



## 管理警报

### OnCommand Unified Manager 9.5

NetApp

October 23, 2024

# 目录

|                 |   |
|-----------------|---|
| 管理警报            | 1 |
| 什么是警报           | 1 |
| 警报电子邮件中包含哪些信息   | 1 |
| 正在添加警报          | 2 |
| 为性能事件添加警报       | 4 |
| 从生成警报中排除灾难恢复目标卷 | 5 |
| 测试警报            | 6 |
| 查看警报            | 6 |
| 编辑警报            | 7 |
| 删除警报            | 7 |
| 警报窗口和对话框的问题描述   | 8 |

# 管理警报

您可以将警报配置为在发生特定事件或特定严重性类型的事件时自动发送通知。您还可以将警报与触发警报时执行的脚本相关联。

## 什么是警报

事件持续发生时，只有当事件满足指定的筛选条件时， Unified Manager 才会生成警报。您可以选择应生成警报的事件，例如，超过空间阈值或对象脱机时。您还可以将警报与触发警报时执行的脚本相关联。

筛选条件包括对象类，名称或事件严重性。

## 警报电子邮件中包含哪些信息

Unified Manager警报电子邮件提供事件类型、事件严重性、为发生原因 事件而违反的策略名称以及事件的问题描述。此电子邮件还为每个事件提供了一个超链接，可用于在用户界面中查看此事件的详细信息页面。

警报电子邮件会发送给订阅接收警报的所有用户。

如果性能计数发生原因器或容量值在收集期间发生较大变化，则对于同一阈值策略，可能会同时触发严重事件和警告事件。在这种情况下，您可能会收到一封有关警告事件的电子邮件和一封有关严重事件的电子邮件。这是因为您可以通过 Unified Manager 单独订阅来接收警告和严重阈值违规的警报。



升级到Unified Manager 7.2或更高版本后、由于事件和警报URL发生更改、从旧版本Unified Manager发送的电子邮件中指向事件和警报的链接将不再起作用。

下面显示了一个警报电子邮件示例：

From: 10.11.12.13@company.com  
Sent: Tuesday, May 1, 2018 7:45 PM  
To: sclaus@company.com; user1@company.com  
Subject: Alert from OnCommand Unified Manager: Thin-Provisioned Volume Space At Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk  
Impact Area - Capacity  
Severity - Warning  
State - New  
Source - svm\_n1:/sm\_vol\_23  
Cluster Name - fas3250-39-33-37  
Cluster FQDN - fas3250-39-33-37-cm.company.com  
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:

<https://10.11.12.13:443/events/94>

Source details:

<https://10.11.12.13:443/health/volumes/106>

Alert details:

<https://10.11.12.13:443/alerting/1>

## 正在添加警报

您可以配置警报，以便在生成特定事件时向您发出通知。您可以为单个资源，一组资源或特定严重性类型的事件配置警报。您可以指定通知频率，并将脚本与警报关联。

### 开始之前

- 您必须已配置通知设置、例如用户电子邮件地址、SMTP服务器和SNMP陷阱主机、以便Unified Manager服务器能够使用这些设置在生成事件时向用户发送通知。
- 您必须了解要触发警报的资源 and 事件，以及要通知的用户的用户名或电子邮件地址。
- 如果要根据事件执行脚本、则必须已使用管理/脚本页面将脚本添加到Unified Manager中。
- 您必须具有OnCommand 管理员或存储管理员角色。

### 关于此任务

除了从配置/警报页面创建警报之外、您还可以在收到事件后直接从事件详细信息页面创建警报、如下所述。

### 步骤

1. 在左侧导航窗格中、单击\*配置\*>\*警报\*。

2. 在\*配置/警报\*页面中、单击\*添加\*。
3. 在 \* 添加警报 \* 对话框中，单击 \* 名称 \* ，然后输入警报的名称和问题描述。
4. 单击 \* 资源 \* ，然后选择要包含在警报中或从警报中排除的资源。

您可以通过在 \* 名称包含 \* 字段中指定文本字符串来设置筛选器，以选择一组资源。根据您指定的文本字符串，可用资源列表仅显示与筛选器规则匹配的资源。指定的文本字符串区分大小写。

如果某个资源同时符合您指定的包含和排除规则，则排除规则优先于包含规则，并且不会为与排除的资源相关的事件生成警报。

5. 单击 \* 事件 \* ，然后根据要触发警报的事件名称或事件严重性类型选择事件。



要选择多个事件，请在选择时按 Ctrl 键。

6. 单击 \* 操作 \* ，然后选择要通知的用户，选择通知频率，选择是否将 SNMP 陷阱发送到陷阱接收方，并分配生成警报时要执行的脚本。



如果修改为用户指定的电子邮件地址并重新打开警报进行编辑，则 " 名称 " 字段将显示为空，因为修改后的电子邮件地址不再映射到先前选择的用户。此外、如果您从"管理/用户"页面修改了选定用户的电子邮件地址、则修改后的电子邮件地址不会针对选定用户进行更新。

