选民手中。
Flexgroup 成分股已接近饱和	警告	FlexGroup卷内的某个组成部分的空间几乎用尽，这可能会导致服务中断。可以创建和扩展文件。但是，如果组成部分空间不足，您可能无法附加或修改组成部分上的文件。	建议您使用“volume modify -files +X”命令为FlexGroup卷添加容量。…或者，从FlexGroup卷中删除文件。然而，很难确定哪些文件已经落入选民手中。

FlexGroup组成部分的 Inode 即将耗尽	警告	FlexGroup卷中的某个组成部分的 inode 几乎用完了，这可能会导致服务中断。该选民收到的创作请求比平均水平要少。这可能会影响FlexGroup卷的整体性能，因为请求被路由到具有更多 inode 的组成部分。	建议您使用“volume modify -files +X”命令为FlexGroup卷添加容量。…或者，从FlexGroup卷中删除文件。然而，很难确定哪些文件已经落入选民手中。
FlexGroup组成 Inode	严重	FlexGroup卷的组成部分的 inode 已用完，这可能会导致服务中断。您不能在此组成部分上创建新文件。这可能会导致整个FlexGroup卷中内容的整体分布不平衡。	建议您使用“volume modify -files +X”命令为FlexGroup卷添加容量。…或者，从FlexGroup卷中删除文件。然而，很难确定哪些文件已经落入选民手中。
LUN 脱机	INFO	当 LUN 手动脱机时会发生此事件。	使 LUN 重新联机。
主机风扇故障	警告	一个或多个主机风扇发生故障。系统仍在运行……但是，如果这种情况持续太长时间，过热可能会触发自动关机。	重新安装发生故障的风扇。如果错误仍然存在，请更换它们。
主机风扇处于警告状态	INFO	当一个或多个主机风扇处于警告状态时，就会发生此事件。	更换指示的风扇以避免过热。
NVRAM 电池电量低	警告	NVRAM电池容量严重不足。如果电池电量耗尽，可能会有数据丢失。…您的系统会生成并传输AutoSupport或“呼叫回家”消息给NetApp技术支持和配置的目的地（如果已配置）。 AutoSupport消息的成功传递显著提高了问题的确定和解决能力。	执行以下操作：…使用“system node environment sensors show”命令查看电池的当前状态、容量和充电状态。…如果最近更换了电池或系统长时间未运行，请监控电池以验证其是否正常充电。…如果电池运行时间持续下降到临界水平以下，并且存储系统自动关闭，请联系NetApp技术支持。

未配置服务处理器	警告	此事件每周发生一次，以提醒您配置服务处理器(SP)。 SP是集成到系统中的物理设备，用于提供远程访问和远程管理功能。您应该配置SP以使用其全部功能。	执行以下纠正措施：…使用“system service-processor network modify”命令配置SP 。…或者，使用“system service-processor network show”命令获取SP的 MAC 地址。…使用“system service-processor network show”命令验证SP网络配置。…使用“system service-processor autosupport invoke”命令验证SP是否可以发送AutoSupport电子邮件。注意：在发出此命令之前，应在ONTAP中配置AutoSupport电子邮件主机和收件人。
服务处理器脱机	严重	即使已采取所有SP恢复操作， ONTAP也不再接收来自服务处理器 (SP) 的心跳。如果没有SP ，ONTAP就无法监控硬件的健康状况……系统将关闭以防止硬件损坏和数据丢失。设置紧急警报，以便在SP离线时立即收到通知。	通过执行以下操作对系统进行电源循环：…将控制器从机箱中拉出。…将控制器推回。…重新打开控制器。…如果问题仍然存在，请更换控制器模块。
搁架风扇故障	严重	指示的机架冷却风扇或风扇模块发生故障。磁盘架中的磁盘可能无法获得足够的冷却气流，这可能会导致磁盘故障。	执行以下操作纠正措施：…验证风扇模块是否完全就位并固定。注意：某些磁盘架的电源模块中集成了风扇。…如果问题仍然存在，请更换风扇模块。…如果问题仍然存在，请联系NetApp技术支持寻求帮助。
由于主机风扇故障，系统无法运行	严重	一个或多个主机风扇发生故障，导致系统运行中断。这可能会导致潜在的数据丢失。	更换发生故障的风扇。
未分配磁盘	INFO	系统有未分配的磁盘 - 容量被浪费，并且您的系统可能存在一些错误配置或应用了部分配置更改。	执行以下纠正措施：…使用“disk show -n”命令确定哪些磁盘未分配。…使用“disk assign”命令将磁盘分配给系统。
防病毒服务器繁忙	警告	防病毒服务器太忙，无法接受任何新的扫描请求。	如果此消息频繁出现，请确保有足够的防病毒服务器来处理 SVM 生成的病毒扫描负载。

IAM 角色的 AWS 凭证已过期	严重	Cloud Volume ONTAP已无法访问。身份和访问管理 (IAM) 基于角色的凭证已过期。凭证是使用 IAM 角色从 Amazon Web Services (AWS) 元数据服务器获取的，并用于签署对 Amazon Simple Storage Service (Amazon S3) 的 API 请求。	执行以下操作：…登录到 AWS EC2 管理控制台。…导航到实例页面。…找到Cloud Volumes ONTAP部署的实例并检查其运行状况。…验证与实例关联的 AWS IAM 角色是否有效以及是否已被授予该实例的适当权限。
未找到 IAM 角色的 AWS 凭证	严重	云凭证线程无法从 AWS 元数据服务器获取基于 Amazon Web Services (AWS) 身份和访问管理 (IAM) 角色的凭证。这些凭证用于签署对 Amazon Simple Storage Service (Amazon S3) 的 API 请求。 Cloud Volume ONTAP已无法访问。…	执行以下操作：…登录到 AWS EC2 管理控制台。…导航到实例页面。…找到Cloud Volumes ONTAP部署的实例并检查其运行状况。…验证与实例关联的 AWS IAM 角色是否有效以及是否已被授予该实例的适当权限。
IAM 角色的 AWS 凭证无效	严重	身份和访问管理 (IAM) 基于角色的凭证无效。凭证是使用 IAM 角色从 Amazon Web Services (AWS) 元数据服务器获取的，并用于签署对 Amazon Simple Storage Service (Amazon S3) 的 API 请求。 Cloud Volume ONTAP已无法访问。	执行以下操作：…登录到 AWS EC2 管理控制台。…导航到实例页面。…找到Cloud Volumes ONTAP部署的实例并检查其运行状况。…验证与实例关联的 AWS IAM 角色是否有效以及是否已被授予该实例的适当权限。
未找到 AWS IAM 角色	严重	身份和访问管理 (IAM) 角色线程无法在 AWS 元数据服务器上找到 Amazon Web Services (AWS) IAM 角色。需要 IAM 角色来获取用于签署对 Amazon Simple Storage Service (Amazon S3) 的 API 请求的基于角色的凭证。 Cloud Volume ONTAP已无法访问。…	执行以下操作：…登录到 AWS EC2 管理控制台。…导航到实例页面。…找到Cloud Volumes ONTAP部署的实例并检查其运行状况。…验证与实例关联的 AWS IAM 角色是否有效。
AWS IAM 角色无效	严重	AWS 元数据服务器上的 Amazon Web Services (AWS) 身份和访问管理 (IAM) 角色无效。 Cloud Volume ONTAP已无法访问。…	执行以下操作：…登录到 AWS EC2 管理控制台。…导航到实例页面。…找到Cloud Volumes ONTAP部署的实例并检查其运行状况。…验证与实例关联的 AWS IAM 角色是否有效以及是否已被授予该实例的适当权限。

AWS 元数据服务器连接失败	严重	身份和访问管理 (IAM) 角色线程无法与 Amazon Web Services (AWS) 元数据服务器建立通信链接。应该建立通信以获取用于签署对 Amazon Simple Storage Service (Amazon S3) 的 API 请求的必要的 AWS IAM 基于角色的凭证。 Cloud Volume ONTAP已无法访问。…	执行以下操作：…登录到 AWS EC2 管理控制台。…导航到“实例”页面。…找到Cloud Volumes ONTAP部署的实例并检查其运行状况。…
FabricPool空间使用限制即将达到	警告	来自容量许可提供商的对象存储的集群范围FabricPool空间总使用量已接近许可限制。	执行以下纠正措施：…使用“storage aggregate object-store show-space”命令检查每个FabricPool存储层使用的许可容量百分比。…使用“volume snapshot delete”命令从分层策略为“snapshot”或“backup”的卷中删除 Snapshot 副本以清理空间。…在集群上安装新许可证以增加许可容量。
FabricPool空间使用限制已达到	严重	来自容量许可提供商的对象存储的集群范围FabricPool空间总使用量已达到许可限制。	执行以下纠正措施：…使用“storage aggregate object-store show-space”命令检查每个FabricPool存储层使用的许可容量百分比。…使用“volume snapshot delete”命令从分层策略为“snapshot”或“backup”的卷中删除 Snapshot 副本以清理空间。…在集群上安装新许可证以增加许可容量。

聚合返回失败	严重	此事件发生在聚合迁移期间，作为存储故障转移 (SFO) 恢复的一部分，此时目标节点无法到达对象存储。	执行以下纠正措施：…使用“network interface show”命令验证集群间 LIF 是否在线且正常运行。…通过目标节点集群间 LIF 使用“ping”命令检查与对象存储服务器的网络连接。…使用“aggregate object-store config show”命令验证对象存储的配置未更改，并且登录和连接信息仍然准确。…或者，您可以通过为 giveback 命令的“require-partner-waiting”参数指定 false 来覆盖错误。…请联系NetApp技术支持以获取更多信息或帮助。
HA 互连中断	警告	高可用性 (HA) 互连已中断。当故障转移不可用时，存在服务中断的风险。	纠正措施取决于平台支持的 HA 互连链路的数量和类型，以及互连中断的原因。 …如果链路中断：…验证 HA 对中的两个控制器是否正常运行。…对于外部连接的链路，请确保互连电缆已正确连接，并且小型可插拔设备 (SFP)（如果适用）已正确安装在两个控制器上。…对于内部连接的链路，使用“ic link off”和“ic link on”命令依次禁用并重新启用链路。…如果链接被禁用，请使用“ic link on”命令启用链接。 …如果对等方未连接，请使用“ic link off”和“ic link on”命令逐个禁用并重新启用链接。…如果问题仍然存在，请联系NetApp技术支持。

超出每个用户的最大会话数	警告	您已超出 TCP 连接上每个用户允许的最大会话数。任何建立会话的请求都将被拒绝，直到某些会话被释放。 …	执行以下纠正措施：…检查客户端上运行的所有应用程序，并终止任何运行不正常的应用程序。…重新启动客户端。…检查问题是由新应用程序还是现有应用程序引起的：…如果应用程序是新的，请使用“cifs option modify -max-opens-same-file-per-tree”命令为客户端设置更高的阈值。在某些情况下，客户端会按预期运行，但需要更高的阈值。您应该具有高级权限来为客户端设置更高的阈值。 …如果问题是由现有应用程序引起的，则客户端可能存在问题。请联系NetApp技术支持以获取更多信息或帮助。
超出每个文件的最大打开次数	警告	您已超出通过 TCP 连接打开文件的最大次数。任何打开此文件的请求都将被拒绝，直到您关闭该文件的某些打开实例。这通常表示应用程序行为异常。…	执行以下纠正措施：…检查使用此 TCP 连接在客户端上运行的应用程序。客户端可能由于其上运行的应用程序而运行不正常。…重新启动客户端。…检查问题是由新应用程序还是现有应用程序引起的：…如果应用程序是新的，请使用“cifs option modify -max-opens-same-file-per-tree”命令为客户端设置更高的阈值。在某些情况下，客户端会按预期运行，但需要更高的阈值。您应该具有高级权限来为客户端设置更高的阈值。 …如果问题是由现有应用程序引起的，则客户端可能存在问题。请联系NetApp技术支持以获取更多信息或帮助。

NetBIOS 名称冲突	严重	NetBIOS 名称服务已从远程计算机收到对名称注册请求的否定响应。这通常是由于 NetBIOS 名称或别名冲突引起的。结果，客户端可能无法访问数据或连接到集群中正确的数据服务节点。	执行以下任一纠正措施：…如果 NetBIOS 名称或别名存在冲突，请执行以下操作之一：…使用“vserver cifs delete -aliases alias -vserver vserver”命令删除重复的 NetBIOS 别名。…通过删除重复的名称并使用“vserver cifs create -aliases alias -vserver vserver”命令添加具有新名称的别名来重命名 NetBIOS 别名。 …如果没有配置别名并且 NetBIOS 名称存在冲突，则使用“vserver cifs delete -vserver vserver”和“vserver cifs create -cifs -server netbiosname”命令重命名 CIFS 服务器。注意：删除 CIFS 服务器可能会导致数据无法访问。…删除 NetBIOS 名称或重命名远程计算机上的 NetBIOS。
NFSv4 存储池已耗尽	严重	NFSv4 存储池已耗尽。	如果 NFS 服务器在此事件发生后超过 10 分钟没有响应，请联系NetApp技术支持。
未注册扫描引擎	严重	防病毒连接器通知ONTAP它没有注册的扫描引擎。如果启用“强制扫描”选项，这可能会导致数据不可用。	执行以下纠正措施：…确保安装在防病毒服务器上的扫描引擎软件与ONTAP兼容。…确保扫描引擎软件正在运行并配置为通过本地环回连接到防病毒连接器。
无 Vscan 连接	严重	ONTAP没有 Vscan 连接来处理病毒扫描请求。如果启用“强制扫描”选项，这可能会导致数据不可用。	确保扫描仪池配置正确，并且防病毒服务器处于活动状态并连接到ONTAP。
节点根卷空间低	严重	系统检测到根卷的空间严重不足。该节点尚未完全运行。数据 LIF 可能已在集群内进行故障转移，因此节点上的 NFS 和 CIFS 访问受到限制。管理能力仅限于节点的本地恢复程序，以清理根卷上的空间。	执行以下纠正措施：…通过删除旧的 Snapshot 副本、从 /mroot 目录中删除不再需要的文件或扩展根卷容量来清理根卷上的空间。…重新启动控制器。…联系NetApp技术支持以获取更多信息或帮助。