您也可以选择通过 SNMP 陷阱通知用户。

7. 单击 \* 保存 \* 。

## 添加警报的示例

此示例显示了如何创建满足以下要求的警报：

- 警报名称： HealthTest
- 资源：包括名称包含 "abc`" 的所有卷，并排除名称包含 "xyz`" 的所有卷
- 事件：包括所有严重运行状况事件
- 操作：包括 "sample@domain.com`"、"Test`"脚本、必须每15分钟通知一次用户

在添加警报对话框中执行以下步骤：

1. 单击\*名称\*、然后输入 HealthTest 在\*警报名称\*字段中。
2. 单击 \* 资源 \* ，然后在包括选项卡中，从下拉列表中选择 \* 卷 \* 。
  - a. 输入 ... abc 在\*名称包含\*字段中、显示名称包含"abc`"的卷。
  - b. 从"Available Resources"区域中选择\* <Resources>\* <All Volumes whose name contains 'abc'> 、然后将其移动到"Selected Resources"区域。
  - c. 单击\*排除\*、然后输入 xyz 在\*名称包含\*字段中、然后单击\*添加\*。
3. 单击 \* 事件 \* ，然后从事件严重性字段中选择 \* 严重 \* 。
4. 从匹配事件区域中选择 \* 所有严重事件 \* ，然后将其移动到选定事件区域。

5. 单击\*操作\*、然后输入 sample@domain.com 在向这些用户发送警报字段中。

6. 选择 \* 每 15 分钟提醒一次 \* 以每 15 分钟通知一次用户。

您可以将警报配置为在指定时间内向收件人重复发送通知。您应确定警报的事件通知处于活动状态的时间。

7. 在选择要执行的脚本菜单中、选择\*测试\*脚本。

8. 单击 \* 保存 \*。

## 添加警报的准则

您可以根据资源添加警报，例如集群，节点，聚合或卷以及特定严重性类型的事件。作为最佳实践，您可以在添加任何关键对象所属的集群后为该对象添加警报。

您可以使用以下准则和注意事项创建警报，以便有效地管理系统：

- 警报问题描述

您应为此警报提供一个问题描述，以帮助您有效地跟踪警报。

- Resources

您应确定哪些物理或逻辑资源需要警报。您可以根据需要包括和排除资源。例如，如果要通过配置警报来密切监控聚合，则必须从资源列表中选择所需的聚合。

- 事件严重性

您应确定指定严重性类型的事件（严重，错误，警告）是否应触发警报，如果是，则应触发哪种严重性类型。

- 事件名称

如果您根据生成的事件类型添加警报、则应确定哪些事件需要警报

- 操作

您必须提供接收通知的用户的用户名和电子邮件地址。您还可以将 SNMP 陷阱指定为通知模式。您可以将脚本与警报关联，以便在生成警报时执行这些脚本。

- 通知频率

您可以将警报配置为在指定时间内向收件人重复发送通知。您应确定警报的事件通知处于活动状态的时间。如果要在事件确认之前重复发送事件通知，则应确定重复发送通知的频率。

- 执行脚本

您可以将脚本与警报关联。生成警报时会执行脚本。

## 为性能事件添加警报

您可以为单个性能事件配置警报，就像 Unified Manager 收到的任何其他事件一样。此外

，如果您希望对所有性能事件进行同样的处理并将电子邮件发送给同一个人，则可以创建一个警报，以便在触发任何严重或警告性能事件时向您发出通知。

## 开始之前

您必须具有OnCommand 管理员或存储管理员角色。

## 关于此任务

以下示例显示了如何为所有严重延迟， IOPS 和 MBps 事件创建事件。您可以使用相同的方法从所有性能计数器中选择事件，并为所有警告事件选择事件。

## 步骤

1. 在左侧导航窗格中、单击\*配置\*>\*警报\*。
2. 在\*配置/警报\*页面中、单击\*添加\*。
3. 在 \* 添加警报 \* 对话框中，单击 \* 名称 \* ，然后输入警报的名称和问题描述。
4. 请勿在 \* 资源 \* 页面上选择任何资源。