不存在的管理员共享	严重	Vscan 问题：客户端尝试连接到不存在的 ONTAP_ADMIN$ 共享。	确保已为提到的 SVM ID 启用 Vscan。在 SVM 上启用 Vscan 会导致自动为 SVM 创建 ONTAP_ADMIN$ 共享。
NVMe 命名空间不足	严重	由于空间不足导致写入失败，NVMe 命名空间已脱机。	向卷添加空间，然后使用“vserver nvme namespace modify”命令使 NVMe 命名空间联机。
NVMe-oF 宽限期处于活动状态	警告	当使用 NVMe over Fabrics (NVMe-oF) 协议且许可证的宽限期处于活动状态时，此事件每天都会发生。许可证宽限期到期后，NVMe-oF 功能需要许可证。许可宽限期结束后，NVMe-oF 功能将被禁用。	联系您的销售代表以获取 NVMe-oF 许可证，并将其添加到集群中，或者从集群中删除所有 NVMe-oF 配置实例。
NVMe-oF 宽限期已结束	警告	NVMe over Fabrics (NVMe-oF) 许可宽限期已结束，NVMe-oF 功能已被禁用。	联系您的销售代表获取 NVMe-oF 许可证，并将其添加到集群中。
NVMe-oF 宽限期开始	警告	在升级到ONTAP 9.5 软件期间检测到 NVMe over Fabrics (NVMe-oF) 配置。许可证宽限期到期后，NVMe-oF 功能需要许可证。	联系您的销售代表获取 NVMe-oF 许可证，并将其添加到集群中。
对象存储主机无法解析	严重	对象存储服务器主机名无法解析为 IP 地址。如果无法解析 IP 地址，对象存储客户端就无法与对象存储服务器通信。因此，数据可能无法访问。	检查 DNS 配置以验证主机名是否使用 IP 地址正确配置。
对象存储集群间 LIF 故障	严重	对象存储客户端找不到可操作的 LIF 来与对象存储服务器通信。在集群间 LIF 运行之前，节点将不允许对象存储客户端流量。因此，数据可能无法访问。	执行以下纠正措施：…使用“network interface show -role intercluster”命令检查集群间 LIF 状态。…验证集群间 LIF 是否配置正确且可运行。…如果未配置集群间 LIF，请使用“network interface create -role intercluster”命令添加它。
对象存储签名不匹配	严重	发送到对象存储服务器的请求签名与客户端计算的签名不匹配。因此，数据可能无法访问。	验证秘密访问密钥是否配置正确。如果配置正确，请联系NetApp技术支持寻求帮助。

READDIR 超时	严重	READDIR 文件操作已超出允许在WAFL中运行的超时时间。这可能是因为目录非常大或稀疏。建议采取纠正措施。	执行以下操作：…使用以下具有“diag”权限的 nodeshell CLI 命令查找特定于最近 READDIR 文件操作已过期的目录的信息：wafl readdir notice show。…检查目录是否指示为稀疏：…如果目录指示为稀疏，建议您将目录的内容复制到新目录以消除目录文件的稀疏性。…如果目录未指示为稀疏且目录很大，建议您通过减少目录中的文件条目数来减小目录文件的大小。
重新定位聚合失败	严重	当目标节点无法到达对象存储时，在聚合重新定位期间会发生此事件。	执行以下纠正措施：…使用“network interface show”命令验证集群间 LIF 是否在线且正常运行。…通过目标节点集群间 LIF 使用“ping”命令检查与对象存储服务器的网络连接。…使用“aggregate object-store config show”命令验证对象存储的配置未更改，并且登录和连接信息仍然准确。…或者，您可以使用重定位命令的“override-destination-checks”参数覆盖错误。…请联系NetApp技术支持以获取更多信息或帮助。
卷影复制失败	严重	卷影复制服务 (VSS)（Microsoft Server 备份和还原服务操作）失败。	使用事件消息中提供的信息检查以下内容：…是否启用了卷影复制配置？…是否安装了适当的许可证？ …在哪些共享上执行卷影复制操作？…共享名称是否正确？…共享路径是否存在？…卷影复制集及其卷影副本的状态如何?
存储开关电源故障	警告	集群交换机中缺少电源。冗余度降低，任何进一步的电源故障都会导致停电风险。	执行以下纠正措施：…确保为集群交换机供电的电源已打开。…确保电源线已连接到电源。…如果问题仍然存在，请联系NetApp技术支持。

CIFS 身份验证过多	警告	许多认证协商同时发生。来自该客户端的 256 个未完成的新会话请求。	调查客户端为何创建了 256 个或更多的新连接请求。您可能需要联系客户端或应用程序的供应商来确定错误发生的原因。
未经授权的用户访问管理员共享	警告	客户端尝试连接到特权 ONTAP_ADMIN$ 共享，即使其登录用户不是允许的用户。	执行以下纠正措施：…确保在其中一个活动的 Vscan 扫描器池中配置了提到的用户名和 IP 地址。…使用“vserver vscan scanner pool show-active”命令检查当前处于活动状态的扫描器池配置。
检测到病毒	警告	Vscan 服务器向存储系统报告了一个错误。这通常表明发现了病毒。但是，Vscan 服务器上的其他错误可能会导致此事件……客户端对该文件的访问被拒绝。 Vscan 服务器可能会根据其设置和配置清理、隔离或删除该文件。	检查“syslog”事件中报告的 Vscan 服务器日志，查看它是否能够成功清理、隔离或删除受感染的文件。如果无法做到这一点，系统管理员可能必须手动删除该文件。
卷脱机	INFO	此消息表明卷已脱机。	使卷重新联机。
卷受限	INFO	此事件表明灵活卷受到限制。	使卷重新联机。
存储虚拟机停止成功	INFO	当“vserver stop”操作成功时会出现此消息。	使用“vserver start”命令启动存储虚拟机上的数据访问。
节点恐慌	警告	当发生恐慌时发出此事件	联系NetApp客户支持。

返回顶部

反勒索软件日志监控器

监视器名称	严重性	描述	更正操作
存储虚拟机反勒索软件监控已禁用	警告	存储虚拟机的反勒索软件监控已禁用。启用反勒索软件来保护存储虚拟机。	无
存储虚拟机反勒索软件监控已启用（学习模式）	INFO	存储虚拟机的反勒索软件监控以学习模式启用。	无
启用批量反勒索软件监控	INFO	该卷的反勒索软件监控已启用。	无
批量反勒索软件监控已禁用	警告	该卷的反勒索软件监控已被禁用。启用反勒索软件来保护卷。	无

启用批量反勒索软件监控（学习模式）	INFO	该卷的反勒索软件监控在学习模式下启用。	无
批量反勒索软件监控已暂停（学习模式）	警告	该卷的反勒索软件监控在学习模式下暂停。	无
批量反勒索软件监控已暂停	警告	该卷的反勒索软件监控已暂停。	无
批量反勒索软件监控禁用	警告	该卷的反勒索软件监控正在禁用。	无
检测到勒索软件活动	严重	为了保护数据免受检测到的勒索软件的侵害，我们制作了快照副本，可用于恢复原始数据。您的系统会生成AutoSupport或“回拨”消息并将其传输至NetApp技术支持和任何配置的目的地。AutoSupport消息可提高问题的确定和解决能力。	请参阅“FINAL-DOCUMENT-NAME”以针对勒索软件活动采取补救措施。

返回顶部

FSx for NetApp ONTAP监视器

监视器名称	阈值	监视器描述	更正操作
FSx 卷容量已满	警告 @ > 85 %…严重 @ > 95 %	卷的存储容量对于存储应用程序和客户数据是必要的。 ONTAP卷中存储的数据越多，未来数据的可用存储空间就越少。如果卷内的数据存储容量达到总存储容量，可能会导致客户因存储容量不足而无法存储数据。监控已用存储容量可确保数据服务的连续性。	如果突破临界阈值，则需要立即采取行动以尽量减少服务中断：…1.考虑删除不再需要的数据以释放空间

FSx 卷高延迟	警告 @ > 1000 µs…严重 @ > 2000 µs	卷是服务于 IO 流量的对象，通常由性能敏感的应用程序（包括 devOps 应用程序、主目录和数据库）驱动。高容量延迟意味着应用程序本身可能会受到影响并且无法完成其任务。监控卷延迟对于维持应用程序的一致性能至关重要。	如果突破临界阈值，则需要立即采取行动以尽量减少服务中断：…1.如果为卷分配了 QoS 策略，请评估其限制阈值，以防它们导致卷工作负载受到限制……如果超过警告阈值，请计划尽快采取以下措施：……1.如果为卷分配了 QoS 策略，请评估其限制阈值，以防它们导致卷工作负载受到限制。…2.如果该节点也遇到高利用率，请将卷移动到另一个节点或减少该节点的总工作负载。
FSx 卷 Inode 限制	警告 @ > 85 %…严重 @ > 95 %	存储文件的卷使用索引节点（inode）来存储文件元数据。当卷耗尽其 inode 分配时，就无法再向其中添加文件。警告警报表明应采取计划措施来增加可用的 inode 数量。严重警报表示文件限制即将耗尽，应采取紧急措施释放 inode 以确保服务连续性	如果突破临界阈值，则需要立即采取行动以尽量减少服务中断：…1.考虑增加卷的 inode 值。如果 inode 值已经达到最大值，则考虑将卷拆分为两个或更多卷，因为文件系统已经超出了最大大小……如果超过警告阈值，计划尽快采取以下措施：……1.考虑增加卷的 inode 值。如果 inode 值已经达到最大值，则考虑将卷拆分为两个或更多卷，因为文件系统已超出最大大小
FSx 卷 Qtree 配额过载	警告 @ > 95 %…严重 @ > 100 %	卷 Qtree 配额过载指定卷被视为被 qtree 配额过载的百分比。已达到卷的 qtree 配额设置的阈值。监控卷 qtree 配额过量提交可确保用户获得不间断的数据服务。	如果突破了关键阈值，则应立即采取措施以尽量减少服务中断：1.删除不需要的数据…当超过警告阈值时，考虑增加卷的空间。

FSx 快照保留空间已满	警告 @ > 90 %…严重 @ > 95 %	卷的存储容量对于存储应用程序和客户数据是必要的。该空间的一部分称为快照保留空间，用于存储允许在本地保护数据的快照。 ONTAP卷中存储的新数据和更新数据越多，使用的快照容量就越多，而可用于未来新数据或更新数据的快照存储容量就越少。如果卷内的快照数据容量达到总快照预留空间，则可能导致客户无法存储新的快照数据，并降低卷中数据的保护级别。监控卷使用的快照容量，确保数据服务的连续性。	如果突破临界阈值，则需要立即采取行动以尽量减少服务中断：…1.考虑配置快照以在快照保留已满时使用卷中的数据空间…2。考虑删除一些可能不再需要的旧快照以释放空间……如果超过警告阈值，计划尽快采取以下措施：……1.考虑增加卷内的快照保留空间以适应增长…2.考虑配置快照，以便在快照保留已满时使用卷中的数据空间
FSx 卷缓存未命中率	警告 @ > 95 %…严重 @ > 100 %	卷缓存未命中率是来自客户端应用程序的读取请求中从磁盘返回而不是从缓存返回的百分比。这意味着音量已经达到设定的阈值。	如果突破了关键阈值，则应立即采取措施以尽量减少服务中断：1.将一些工作负载移出卷的节点以减少 IO 负载 2.通过 QoS 限制降低同一节点上较低优先级工作负载的需求……当超过警告阈值时考虑立即采取行动：1.将一些工作负载移出卷的节点以减少 IO 负载 2.通过QoS限制3降低同一节点上较低优先级工作负载的需求。改变工作负载特征（块大小、应用程序缓存等）

返回顶部

K8s 监视器

监视器名称	描述	更正操作	严重程度/阈值

持久卷延迟高	高持久卷延迟意味着应用程序本身可能会受到影响并且无法完成其任务。监控持久卷延迟对于维持应用程序的一致性能至关重要。以下是基于媒体类型的预期延迟 - SSD 最多 1-2 毫秒；SAS 最多 8-10 毫秒，SATA HDD 最多 17-20 毫秒。	立即采取行动 如果突破了关键阈值，请考虑立即采取行动以尽量减少服务中断：如果卷分配了 QoS 策略，请评估其限制阈值，以防它们导致卷工作负载受到限制。 即将采取的行动 如果超出警告阈值，请计划立即采取以下行动：1.如果存储池也遇到高利用率，请将卷移动到另一个存储池。2.如果卷分配了 QoS 策略，请评估其限制阈值，以防它们导致卷工作负载受到限制。3.如果控制器的利用率也很高，请将卷移至另一个控制器或减少控制器的总工作负载。	警告 @ > 6,000 µs 严重 @ > 12,000 µs
集群内存饱和度高	集群可分配内存饱和度高。集群 CPU 饱和度的计算方法是将内存使用量总和除以所有 K8s 节点上可分配内存的总和。	添加节点。修复任何未安排的节点。适当大小的 pod 可以释放节点上的内存。	警告 @ > 80 % 严重 @ > 90 %
POD 连接失败	当带有 POD 的卷附件失败时会出现此警报。		警告
高重传率	高 TCP 重传率	检查网络拥塞 - 识别消耗大量网络带宽的工作负载。检查 Pod CPU 利用率是否过高。检查硬件网络性能。	警告 @ > 10% 严重 @ > 25%
节点文件系统容量高	节点文件系统容量高	- 增加节点磁盘的大小以确保有足够的空间容纳应用程序文件。 - 减少应用程序文件的使用。	警告 @ > 80 % 严重 @ > 90 %
工作负载网络抖动高	高 TCP 抖动（高延迟/响应时间变化）	检查网络拥塞情况。识别消耗大量网络带宽的工作负载。检查 Pod CPU 利用率是否过高。检查硬件网络性能	警告 @ > 30 毫秒 严重 @ > 50 毫秒

持久卷吞吐量	当持久卷超出预定义的性能预期时，可以使用持久卷上的 MBPS 阈值来提醒管理员，这可能会影响其他持久卷。激活此监视器将生成适合 SSD 上持久卷的典型吞吐量配置文件的警报。该监视器将覆盖租户上的所有持久卷。可以根据您的监控目标，通过复制此监控器并设置适合您的存储类别的阈值来调整警告和临界阈值。重复的监视器可以进一步定位到租户上的持久卷的子集。	立即采取行动 如果突破关键阈值，请立即采取行动以尽量减少服务中断：1.引入卷的 QoS MBPS 限制。2.检查驱动卷工作负载的应用程序是否存在异常。 即将采取的行动 如果超出警告阈值，计划立即采取以下行动：1.引入卷的 QoS MBPS 限制。2.检查驱动卷工作负载的应用程序是否存在异常。	警告 @ > 10,000 MB/s 严重 @ > 15,000 MB/s
面临 OOM 风险的容器被杀死	容器的内存限制设置得太低。该容器有被驱逐的风险（因内存不足而被杀死）。	增加容器内存限制。	警告 @ > 95%
减少工作量	工作负载没有健康的 pod。		严重@<1
持久卷声明绑定失败	当 PVC 上的绑定失败时会出现此警报。		警告
ResourceQuota 内存限制即将超出	命名空间的内存限制即将超过 ResourceQuota		警告 @ > 80 % 严重 @ > 90 %
ResourceQuota 内存请求即将超出	Namespace 的内存请求即将超出 ResourceQuota		警告 @ > 80 % 严重 @ > 90 %
节点创建失败	由于配置错误，无法调度该节点。	检查 Kubernetes 事件日志以了解配置失败的原因。	批判的
持久卷回收失败	该卷的自动回收失败。		警告@>0B
容器 CPU 限制	容器的 CPU 限制设置得太低。容器进程变慢。	增加容器 CPU 限制。	警告 @ > 95 % 严重 @ > 98 %
服务负载均衡器删除失败			警告
持久卷 IOPS	当持久卷超出预定义的性能预期时，可以使用持久卷上的 IOPS 阈值来提醒管理员。激活此监视器将生成适合持久卷的典型 IOPS 配置文件的警报。该监视器将覆盖租户上的所有持久卷。可以根据您的监控目标，通过复制此监控器并设置适合您的工作负载的阈值来调整警告和临界阈值。	立即采取行动 如果突破关键阈值，请计划立即采取行动以尽量减少服务中断：1.引入卷的 QoS IOPS 限制。2.检查驱动卷工作负载的应用程序是否存在异常。 即将采取的行动 如果超出警告阈值，请计划立即采取以下行动：1.引入卷的 QoS IOPS 限制。2.检查驱动卷工作负载的应用程序是否存在异常。	警告 @ > 20,000 IO/s 严重 @ > 25,000 IO/s

服务负载均衡器更新失败			警告
POD 挂载失败	当 POD 上的挂载失败时会出现此警报。		警告
节点PID压力	(Linux) 节点上的可用进程标识符已低于驱逐阈值。	查找并修复生成许多进程并导致节点缺乏可用进程 ID 的 pod。设置 PodPidsLimit 来保护您的节点免受产生过多进程的 pod 或容器的影响。	严重 @ > 0
Pod 镜像拉取失败	Kubernetes 无法拉取 pod 容器镜像。	- 确保 pod 配置中 pod 的图像拼写正确。 - 检查您的注册表中是否存在图像标签。 - 验证图像注册表的凭据。 - 检查注册表连接问题。 - 确认您没有达到公共注册提供商所施加的速率限制。	警告
作业运行时间过长	作业运行时间过长		警告 @ > 1 小时 严重 @ > 5 小时
节点内存高	节点内存使用率高	添加节点。修复任何未安排的节点。适当大小的 pod 可以释放节点上的内存。	警告 @ > 85 % 严重 @ > 90 %
ResourceQuota CPU 限制即将超出	命名空间的 CPU 限制即将超出 ResourceQuota		警告 @ > 80 % 严重 @ > 90 %
Pod 崩溃循环退避	Pod 已崩溃并尝试重新启动多次。		严重@>3
节点 CPU 高	节点CPU使用率高。	添加节点。修复任何未安排的节点。适当大小的 pod 可以释放节点上的 CPU。	警告 @ > 80 % 严重 @ > 90 %
工作负载网络延迟 RTT 高	TCP RTT（往返时间）延迟高	检查网络拥塞▒识别消耗大量网络带宽的工作负载。检查 Pod CPU 利用率是否过高。检查硬件网络性能。	警告 @ > 150 毫秒 严重 @ > 300 毫秒
作业失败	由于节点崩溃或重启、资源耗尽、作业超时或 pod 调度失败，作业未成功完成。	检查 Kubernetes 事件日志以了解失败原因。	警告@>1
持久卷几天内就会满	持久卷将在几天内耗尽空间	-增加卷大小以确保有足够的空间容纳应用程序文件。 -减少应用程序中存储的数据量。	警告@<8天严重@<3天

节点内存压力	节点内存不足。可用内存已达到驱逐阈值。	添加节点。修复任何未安排的节点。适当大小的 pod 可以释放节点上的内存。	严重 @ > 0
节点未就绪	节点已处于未就绪状态 5 分钟	验证节点是否具有足够的 CPU、内存和磁盘资源。检查节点网络连接。检查 Kubernetes 事件日志以了解失败原因。	严重@<1
持久卷容量高	持久卷后端已用容量较高。	- 增加卷大小以确保有足够的空间容纳应用程序文件。 - 减少应用程序中存储的数据量。	警告 @ > 80 % 严重 @ > 90 %
服务负载均衡器创建失败	服务负载均衡器创建失败		批判的
工作负载副本不匹配	某些 pod 目前不适用于 Deployment 或 DaemonSet。		警告@>1
ResourceQuota CPU 请求即将超出	Namespace 的 CPU 请求即将超出 ResourceQuota		警告 @ > 80 % 严重 @ > 90 %
高重传率	高 TCP 重传率	检查网络拥塞 - 识别消耗大量网络带宽的工作负载。检查 Pod CPU 利用率是否过高。检查硬件网络性能。	警告 @ > 10% 严重 @ > 25%
节点磁盘压力	节点的根文件系统或映像文件系统上的可用磁盘空间和 inode 已满足驱逐阈值。	- 增加节点磁盘的大小以确保有足够的空间容纳应用程序文件。 - 减少应用程序文件的使用。	严重 @ > 0
集群 CPU 饱和度高	集群可分配 CPU 饱和度高。集群 CPU 饱和度的计算方法是将 CPU 使用率总和除以所有 K8s 节点上可分配的 CPU 总和。	添加节点。修复任何未安排的节点。适当大小的 pod 可以释放节点上的 CPU。	警告 @ > 80 % 严重 @ > 90 %

返回顶部

变更日志监视器

监视器名称	严重性	监视器描述
发现内部卷	信息	当发现内部卷时会出现此消息。
内部体积已修改	信息	当内部卷被修改时会出现此消息。
发现存储节点	信息	当发现存储节点时会出现此消息。
存储节点已移除	信息	当存储节点被移除时会出现此消息。
已发现存储池	信息	发现存储池时会出现此消息。

已发现存储虚拟机	信息	当发现存储虚拟机时会出现此消息。
存储虚拟机已修改	信息	当存储虚拟机被修改时会出现此消息。

返回顶部

数据收集监视器

监视器名称	描述	更正操作
采集单元关闭	Data Infrastructure Insights采集单元会定期重启，作为升级的一部分来引入新功能。在典型环境中，这种情况每月发生一次或更少。警告警报指出，采集单元已关闭，随后应立即发出决议，指出新重启的采集单元已完成Data Infrastructure Insights的注册。通常，从关机到注册的周期需要 5 到 15 分钟。	如果警报频繁发生或持续时间超过 15 分钟，请检查托管采集单元的系统、网络以及将 AU 连接到互联网的任何代理的运行情况。
收集器失败	数据收集器的轮询遇到了意外的失败情况。	访问Data Infrastructure Insights中的数据收集器页面以了解更多情况。
收集器警告	此警报通常是由于数据收集器或目标系统的错误配置而引起的。重新审视配置以防止将来出现警报。这也可能是由于数据收集器收集了所有可能的数据，但检索的数据并不完整。当数据收集过程中情况发生变化时，就会发生这种情况（例如，在数据收集过程中和捕获其数据之前删除了数据收集开始时存在的虚拟机）。	检查数据收集器或目标系统的配置。请注意，收集器警告监视器可以比其他监视器类型发送更多警报，因此建议不要设置警报收件人，除非您正在进行故障排除。

返回顶部

安全监视器

监视器名称	阈值	监视器描述	更正操作
已禁用 AutoSupport HTTPS 传输	警告@<1	AutoSupport支持 HTTPS、HTTP 和 SMTP 作为传输协议。由于AutoSupport消息的敏感性， NetApp强烈建议使用 HTTPS 作为向NetApp支持发送AutoSupport消息的默认传输协议。	要将 HTTPS 设置为AutoSupport消息的传输协议，请运行以下ONTAP命令：…system node autosupport modify -transport https

集群不安全的 SSH 密码	警告@<1	表示 SSH 正在使用不安全的密码，例如以 *cbc 开头的密码。	要删除 CBC 密码，请运行以下ONTAP命令：…security ssh remove -vserver <admin vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
集群登录横幅已禁用	警告@<1	表示对于访问ONTAP系统的用户，登录横幅已被禁用。显示登录横幅有助于建立对系统访问和使用的期望。	要配置集群的登录横幅，请运行以下ONTAP命令：…security login banner modify -vserver <admin svm> -message "Access restricted to authorized users"
集群对等通信未加密	警告@<1	在复制数据以进行灾难恢复、缓存或备份时，您必须在从一个ONTAP集群到另一个 ONTAP 集群通过网络传输数据期间保护该数据。必须在源集群和目标集群上配置加密。	要对 ONTAP 9.6 之前创建的集群对等关系启用加密，必须将源和目标集群升级到 9.6 版。然后使用“cluster peer modify”命令将源集群对等点和目标集群对等点更改为使用集群对等加密。…有关详细信息，请参阅《NetApp ONTAP 9 安全强化指南》。
已启用默认本地管理员用户	警告@>0	NetApp建议使用 lock 命令锁定（禁用）任何不需要的默认管理员用户（内置）帐户。它们主要是默认帐户，其密码从未更新或更改过。	要锁定内置“管理员”帐户，请运行以下ONTAP命令：…security login lock -username admin
已禁用 FIPS 模式	警告@<1	启用 FIPS 140-2 合规性后，TLSv1 和 SSLv3 将被禁用，只有 TLSv1.1 和 TLSv1.2 保持启用状态。当启用 FIPS 140-2 合规性时， ONTAP会阻止您启用 TLSv1 和 SSLv3。	要在集群上启用 FIPS 140-2 合规性，请在高级权限模式下运行以下ONTAP命令：…security config modify -interface SSL -is -fips-enabled true
日志转发未加密	警告@<1	卸载系统日志信息对于将违规的范围或影响限制在单个系统或解决方案中是必要的。因此， NetApp建议将系统日志信息安全地卸载到安全的存储或保留位置。	一旦创建了日志转发目标，其协议就无法更改。要更改为加密协议，请使用以下ONTAP命令删除并重新创建日志转发目标：…cluster log-forwarding create -destination <destination ip> -protocol tcp-encrypted

MD5 哈希密码	警告@>0	NetApp强烈建议对ONTAP用户帐户密码使用更安全的 SHA-512 哈希函数。使用安全性较低的 MD5 哈希函数的帐户应迁移到 SHA-512 哈希函数。	NetApp强烈建议用户更改密码，将用户帐户迁移到更安全的 SHA-512 解决方案。…要使用 MD5 哈希函数的密码锁定帐户，请运行以下ONTAP命令：…security login lock -vserver * -username * -hash -function md5
未配置 NTP 服务器	警告@<1	表示集群没有配置NTP服务器。为了实现冗余和最佳服务， NetApp建议您将至少三个 NTP 服务器与集群关联。	要将 NTP 服务器与集群关联，请运行以下ONTAP命令：cluster time-service ntp server create -server <ntp 服务器主机名或 IP 地址>
NTP 服务器计数不足	警告@<3	表示集群配置的NTP服务器少于3个。为了实现冗余和最佳服务， NetApp建议您将至少三个 NTP 服务器与集群关联。	要将 NTP 服务器与集群关联，请运行以下ONTAP命令：…cluster time-service ntp server create -server <ntp 服务器主机名或 IP 地址>
已启用远程 Shell	警告@>0	远程 Shell 不是建立对ONTAP解决方案的命令行访问的安全方法。应禁用远程 Shell 以实现安全的远程访问。	NetApp建议使用安全外壳 (SSH) 进行安全远程访问。…要在集群上禁用远程外壳，请在高级权限模式下运行以下ONTAP命令：…安全协议修改 -application rsh- enabled false
存储虚拟机审核日志已禁用	警告@<1	表示已禁用 SVM 的审计日志记录。	要为虚拟服务器配置审计日志，请运行以下ONTAP命令：…vserver audit enable -vserver <svm>
存储虚拟机 SSH 的不安全密码	警告@<1	表示 SSH 正在使用不安全的密码，例如以 *cbc 开头的密码。	要删除 CBC 密码，请运行以下ONTAP命令：…security ssh remove -vserver <vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
存储虚拟机登录横幅已禁用	警告@<1	表示对于访问系统上的 SVM 的用户，登录横幅已被禁用。显示登录横幅有助于建立对系统访问和使用的期望。	要配置集群的登录横幅，请运行以下ONTAP命令：…security login banner modify -vserver <svm> -message "Access restricted to authorized users"

已启用 Telnet 协议	警告@>0	Telnet 不是建立ONTAP解决方案命令行访问的安全方法。应禁用 Telnet 以实现安全的远程访问。	NetApp建议使用安全外壳 (SSH) 进行安全远程访问。要在集群上禁用 Telnet，请在高级权限模式下运行以下ONTAP命令：…security protocol modify -application telnet -enabled false

返回顶部

数据保护监控器

监视器名称	阈值	监视器描述	更正操作
Lun 快照复制空间不足	（过滤器 contains_luns = 是）警告 @ > 95%…严重 @ > 100%	卷的存储容量对于存储应用程序和客户数据是必要的。该空间的一部分称为快照保留空间，用于存储允许在本地保护数据的快照。 ONTAP卷中存储的新数据和更新数据越多，使用的快照容量就越多，而可用于未来新数据或更新数据的快照存储容量就越少。如果卷内的快照数据容量达到总快照预留空间，则可能导致客户无法存储新的快照数据，并降低卷中 LUN 中数据的保护级别。监控卷使用的快照容量，确保数据服务的连续性。	立即采取行动 如果突破关键阈值，请考虑立即采取行动以尽量减少服务中断：1.配置快照以在快照保留已满时使用卷中的数据空间。2.删除一些不需要的旧快照以释放空间。 即将采取的行动 如果超出警告阈值，计划立即采取以下行动：1.增加卷内的快照保留空间以适应增长。2.配置快照以在快照保留已满时使用卷中的数据空间。
SnapMirror关系滞后	警告 @ > 150%…严重 @ > 300%	SnapMirror关系滞后是快照时间戳与目标系统上的时间之间的差异。lag_time_percent 是滞后时间与SnapMirror策略的计划间隔的比率。如果滞后时间等于计划间隔，则 lag_time_percent 将为 100%。如果SnapMirror策略没有计划，则不会计算 lag_time_percent 。	使用“snapmirror show”命令监控SnapMirror状态。使用“snapmirror show-history”命令检查SnapMirror传输历史记录

返回顶部

云量 **(CVO)** 监视器

监视器名称	CI 严重性	监视器描述	更正操作

CVO 磁盘停止服务	INFO	当磁盘因被标记为故障、正在被清理或已进入维护中心而被从服务中移除时，会发生此事件。	无
CVO 存储池交还失败	严重	此事件发生在聚合迁移期间，作为存储故障转移 (SFO) 恢复的一部分，此时目标节点无法到达对象存储。	执行以下纠正措施：使用“network interface show”命令验证集群间 LIF 是否在线且正常运行。通过目标节点集群间 LIF 使用“ping”命令检查与对象存储服务器的网络连接。使用“aggregate object-store config show”命令验证对象存储的配置是否未更改，以及登录和连接信息是否仍然准确。或者，您可以通过将 giveback 命令的“require-partner-waiting”参数指定为 false 来覆盖错误。请联系NetApp技术支持以获取更多信息或帮助。
CVO HA 互连中断	警告	高可用性 (HA) 互连已中断。当故障转移不可用时，存在服务中断的风险。	纠正措施取决于平台支持的 HA 互连链路的数量和类型，以及互连中断的原因。如果链接断开：请验证 HA 对中的两个控制器是否正常运行。对于外部连接的链路，请确保互连电缆连接正确，并且小型可插拔设备 (SFP)（如果适用）在两个控制器上均正确就位。对于内部连接的链接，使用“ic link off”和“ic link on”命令依次禁用并重新启用链接。如果链接被禁用，请使用“ic link on”命令启用链接。如果对等方未连接，请使用“ic link off”和“ic link on”命令依次禁用并重新启用链接。如果问题仍然存在，请联系NetApp技术支持。

已超出每位用户的 CVO 最大会话数	警告	您已超出 TCP 连接上每个用户允许的最大会话数。任何建立会话的请求都将被拒绝，直到某些会话被释放。	执行以下纠正措施：检查客户端上运行的所有应用程序，并终止任何运行不正常的应用程序。重新启动客户端。检查问题是否由新应用程序或现有应用程序引起：如果应用程序是新的，请使用“cifs option modify -max-opens -same-file-per-tree”命令为客户端设置更高的阈值。在某些情况下，客户端会按预期运行，但需要更高的阈值。您应该具有高级权限来为客户端设置更高的阈值。如果问题是由现有应用程序引起的，则客户端可能存在问题。请联系NetApp技术支持以获取更多信息或帮助。
CVO NetBIOS 名称冲突	严重	NetBIOS 名称服务已从远程计算机收到对名称注册请求的否定响应。这通常是由于 NetBIOS 名称或别名冲突引起的。结果，客户端可能无法访问数据或连接到集群中正确的数据服务节点。	执行以下任一纠正措施：如果 NetBIOS 名称或别名存在冲突，请执行以下操作之一：使用“vserver cifs delete -aliases alias -vserver vserver”命令删除重复的 NetBIOS 别名。通过删除重复的名称并使用“vserver cifs create -aliases alias -vserver vserver”命令添加具有新名称的别名来重命名 NetBIOS 别名。如果没有配置别名并且 NetBIOS 名称存在冲突，则使用“vserver cifs delete -vserver vserver” 和“vserver cifs create -cifs -server netbiosname”命令重命名 CIFS 服务器。注意：删除 CIFS 服务器可能会导致数据无法访问。删除 NetBIOS 名称或重命名远程计算机上的 NetBIOS。
CVO NFSv4 存储池已耗尽	严重	NFSv4 存储池已耗尽。	如果 NFS 服务器在此事件发生后超过 10 分钟没有响应，请联系NetApp技术支持。
CVO 节点恐慌	警告	当发生恐慌时发出此事件	联系NetApp客户支持。

CVO 节点根卷空间低	严重	系统检测到根卷的空间严重不足。该节点尚未完全运行。数据 LIF 可能已在集群内进行故障转移，因此节点上的 NFS 和 CIFS 访问受到限制。管理能力仅限于节点的本地恢复程序，以清理根卷上的空间。	执行以下纠正措施：通过删除旧的 Snapshot 副本、从 /mroot 目录中删除不再需要的文件或扩展根卷容量来清理根卷上的空间。重新启动控制器。请联系NetApp技术支持以获取更多信息或帮助。
CVO 不存在 管理员共享	严重	Vscan 问题：客户端尝试连接到不存在的 ONTAP_ADMIN$ 共享。	确保已为提到的 SVM ID 启用 Vscan。在 SVM 上启用 Vscan 会导致自动为 SVM 创建 ONTAP_ADMIN$ 共享。
CVO 对象存储主机无法解析	严重	对象存储服务器主机名无法解析为 IP 地址。如果无法解析 IP 地址，对象存储客户端就无法与对象存储服务器通信。因此，数据可能无法访问。	检查 DNS 配置以验证主机名是否使用 IP 地址正确配置。
CVO 对象存储集群间 LIF 故障	严重	对象存储客户端找不到可操作的 LIF 来与对象存储服务器通信。在集群间 LIF 运行之前，节点将不允许对象存储客户端流量。因此，数据可能无法访问。	执行以下纠正措施：使用“network interface show -role intercluster”命令检查集群间 LIF 状态。验证集群间 LIF 是否配置正确且可运行。如果未配置集群间 LIF，请使用“network interface create -role intercluster”命令添加它。
CVO 对象存储签名不匹配	严重	发送到对象存储服务器的请求签名与客户端计算的签名不匹配。因此，数据可能无法访问。	验证秘密访问密钥是否配置正确。如果配置正确，请联系NetApp技术支持寻求帮助。
CVO QoS 监控内存已满	严重	QoS 子系统的动态内存已达到当前平台硬件的限制。某些 QoS 功能可能以有限的容量运行。	删除一些活动的工作负载或流以释放内存。使用“statistics show -object workload -counter ops”命令来确定哪些工作负载是活动的。活动工作负载显示非零操作。然后多次使用“workload delete <workload_name>”命令来删除特定的工作负载。或者，使用“stream delete -workload <workload name> *”命令从活动工作负载中删除关联的流。

CVO READDIR 超时	严重	READDIR 文件操作已超出允许在WAFL中运行的超时时间。这可能是因为目录非常大或稀疏。建议采取纠正措施。	执行以下纠正措施：使用以下“diag”权限 nodeshell CLI 命令查找特定于最近 READDIR 文件操作已过期的目录的信息：wafl readdir notice show。检查目录是否被指示为稀疏：如果目录被指示为稀疏，建议您将目录的内容复制到新目录以消除目录文件的稀疏性。如果目录未指示为稀疏且目录很大，则建议您通过减少目录中的文件条目数来减小目录文件的大小。
CVO 存储池重新定位失败	严重	当目标节点无法到达对象存储时，在聚合重新定位期间会发生此事件。	执行以下纠正措施：使用“network interface show”命令验证集群间 LIF 是否在线且正常运行。通过目标节点集群间 LIF 使用“ping”命令检查与对象存储服务器的网络连接。使用“aggregate object-store config show”命令验证对象存储的配置是否未更改，以及登录和连接信息是否仍然准确。或者，您可以使用重定位命令的“override-destination-checks”参数来覆盖错误。请联系NetApp技术支持以获取更多信息或帮助。
CVO 卷影复制失败	严重	卷影复制服务 (VSS)（Microsoft Server 备份和还原服务操作）失败。	使用事件消息中提供的信息检查以下内容：是否启用了卷影复制配置？是否安装了适当的许可证？卷影复制操作在哪些共享上执行？股票名称正确吗？共享路径是否存在？卷影副本集及其卷影副本的状态是什么？
CVO 存储虚拟机停止成功	INFO	当“vserver stop”操作成功时会出现此消息。	使用“vserver start”命令启动存储虚拟机上的数据访问。
CVO 过多 CIFS 身份验证	警告	许多认证协商同时发生。来自该客户端的 256 个未完成的新会话请求。	调查客户端为何创建了 256 个或更多的新连接请求。您可能需要联系客户端或应用程序的供应商来确定错误发生的原因。

CVO 未分配磁盘	INFO	系统有未分配的磁盘 - 容量被浪费，并且您的系统可能存在一些错误配置或应用了部分配置更改。	执行以下纠正措施：使用“disk show -n”命令确定哪些磁盘未分配。使用“disk assign”命令将磁盘分配给系统。
CVO 未经授权的用户访问管理员共享	警告	客户端尝试连接到特权 ONTAP_ADMIN$ 共享，即使其登录用户不是允许的用户。	执行以下纠正措施：确保在其中一个活动的 Vscan 扫描程序池中配置了提到的用户名和 IP 地址。使用“vserver vscan scanner pool show-active”命令检查当前处于活动状态的扫描仪池配置。
检测到 CVO 病毒	警告	Vscan 服务器向存储系统报告了一个错误。这通常表明发现了病毒。但是，Vscan 服务器上的其他错误也可能导致此事件。客户端访问该文件被拒绝。 Vscan 服务器可能会根据其设置和配置清理、隔离或删除该文件。	检查“syslog”事件中报告的 Vscan 服务器日志，查看它是否能够成功清理、隔离或删除受感染的文件。如果无法做到这一点，系统管理员可能必须手动删除该文件。
CVO 卷离线	INFO	此消息表明卷已脱机。	使卷重新联机。
CVO 容量受限	INFO	此事件表明灵活卷受到限制。	使卷重新联机。

返回顶部

SnapMirror业务连续性 **(SMBC)** 调解器日志监视器

监视器名称	严重性	监视器描述	更正操作
已添加ONTAP调解器	INFO	当ONTAP调解器成功添加到集群时，会出现此消息。	无
ONTAP调解器无法访问	严重	当ONTAP调解器被重新利用或调解器软件包不再安装在调解器服务器上时，会出现此消息。因此，SnapMirror故障转移是不可能的。	使用“snapmirror mediator remove”命令删除当前ONTAP调解器的配置。使用“snapmirror mediator add”命令重新配置对ONTAP Mediator 的访问。
ONTAP调解器已移除	INFO	当ONTAP调解器成功从集群中删除时，会出现此消息。	无

ONTAP调解器无法访问	警告	当集群上的ONTAP调解器无法访问时，会出现此消息。因此， SnapMirror故障转移是不可能的。	使用“network ping”和“network traceroute”命令检查与ONTAP Mediator的网络连接。如果问题仍然存在，请使用“snapmirror mediator remove”命令删除当前ONTAP Mediator 的配置。使用“snapmirror mediator add”命令重新配置对ONTAP Mediator 的访问。
SMBC CA 证书已过期	严重	当ONTAP调解器证书颁发机构 (CA) 证书过期时会出现此消息。因此，将无法与ONTAP Mediator 进行任何进一步的通信。	使用“snapmirror mediator remove”命令删除当前ONTAP调解器的配置。在ONTAP调解器服务器上更新新的 CA 证书。使用“snapmirror mediator add”命令重新配置对ONTAP Mediator 的访问。
SMBC CA 证书即将到期	警告	当ONTAP调解器证书颁发机构 (CA) 证书即将在未来 30 天内到期时，会出现此消息。	在此证书过期之前，使用“snapmirror mediator remove”命令删除当前ONTAP调解器的配置。在ONTAP调解器服务器上更新新的 CA 证书。使用“snapmirror mediator add”命令重新配置对ONTAP Mediator 的访问。
SMBC 客户端证书已过期	严重	当ONTAP调解器客户端证书过期时会出现此消息。因此，将无法与ONTAP Mediator 进行任何进一步的通信。	使用“snapmirror mediator remove”命令删除当前ONTAP调解器的配置。使用“snapmirror mediator add”命令重新配置对ONTAP Mediator 的访问。
SMBC 客户端证书即将过期	警告	当ONTAP调解器客户端证书即将在未来 30 天内过期时，会出现此消息。	在此证书过期之前，使用“snapmirror mediator remove”命令删除当前ONTAP调解器的配置。使用“snapmirror mediator add”命令重新配置对ONTAP Mediator 的访问。

SMBC 关系不同步 注意：UM 没有这个	严重	当SnapMirror for Business Continuity (SMBC) 关系的状态从“同步”更改为“不同步”时，会出现此消息。由于 RPO=0，数据保护将会中断。	检查源卷和目标卷之间的网络连接。通过在目标上使用“snapmirror show”命令，并在源上使用“snapmirror list-destinations”命令来监控 SMBC 关系状态。自动重新同步将尝试使关系恢复到“同步”状态。如果重新同步失败，请验证集群中的所有节点是否都达到法定人数并且运行状况良好。
SMBC 服务器证书已过期	严重	当ONTAP调解器服务器证书过期时会出现此消息。因此，将无法与ONTAP Mediator 进行任何进一步的通信。	使用“snapmirror mediator remove”命令删除当前ONTAP调解器的配置。在ONTAP调解器服务器上更新新的服务器证书。使用“snapmirror mediator add”命令重新配置对ONTAP Mediator 的访问。
SMBC 服务器证书即将过期	警告	当ONTAP调解器服务器证书即将在未来 30 天内过期时，会出现此消息。	在此证书过期之前，使用“snapmirror mediator remove”命令删除当前ONTAP调解器的配置。在ONTAP调解器服务器上更新新的服务器证书。使用“snapmirror mediator add”命令重新配置对ONTAP Mediator 的访问。

返回顶部

附加电源、心跳和其他系统监视器

监视器名称	严重性	监视器描述	更正操作
发现磁盘架电源	信息	当电源单元添加到磁盘架时会出现此消息。	无
磁盘架电源已移除	信息	从磁盘架上移除电源单元时会出现此消息。	无
已禁用 MetroCluster 自动计划外切换	严重	当自动计划外切换功能被禁用时，会出现此消息。	对集群中的每个节点运行“metrocluster modify -node-name <nodename> -automatic-switchover -onfailure true”命令以启用自动切换。

监视器名称	严重性	监视器描述	更正操作
MetroCluster存储桥无法访问	严重	无法通过管理网络访问存储桥	1) 如果网桥由 SNMP 监控，请使用“network interface show”命令验证节点管理 LIF 是否已启动。使用“网络 ping”命令验证网桥是否处于活动状态。 2) 如果桥接器是带内监控的，请检查桥接器的结构布线，然后验证桥接器是否已通电。
MetroCluster桥接温度异常 - 低于临界值	严重	光纤通道桥接器上的传感器报告的温度低于临界阈值。	1）检查存储桥上风扇的运行状态。 2）验证桥梁是否在建议的温度条件下运行。
MetroCluster桥接温度异常 - 高于临界值	严重	光纤通道桥接器上的传感器报告的温度高于临界阈值。	1) 使用命令“storage bridge show -cooling”检查存储桥上底盘温度传感器的运行状态。 2) 验证储存桥是否在建议的温度条件下运行。
MetroCluster 遗留了聚合	警告	在折返过程中，骨料被留在了后面。	1) 使用命令“aggr show”检查聚合状态。 2) 如果聚合处于在线状态，则使用命令“metrocluster switchback”将其返回给其原始所有者。
Metrocluster 合作伙伴之间的所有链接均已关闭	严重	RDMA 互连适配器和集群间 LIF 与对等集群的连接已断开，或者对等集群已关闭。	1) 确保集群间 LIF 已启动并正在运行。如果集群间 LIF 发生故障，请修复它们。 2) 使用“cluster peer ping”命令验证对等集群是否已启动并正在运行。如果对等集群发生故障，请参阅《MetroCluster灾难恢复指南》。 3) 对于结构MetroCluster，验证后端结构 ISL 是否已启动并正在运行。如果后端结构 ISL 出现故障，请修复它们。 4) 对于非结构MetroCluster配置，请验证 RDMA 互连适配器之间的布线是否正确。如果链路中断，请重新配置电缆。

监视器名称	严重性	监视器描述	更正操作
无法通过对等网络访问 MetroCluster 配对集群	严重	与对等集群的连接已中断。	1) 确保端口连接到正确的网络/交换机。 2) 确保集群间 LIF 与对等集群连接。 3) 使用命令“cluster peer ping”确保对等集群已启动并正在运行。如果对等集群发生故障，请参阅《MetroCluster灾难恢复指南》。
MetroCluster内部交换机所有链路均关闭	严重	存储交换机上的所有交换机间链路 (ISL) 均已关闭。	1) 修复存储交换机上的后端结构 ISL。 2) 确保合作伙伴交换机已启动并且其 ISL 可运行。 3) 确保中间设备（如 xWDM 设备）正常运行。
MetroCluster节点到存储堆栈 SAS 链路断开	警告	SAS 适配器或其连接的电缆可能有故障。	1.验证 SAS 适配器是否在线且正在运行。2.验证物理电缆连接是否安全且正常运行，如有必要，请更换电缆。3.如果 SAS 适配器连接到磁盘架，请确保 IOM 和磁盘已正确就位。
MetroClusterFC 启动器链路断开	严重	FC 启动器适配器出现故障。	1.确保 FC 启动器链路未被篡改。2.使用命令“system node run -node local -command storage show adapter”验证 FC 启动器适配器的运行状态。
FC-VI 互连链路中断	严重	FC-VI端口上的物理链路处于离线状态。	1.确保 FC-VI 链路未被篡改。2.使用命令“metrocluster interconnect adapter show”验证 FC-VI 适配器的物理状态是否为“Up”。3.如果配置包括结构交换机，请确保它们正确布线和配置。
MetroCluster 遗留了备用磁盘	警告	切换过程中留下了备用磁盘。	如果磁盘没有故障，请使用命令“metrocluster switchback”将其返回给原始所有者。
MetroCluster存储桥端口关闭	严重	存储桥接器上的端口处于离线状态。	1）使用命令“storage bridge show -ports”检查存储桥上端口的运行状态。 2) 验证端口的逻辑和物理连接。

监视器名称	严重性	监视器描述	更正操作
MetroCluster存储交换机风扇出现故障	严重	存储交换机上的风扇发生故障。	1) 使用命令“storage switch show -cooling”确保交换机中的风扇正常运行。 2) 确保风扇 FRU 正确插入并正常运行。
MetroCluster存储交换机无法访问	严重	无法通过管理网络访问存储交换机。	1) 使用命令“network interface show”确保节点管理 LIF 已启动。 2）使用命令“network ping”确保交换机处于活动状态。 3) 登录交换机后，检查其 SNMP 设置，确保可以通过 SNMP 访问交换机。
MetroCluster交换机电源发生故障	严重	存储交换机上的电源装置无法运行。	1) 使用命令“storage switch show -error -switch -name <swtich name>”检查错误详情。 2) 使用命令“storage switch show -power -switch-name <switch name>”识别故障电源单元。 3) 确保电源装置正确插入存储交换机的底盘并完全正常运行。
MetroCluster交换机温度传感器发生故障	严重	光纤通道交换机上的传感器发生故障。	1) 使用命令“storage switch show -cooling”检查存储交换机上温度传感器的运行状态。 2) 验证开关是否在建议的温度条件下运行。
MetroCluster交换机温度异常	严重	光纤交换机上的温度传感器报告温度异常。	1) 使用命令“storage switch show -cooling”检查存储交换机上温度传感器的运行状态。 2) 验证开关是否在建议的温度条件下运行。
服务处理器心跳丢失	信息	当ONTAP未从服务处理器(SP) 接收到预期的“心跳”信号时，会出现此消息。随着此消息，来自SP的日志文件也将被发送出去以供调试。 ONTAP将重置SP以尝试恢复通信。SP重新启动时将最多两分钟不可用。	联系NetApp技术支持。

监视器名称	严重性	监视器描述	更正操作
服务处理器心跳停止	警告	当ONTAP不再从服务处理器 (SP) 接收心跳时，会出现此消息。根据硬件设计，系统可能会继续提供数据，或者决定关闭以防止数据丢失或硬件损坏。系统继续提供数据，但由于SP可能无法工作，系统无法发送设备关闭、启动错误或开放固件 (OFW) 开机自检 (POST) 错误的通知。如果您的系统配置为这样做，它会生成并传输AutoSupport （或“回拨”）消息给NetApp技术支持和配置的目的地。成功传递AutoSupport消息可显著提高问题的确定和解决能力。	如果系统已关闭，请尝试硬电源循环：将控制器从底盘拉出，再推回，然后打开系统电源。如果电源循环后问题仍然存在，或者存在任何其他需要注意的情况，请联系NetApp技术支持。

返回顶部

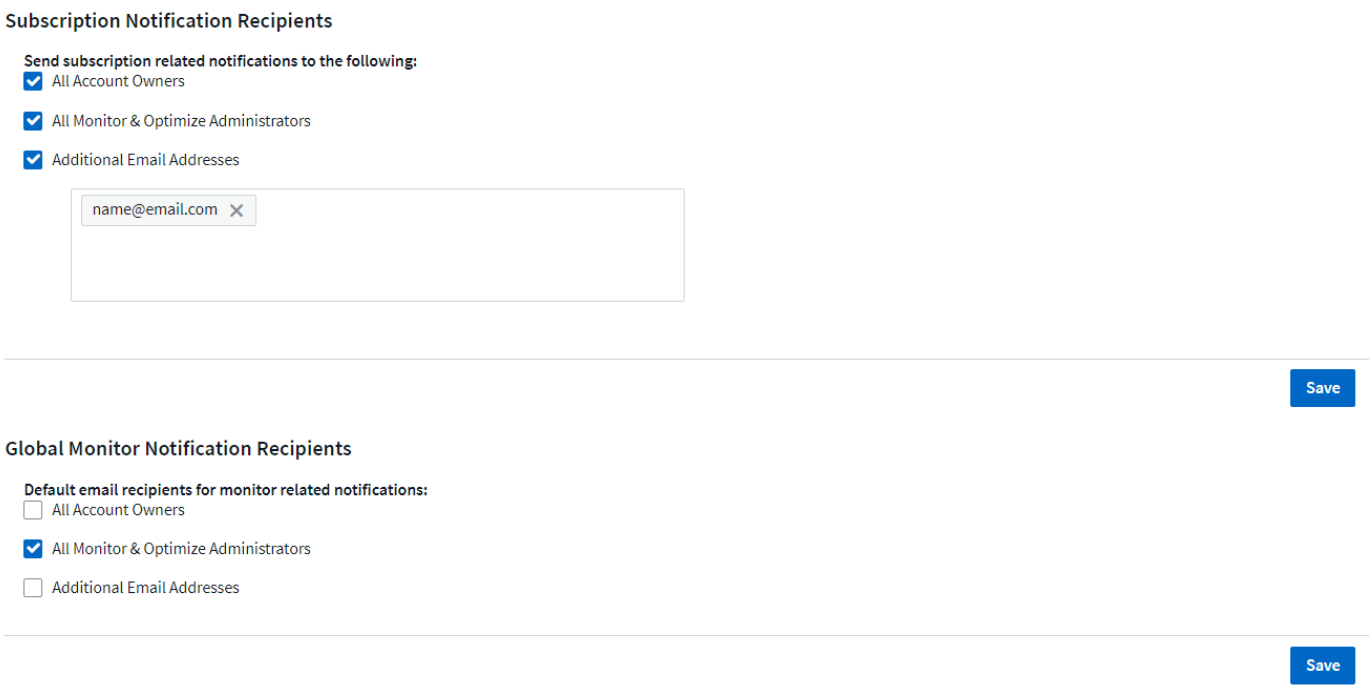
更多信息

- "查看和关闭警报"

配置电子邮件通知

您可以配置与订阅相关的通知的电子邮件列表，以及用于通知性能策略阈值违规的收件人的全局电子邮件列表。

要配置通知电子邮件收件人设置，请转到*管理>通知*页面并选择_电子邮件_选项卡。



订阅通知收件人

要配置订阅相关事件通知的收件人，请转到“订阅通知收件人”部分。您可以选择将订阅相关事件的电子邮件通知发送给以下任何或所有收件人：

- 所有账户所有者
- 所有_监控和优化_管理员
- 您指定的其他电子邮件地址

以下是可能发送的通知类型以及您可以采取的用户操作的示例。

通知：	用户操作：
试用版或订阅版已更新	查看订阅详情"订阅"页
订阅将在 90 天后到期 订阅将在 30 天后到期	如果启用了“自动续订”，则无需采取任何行动，请联系NetApp销售人员续订
试用期将于 2 天后结束	续订试用版"订阅"页。您可以续订一次试用版。联系NetApp销售人员购买订阅
试用或订阅已过期 帐户将在 48 小时后停止收集数据 帐户将在 48 小时后被删除	联系NetApp销售人员购买订阅

为了确保您的收件人收到来自Data Infrastructure Insights的通知，请将以下电子邮件地址添加到任何“允许”列表中：

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

警报的全局收件人列表

对于针对警报采取的每个操作，都会向警报收件人列表发送警报的电子邮件通知。您可以选择向全球收件人列表发送警报通知。

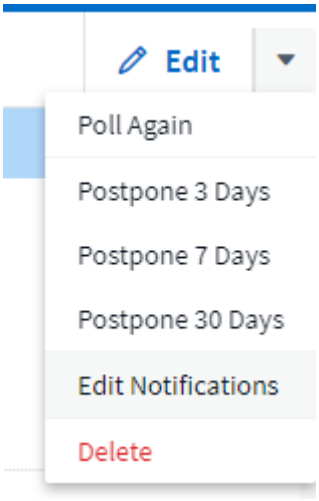
要配置全局警报收件人，请在“全局监控通知收件人”部分中选择所需的收件人。

在创建或修改监视器时，您始终可以覆盖单个监视器的全局收件人列表。

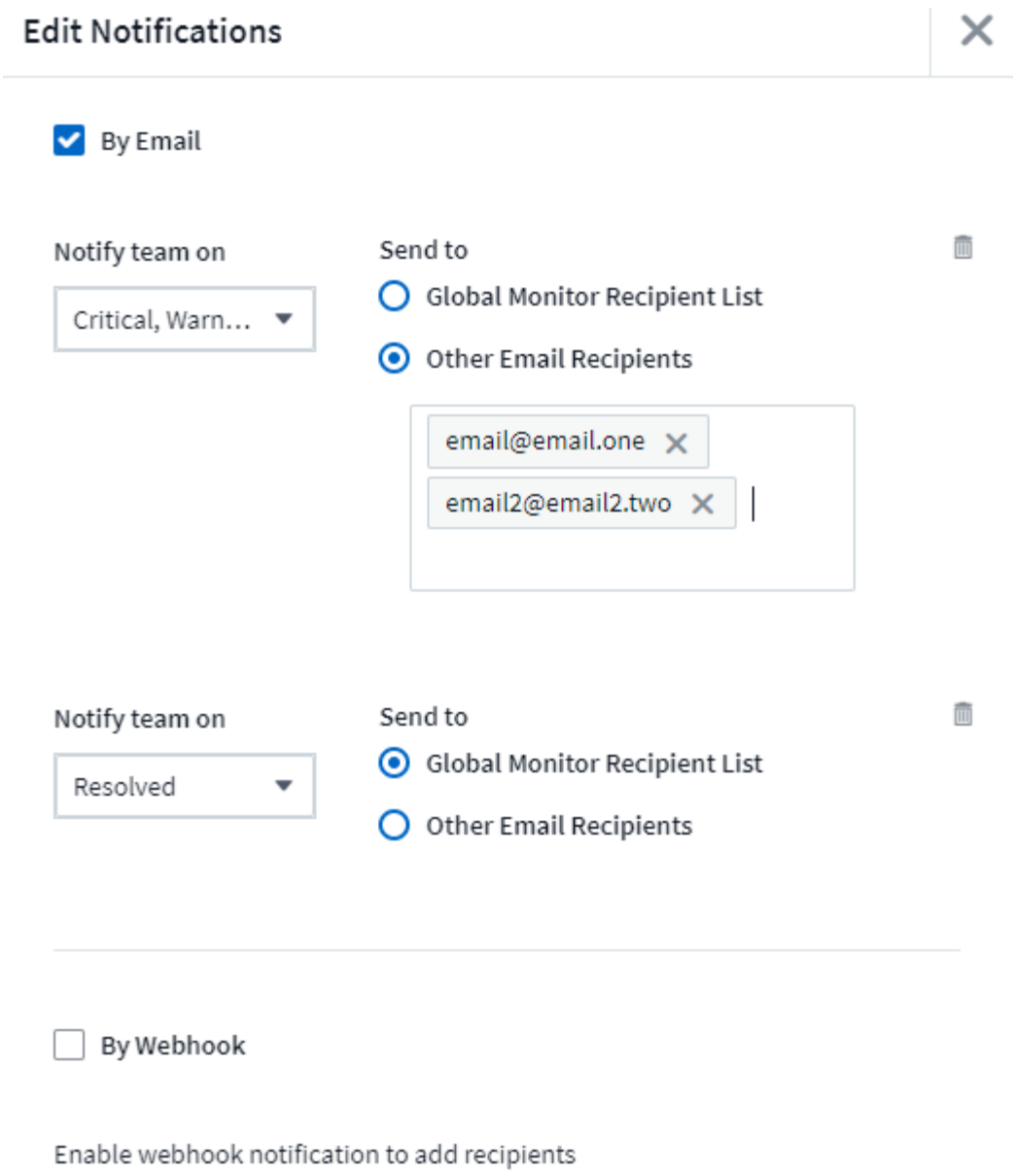
ONTAP数据收集器通知优先于与集群/数据收集器相关的任何特定监视器通知。您为数据收集器本身设置的收件人列表将接收数据收集器警报。如果没有活动的数据收集器警报，则监视器生成的警报将发送给特定的监视器接收者。

编辑ONTAP的通知

您可以通过从存储登录页面右上角的下拉菜单中选择“编辑通知”来修改ONTAP集群的通知。



从这里，您可以设置严重、警告、信息和/或已解决警报的通知。每个场景都可以通知全局收件人列表或您选择的其他收件人。



Webhook 通知

使用 **Webhook** 进行通知

Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送警报通知。

很多商业应用都支持webhooks作为标准输入接口，例如：Slack、PagerDuty、Teams、Discord都支持webhooks。通过支持通用、可定制的 webhook 通道， Data Infrastructure Insights可以支持许多此类交付通道。可以在这些应用程序网站上找到有关 webhook 的信息。例如，Slack 提供"这个有用的指南"。

您可以创建多个 webhook 通道，每个通道针对不同的目的；单独的应用程序、不同的收件人等。

Webhook 通道实例由以下元素组成：

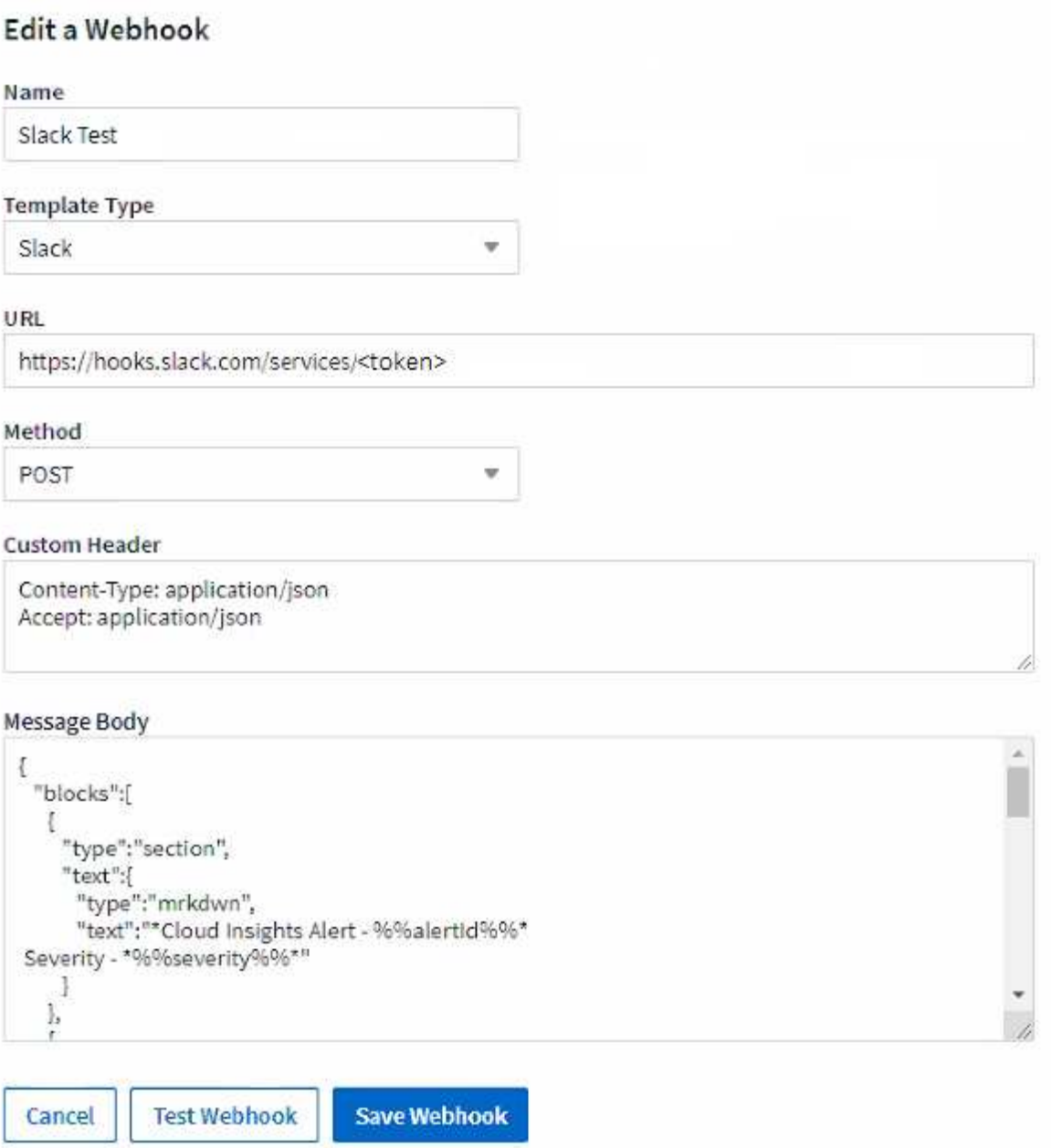
名称	唯一名称

URL	Webhook 目标 URL，包括 *http://* 或 *https://* 前缀以及 URL 参数
方法	GET、POST - 默认为 POST
自定义标题	在此指定任何自定义标题行
消息正文	在此处填写您的邮件正文
默认警报参数	列出 webhook 的默认参数
自定义参数和机密	自定义参数和秘密允许您添加唯一参数和安全元素，例如密码

创建 **Webhook**

要创建Data Infrastructure Insightswebhook，请转到 管理 **>** 通知 并选择 **Webhooks** 选项卡。

下图显示了为 Slack 配置的示例 webhook：



在每个字段中输入适当的信息，完成后单击“保存”。

您也可以点击“测试 Webhook”按钮来测试连接。请注意，这将根据所选方法将“消息正文”（不带替换）发送到定义的 URL。

Data Infrastructure Insightswebhook 包含许多默认参数。此外，您还可以创建自己的自定义参数或秘密。

Default Alert Parameters

Name	Description
%%alertDescription%%	Alert description
%%alertId%%	Alert ID
%%alertRelativeUrl%%	Relative URL to the Alert page. To build alert link use https://%%cloudInsightsHostName%%%%alertRelativeUrl%%
%%metricName%%	Monitored metric
%%monitorName%%	Monitor name
%%objectType%%	Monitored object type
%%severity%%	Alert severity level
%%alertCondition%%	Alert condition
%%triggerTime%%	Alert trigger time in GMT ('Tue, 27 Oct 2020 01:20:30 GMT')
%%triggerTimeEpoch%%	Alert trigger time in Epoch format (milliseconds)
%%triggeredOn%%	Triggered On (key:value pairs separated by commas)
%%value%%	Metric value that triggered the alert
%%cloudInsightsLogoUrl%%	Cloud Insights logo URL
%%cloudInsightsHostname%%	Cloud Insights Hostname (concatenate with relative URL to build alert link)

Custom Parameters and Secrets

Name	Value	Description
No Data Available		

+ Parameter

参数：它们是什么以及如何使用它们?

警报参数是每个警报填充的动态值。例如，*%%TriggeredOn%%* 参数将被替换为触发警报的对象。

您可以将任何对象属性（例如，存储名称）作为参数添加到 webhook。例如，您可以在 webhook 描述中设置卷名称和存储名称的参数，如："卷的高延迟：*%%relatedObject.volume.name%%*，存储：*%%relatedObject.storage.name%%*"。

请注意，在本节中，单击"测试 Webhook"按钮时不会执行替换；该按钮发送一个显示 %% 替换的有效负载，但

不会用数据替换它们。

自定义参数和机密

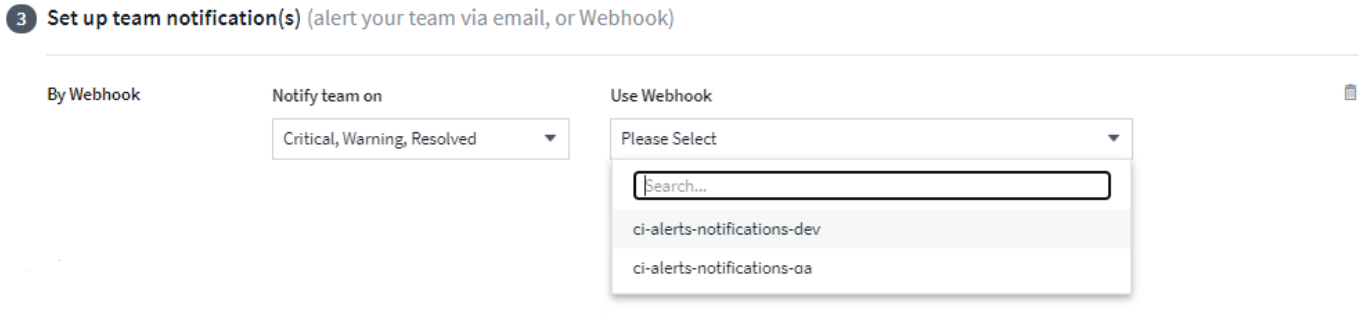
在本节中，您可以添加任何您想要的自定义参数和/或秘密。出于安全原因，如果定义了机密，则只有 webhook 创建者可以修改此 webhook 通道。对于其他人来说它是只读的。您可以在 URL/Headers 中使用秘密作为 *%%<secret_name>%%*。

Webhook 列表页面

Webhooks 列表页面显示名称、创建者、创建日期、状态、安全和上次报告字段。

在监视器中选择 **Webhook** 通知

要选择 webhook 通知"监视器"，转到*警报>管理监视器*并选择所需的监视器，或添加新的监视器。在“设置团队通知”部分，选择“Webhook”作为传送方式。选择警报级别（严重、警告、已解决），然后选择所需的 webhook。



Webhook 示例：

Webhook 适用于"松弛"Webhook 适用于"PagerDuty"Webhook 适用于"团队"Webhook 适用于"不和谐"

Discord 的 Webhook 示例

Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送警报通知。本页提供了为 Discord 设置 webhook 的示例。

本页引用第三方说明，可能会有所变更。请参阅"Discord 文档"以获取最新信息。

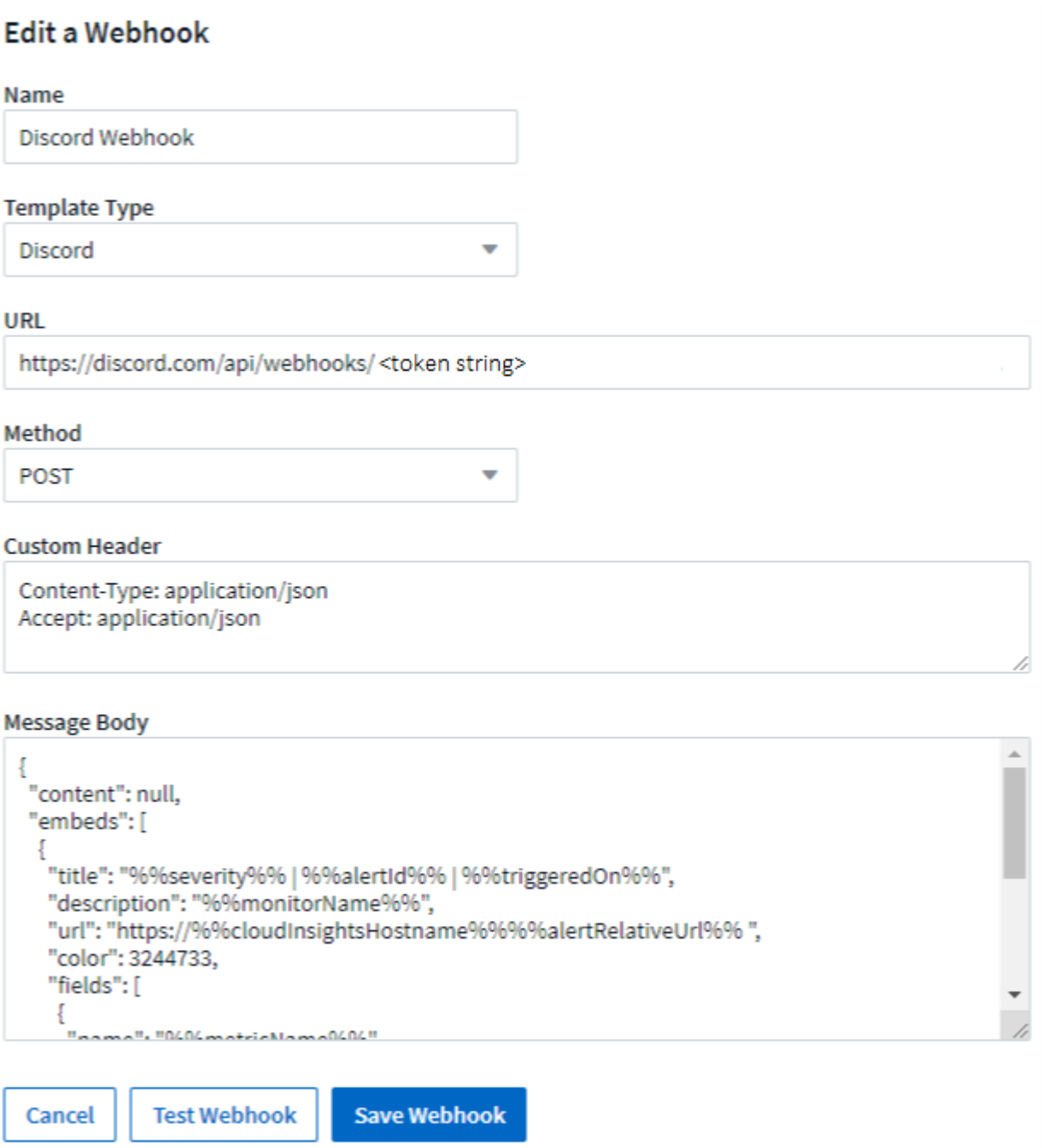
Discord 设置：

- 在 Discord 中，选择服务器，在文本频道下，选择编辑频道（齿轮图标）
- 选择“集成”>“查看 Webhook”，然后单击“新建 Webhook”
- 复制 Webhook URL。您需要将其粘贴到Data Infrastructure Insightswebhook 配置中。

创建**Data Infrastructure InsightsWebhook**：

1. 在Data Infrastructure Insights中，导航到 管理 > 通知 并选择 **Webhooks** 选项卡。单击 **+Webhook** 创建一个新 webhook。

2. 为 webhook 赋予一个有意义的名称，例如“Discord”。
3. 在“模板类型”下拉菜单中，选择“Discord”。
4. 将上面的 URL 粘贴到 *URL* 字段中。

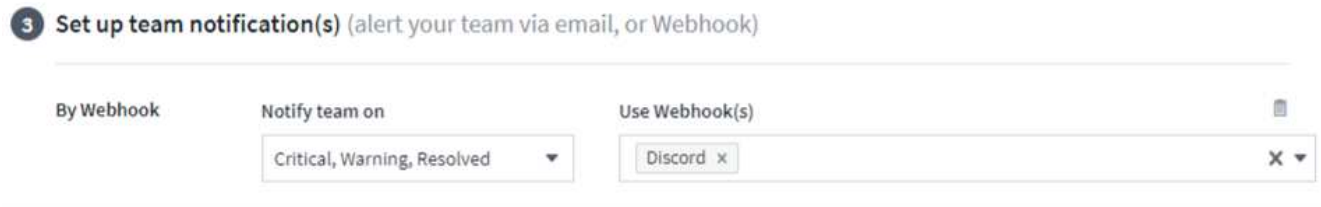


为了测试 webhook，请暂时将消息正文中的 url 值替换为任何有效的 URL（例如 *https://netapp.com*），然后单击 测试 *Webhook* 按钮。测试完成后，请务必将消息正文重新设置。

通过 **Webhook** 发送通知

要通过 webhook 通知事件，请在Data Infrastructure Insights中导航至 **Alerts > Monitors**，然后单击 **+Monitor** 以创建新的"监视器"。

- 选择一个指标并定义监视器的条件。
- 在“设置团队通知”下，选择“Webhook”传送方式。
- 为所需事件（严重、警告、已解决）选择“Discord” webhook



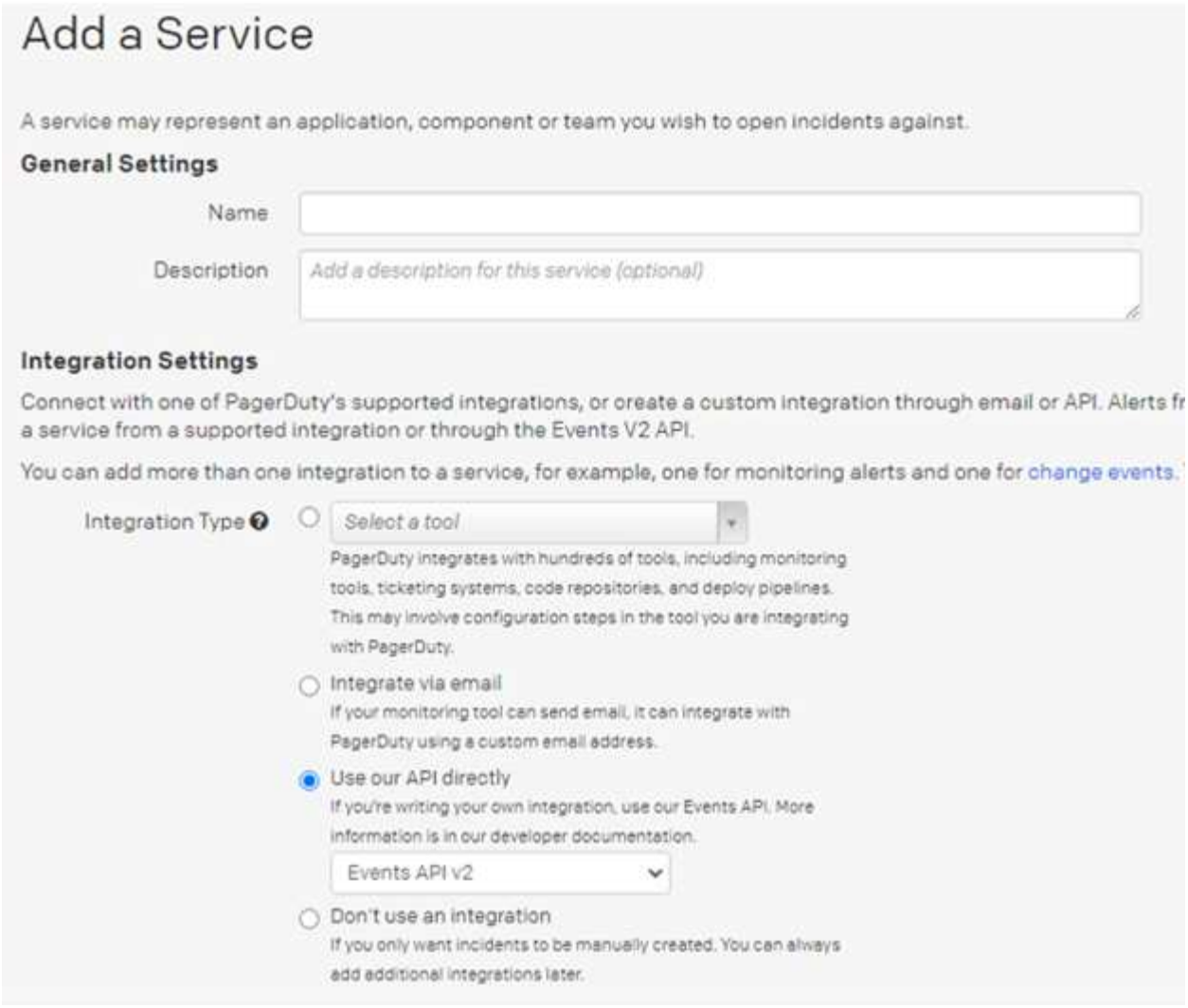
PagerDuty 的 Webhook 示例

Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送警报通知。本页面提供了为 PagerDuty 设置 webhook 的示例。

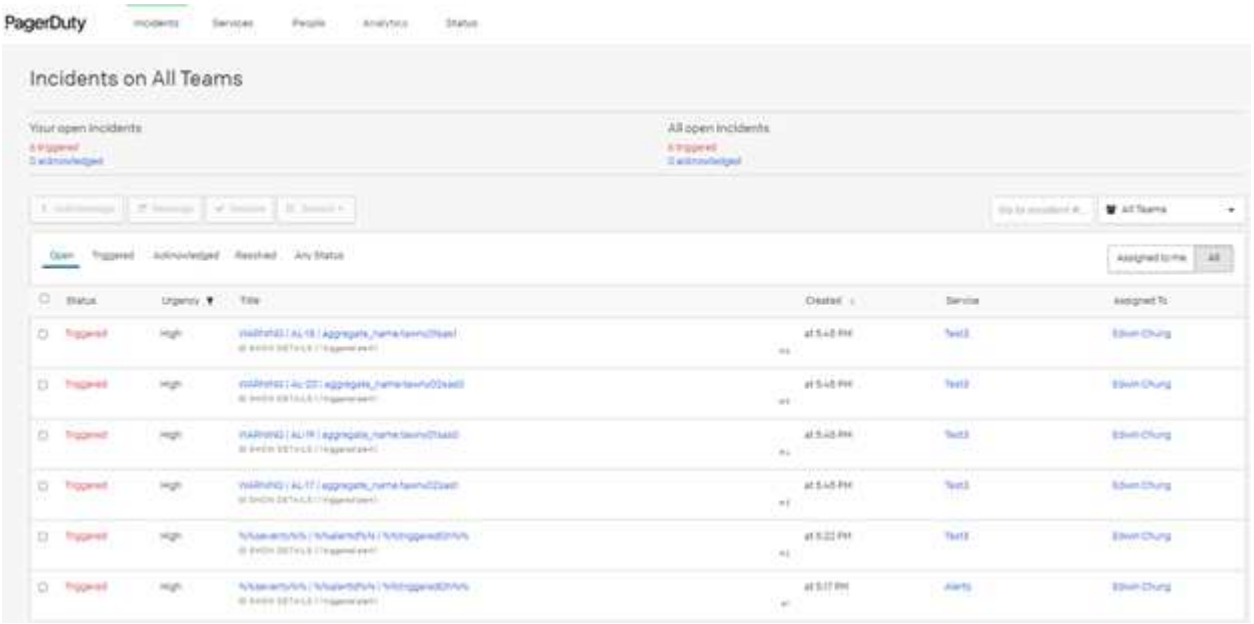
本页引用第三方说明，可能会有所变更。请参阅"PagerDuty 文档"以获取最新信息。

PagerDuty 设置：

1. 在 PagerDuty 中，导航至 服务 **>** 服务目录，然后单击 **+**新服务 按钮
2. 输入_名称_并选择_直接使用我们的 API_。点击_添加服务_。

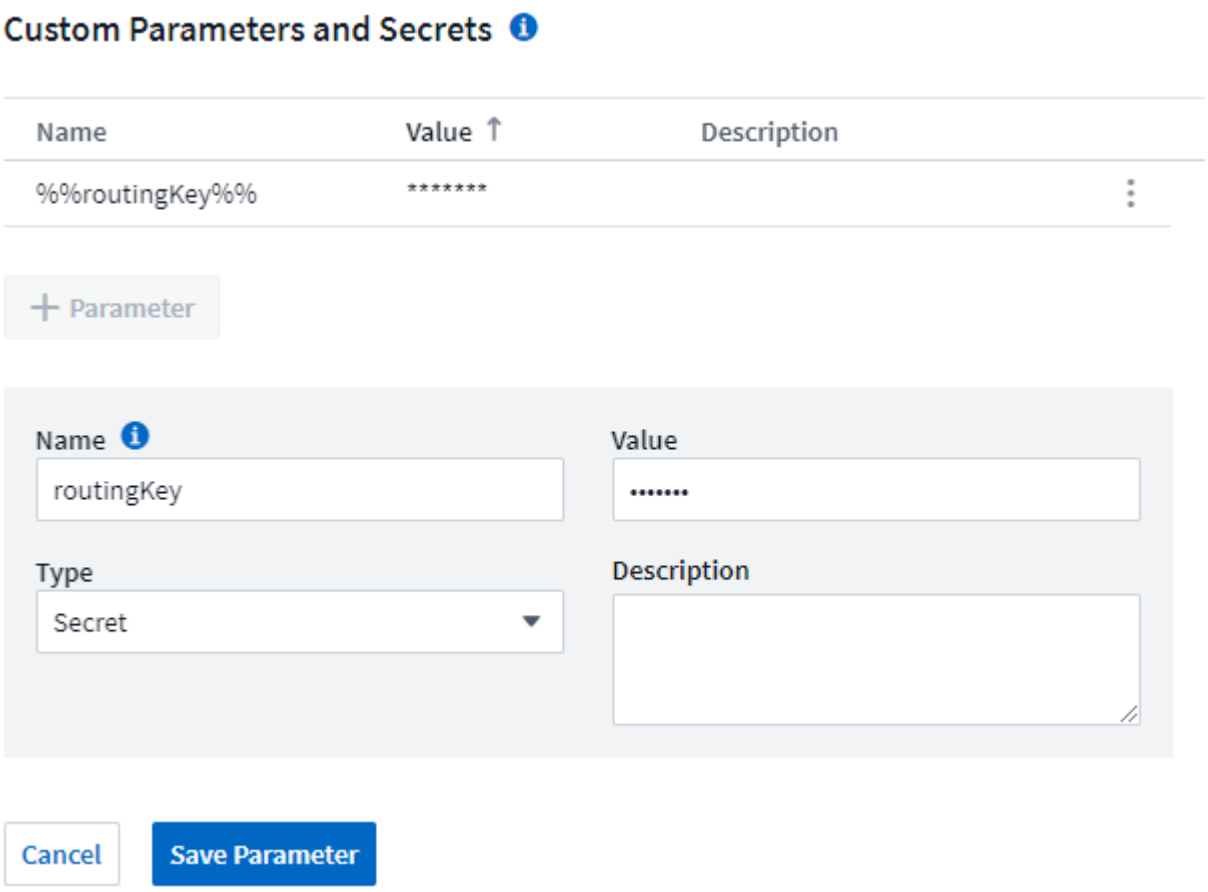


3. 单击“Integrations”选项卡即可查看“Integration Key”。当您创建下面的Data Infrastructure Insightswebhook时，您将需要此密钥。
4. 前往*事件*或*服务*查看警报。



创建**Data Infrastructure InsightsWebhook**：

1. 在Data Infrastructure Insights中，导航到 管理 > 通知 并选择 **Webhooks** 选项卡。单击 **+Webhook** 创建一个新 webhook。
2. 为 webhook 赋予一个有意义的名称，例如“PagerDuty Trigger”。您将使用此 webhook 来处理严重和警告级别的事件。
3. 在“模板类型”下拉菜单中，选择“PagerDuty”。
4. 创建一个名为 *routingKey* 的自定义参数机密，并将其值设置为上面的 PagerDuty *Integration Key* 值。



重复这些步骤，为已解决的事件创建“PagerDuty Resolve”webhook。

PagerDutyData Infrastructure Insights字段映射

下表和图片显示了 PagerDuty 和Data Infrastructure Insights之间的字段映射：

PagerDuty	Data Infrastructure Insights
警报键	Alert ID
源	触发于
组件	指标名称
组	对象类型
班级	监视器名称

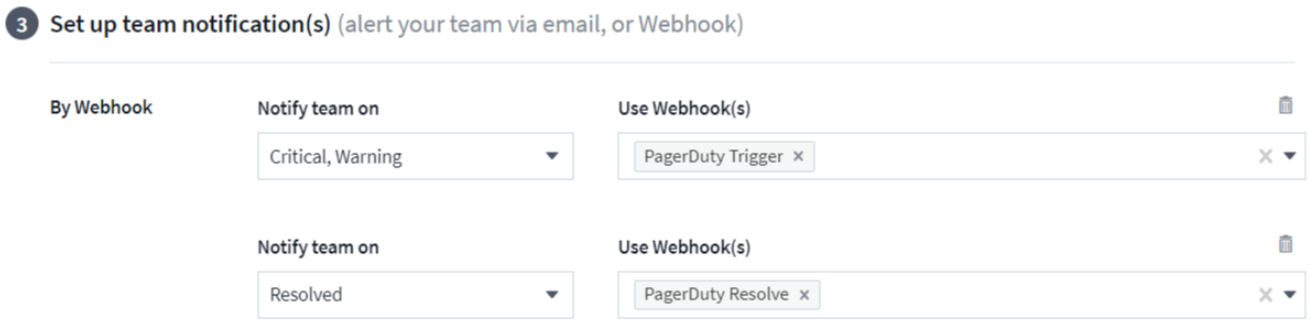
Message Body

```
{
 "dedup_key": "%%alertId%%",
 "event_action": "trigger",
 "links": [
  {
   "href": "https://%%cloudInsightsHostname%%%%alertRelativeUrl%%",
   "text": "'%%metricName%%' value of %%value%% (%%alertCondition%%) for
%%triggeredOn%%"
  }
 ],
 "payload": {
  "class": "%%monitorName%%",
  "component": "%%metricName%%",
  "group": "%%objectType%%",
  "severity": "critical",
  "source": "%%triggeredOn%%",
  "summary": "%%severity%% | %%alertId%% | %%triggeredOn%%"
 },
 "routing_key": "%%routingKey%%"
}
```

通过 **Webhook** 发送通知

要通过 webhook 通知事件，请在Data Infrastructure Insights中导航至 **Alerts > Monitors**，然后单击 **+Monitor** 以创建新的"监视器"。

- 选择一个指标并定义监视器的条件。
- 在“设置团队通知”下，选择“Webhook”传送方式。
- 为严重和警告级别事件选择“PagerDuty Trigger”webhook。
- 为已解决的事件选择“PagerDuty Resolve”。



为触发事件和已解决事件设置单独的通知是最佳做法，因为 PagerDuty 处理触发事件的方式与处理已解决事件的方式不同。

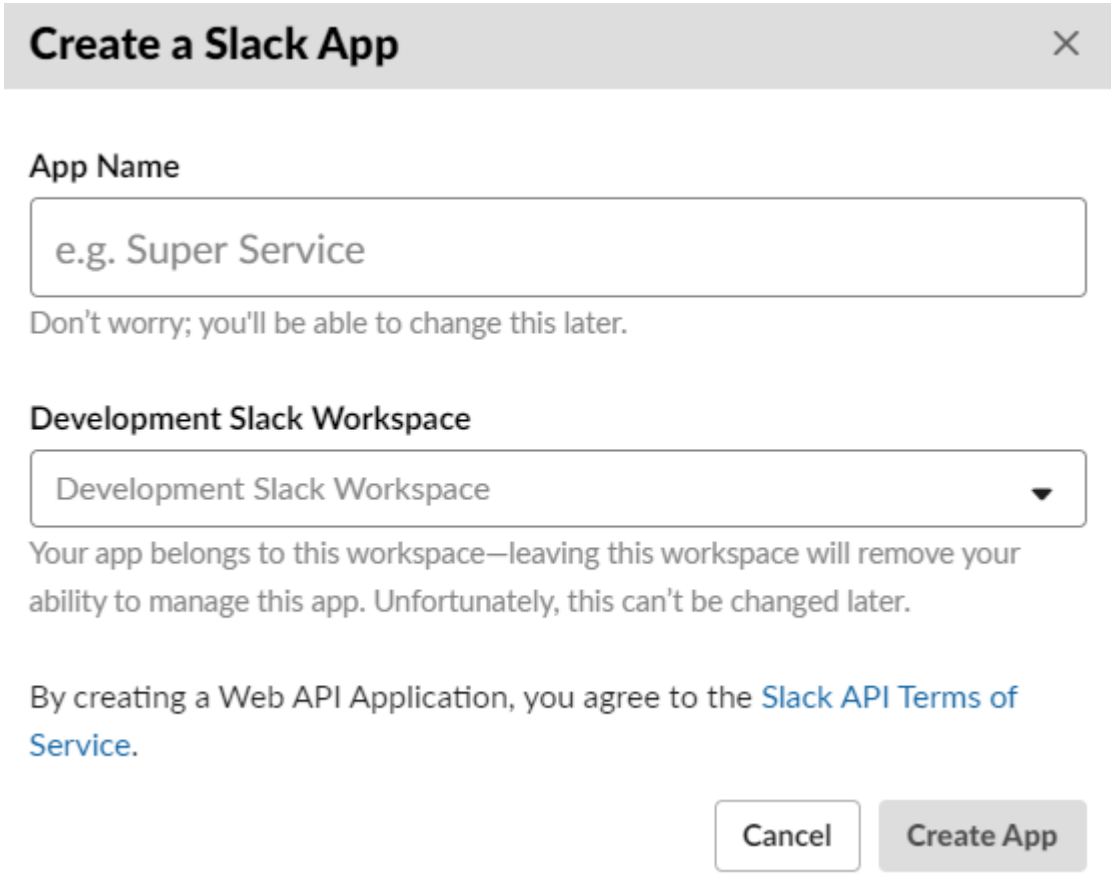
Slack 的 Webhook 示例

Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送警报通知。本页提供了为 Slack 设置 webhook 的示例。

本页引用第三方说明，可能会有所变更。请参阅"Slack 文档"以获取最新信息。

Slack 示例：

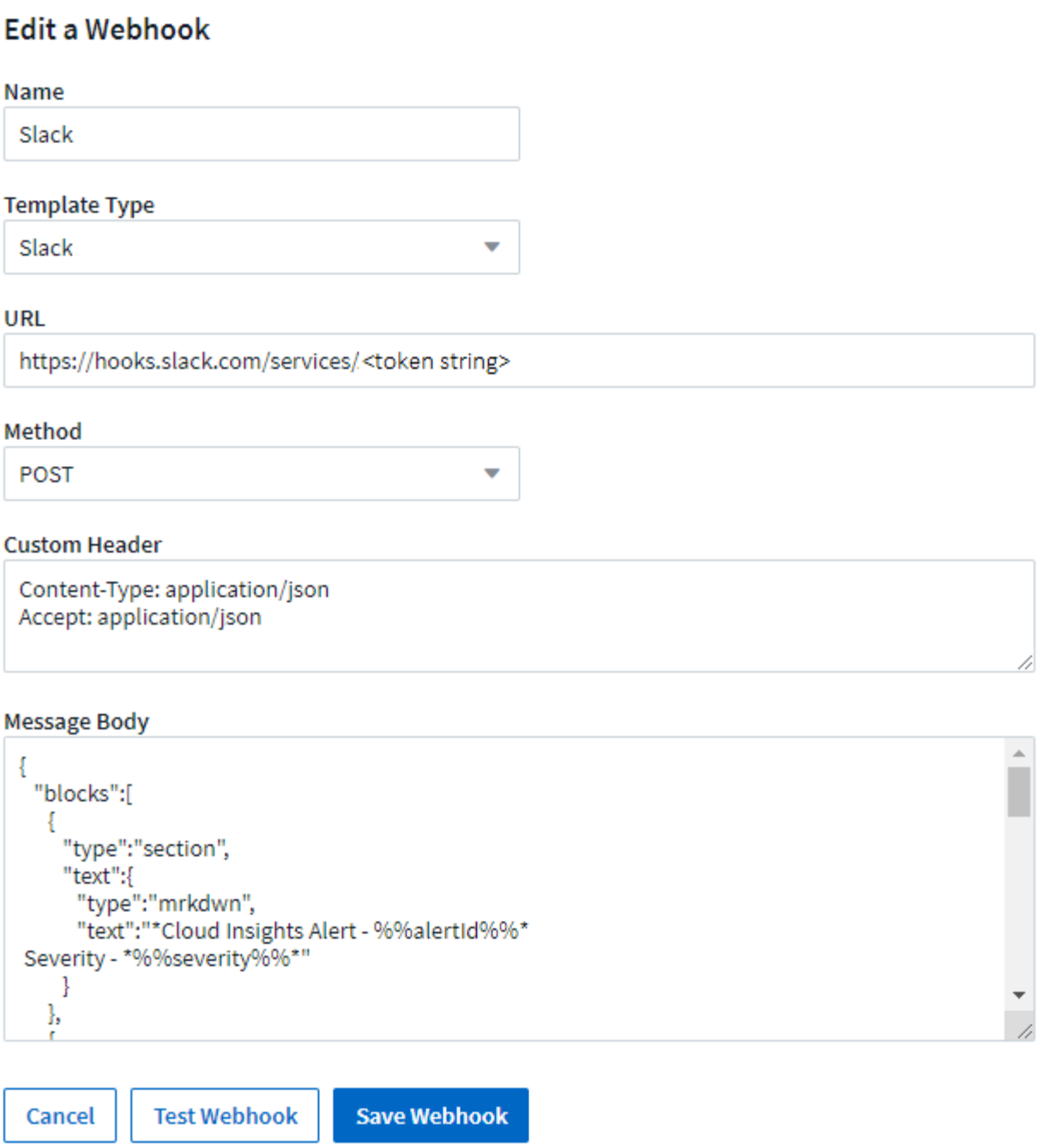
- 前往 https://api.slack.com/apps并创建一个新的应用程序。给它一个有意义的名字并选择 Slack Workspace。



- 转到传入 Webhook，单击_激活传入 Webhook_，请求_添加新 Webhook_，然后选择要发布的频道。
- 复制 Webhook URL。您需要将其粘贴到Data Infrastructure Insightswebhook 配置中。

创建**Data Infrastructure InsightsWebhook**：

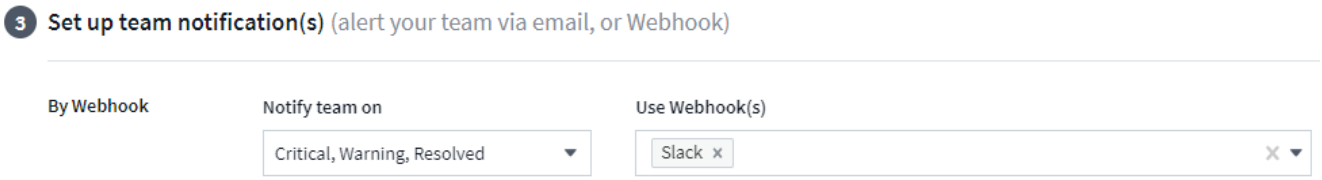
1. 在Data Infrastructure Insights中，导航到 管理 > 通知 并选择 **Webhooks** 选项卡。单击 **+Webhook** 创建一个新 webhook。
2. 为 webhook 赋予一个有意义的名称，例如“Slack Webhook”。
3. 在“模板类型”下拉菜单中，选择“Slack”。
4. 将上面的 URL 粘贴到 *URL* 字段中。



通过 **Webhook** 发送通知

要通过 webhook 通知事件，请在Data Infrastructure Insights中导航至 **Alerts > Monitors**，然后单击 **+Monitor** 以创建新的"监视器"。

- 选择一个指标并定义监视器的条件。
- 在“设置团队通知”下，选择“Webhook”传送方式。
- 为所需事件（严重、警告、已解决）选择“Slack”webhook



更多信息：

- 要修改消息格式和布局，请参阅 https://api.slack.com/messaging/composing
- 错误处理： https://api.slack.com/messaging/webhooks#handling_errors

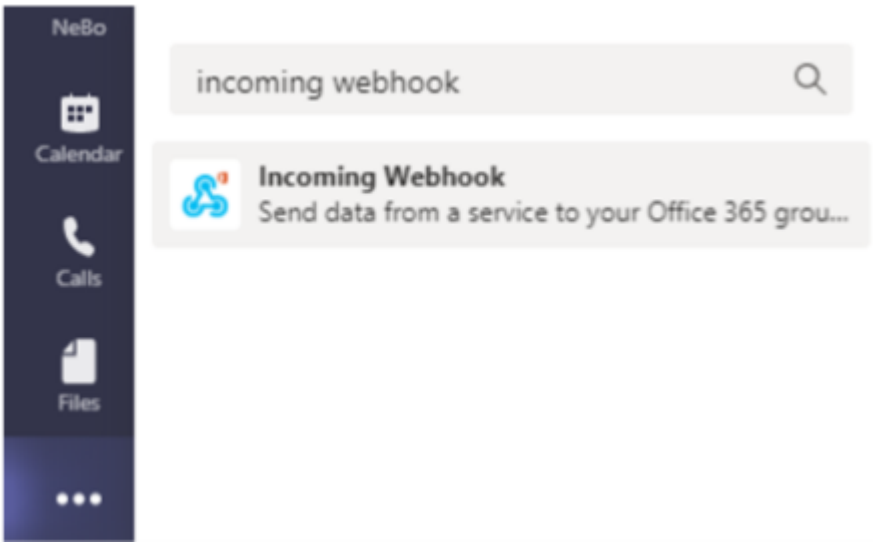
Microsoft Teams 的 Webhook 示例

Webhook 允许用户使用自定义的 webhook 通道向各种应用程序发送警报通知。本页提供了为 Teams 设置 webhook 的示例。

本页引用第三方说明，可能会有所变更。请参阅"团队文档"以获取最新信息。

团队设置：

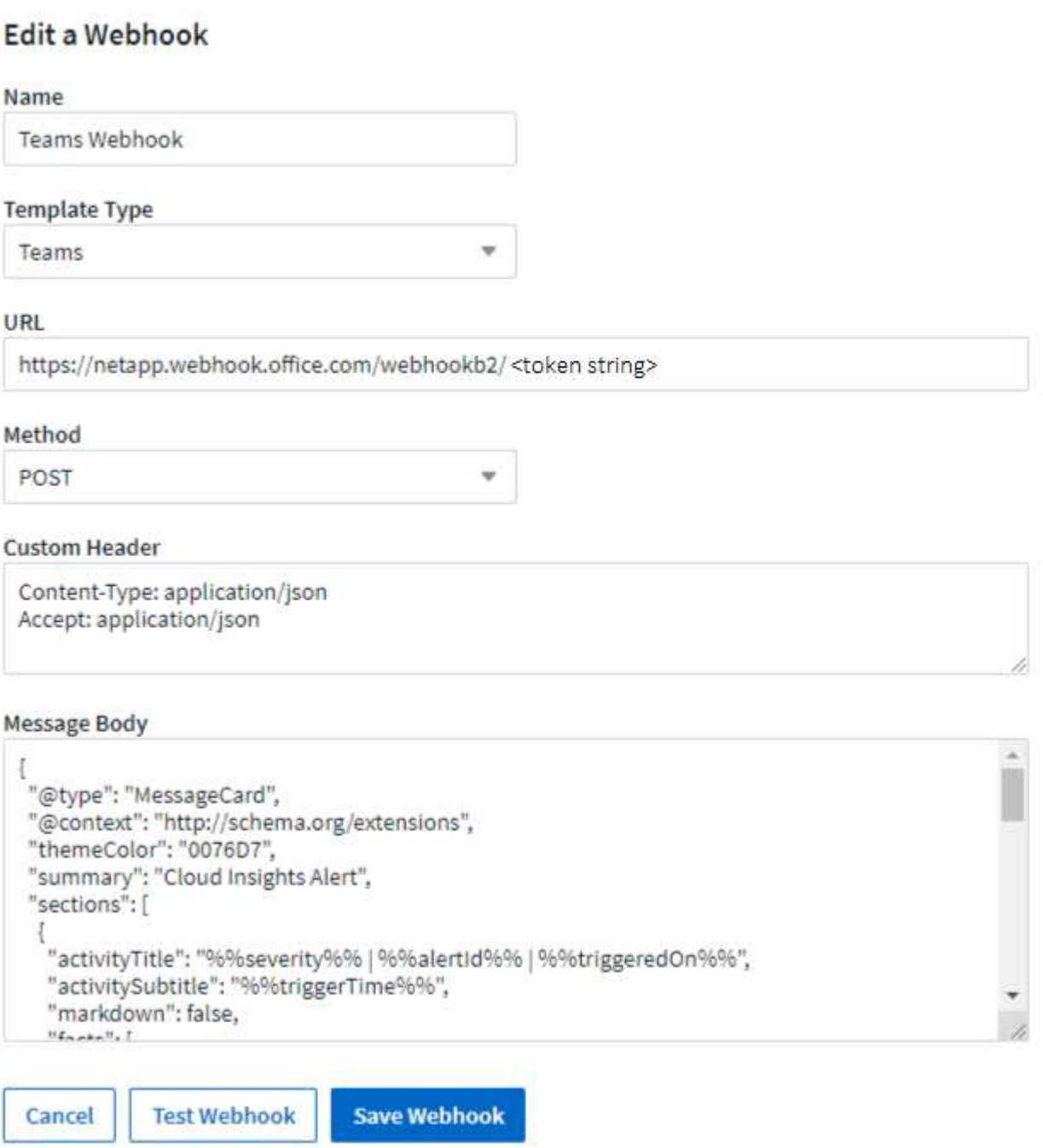
1. 在 Teams 中，选择 kebab，然后搜索 Incoming Webhook。



2. 选择*添加到团队>选择团队>设置连接器*。
3. 复制 Webhook URL。您需要将其粘贴到Data Infrastructure Insightswebhook 配置中。

创建**Data Infrastructure InsightsWebhook**：

1. 在Data Infrastructure Insights中，导航到 管理 > 通知 并选择 **Webhooks** 选项卡。单击 **+Webhook** 创建一个新 webhook。
2. 为 webhook 赋予一个有意义的名称，例如“Teams Webhook”。
3. 在“模板类型”下拉菜单中，选择“团队”。

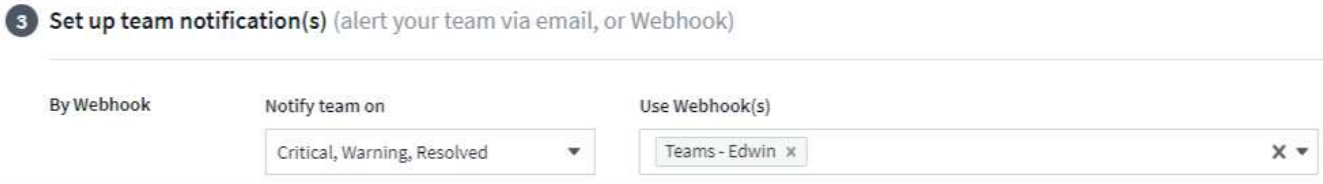


1. 将上面的 URL 粘贴到 *URL* 字段中。

通过 **Webhook** 发送通知

要通过 webhook 通知事件，请在Data Infrastructure Insights中导航至 **Alerts > Monitors**，然后单击 **+Monitor** 以创建新的"监视器"。

- 选择一个指标并定义监视器的条件。
- 在“设置团队通知”下，选择“Webhook”传送方式。
- 为所需事件（严重、警告、已解决）选择“团队” webhook


3
Set up team notification(s) (alert your team via email, or Webhook)
By Webhook
Notify team on
Critical, Warning, Resolved
Use Webhook(s)
Teams - Edwin ×

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。