由于未选择任何资源，因此警报将应用于接收这些事件的所有集群，聚合，卷等。

5. 单击 \* 事件 \* 并执行以下操作：
  - a. 在事件严重性列表中，选择 \* 严重 \* 。
  - b. 在Event Name contains字段中、输入 latency 然后单击箭头以选择所有匹配的事件。
  - c. 在Event Name contains字段中、输入 iops 然后单击箭头以选择所有匹配的事件。
  - d. 在Event Name contains字段中、输入 mbps 然后单击箭头以选择所有匹配的事件。
6. 单击 \* 操作 \* ，然后在 \* 提醒这些用户 \* 字段中选择要接收警报电子邮件的用户的名称。
7. 在此页面上配置任何其他选项以发出 SNMP 陷阱并执行脚本。
8. 单击 \* 保存 \* 。

## 从生成警报中排除灾难恢复目标卷

配置卷警报时，您可以在警报对话框中指定一个字符串，用于标识一个卷或一组卷。但是，如果为 SVM 配置了灾难恢复，则源卷和目标卷的名称相同，因此您将收到这两个卷的警报。

## 开始之前

您必须具有OnCommand 管理员或存储管理员角色。

## 关于此任务

您可以通过排除名称为目标 SVM 的卷来禁用灾难恢复目标卷的警报。之所以可以这样<volume\_name> 做、是

因为卷事件的标识符同时包含SVM名称和卷名称、格式为"<svm\_name> : /SVM"。

以下示例显示了如何在主SVM"vs1"上为卷"vol1"创建警报、但不会在SVM"vs1-dr"上的同名卷上生成警报。

在添加警报对话框中执行以下步骤：

## 步骤

1. 单击 \* 名称 \* ，然后输入警报的名称和问题描述。
2. 单击 \* 资源 \* ，然后选择 \* 包括 \* 选项卡。
  - a. 从下拉列表中选择\*卷\*、然后输入 vol1 在\*名称包含\*字段中、显示名称包含"vol1"的卷。
  - b. 选择\*[All Volumes whose name contains 'vol1']\*、然后将其移动到\*选定资源\*区域。
3. 选择\*排除\*选项卡、选择\*卷\*、然后输入 vs1-dr 在\*名称包含\*字段中、然后单击\*添加\*。

这样就不会为SVM"vs1-dr"上的卷"vol1"生成警报。

4. 单击 \* 事件 \* 并选择要应用于卷的一个或多个事件。
5. 单击 \* 操作 \* ，然后在 \* 提醒这些用户 \* 字段中选择要接收警报电子邮件的用户的名称。
6. 在此页面上配置用于发出 SNMP 陷阱和执行脚本的任何其他选项，然后单击 \* 保存 \* 。

## 测试警报

您可以测试警报，以验证是否已正确配置警报。触发事件后，系统将生成警报，并向配置的收件人发送警报电子邮件。您可以使用测试警报验证是否发送通知以及是否执行脚本。

### 开始之前

- 您必须已配置通知设置，例如收件人的电子邮件地址，SMTP 服务器和 SNMP 陷阱。

Unified Manager 服务器可以使用这些设置在生成事件时向用户发送通知。

- 您必须已分配脚本并将脚本配置为在生成警报时运行。
- 您必须具有OnCommand 管理员角色。

## 步骤

1. 在左侧导航窗格中、单击\*配置\*>\*警报\*。
2. 在\*配置/警报\*页面中、选择要测试的警报、然后单击\*测试\*。

系统会向您创建警报时指定的电子邮件地址发送测试警报电子邮件。

## 查看警报

您可以从配置/警报页面查看为各种事件创建的警报列表。您还可以查看警报属性，例如警

报问题描述，通知方法和频率，触发警报的事件，警报的电子邮件收件人以及受影响的资源（例如集群，聚合和卷）。

## 开始之前

您必须具有操作员、OnCommand 管理员或存储管理员角色。

## 步骤

1. 在左侧导航窗格中、单击\*配置\*>\*警报\*。

警报列表将显示在配置/警报页面中。

## 编辑警报

您可以编辑警报属性，例如与警报关联的资源，事件，收件人，通知选项，通知频率，和关联脚本。

## 开始之前

您必须具有OnCommand 管理员角色。

## 步骤

1. 在左侧导航窗格中、单击\*配置\*>\*警报\*。
2. 在\*配置/警报\*页面中、选择要编辑的警报、然后单击\*编辑\*。
3. 在 \* 编辑警报 \* 对话框中，编辑名称，资源，事件和操作部分， 根据需要。

您可以更改或删除与警报关联的脚本。

4. 单击 \* 保存 \*。

## 删除警报

您可以删除不再需要的警报。例如，如果 Unified Manager 不再监控某个特定资源，则可以删除为该资源创建的警报。

## 开始之前

您必须具有OnCommand 管理员角色。

## 步骤

1. 在左侧导航窗格中、单击\*配置\*>\*警报\*。
2. 在\*配置/警报\*页面上、选择要删除的警报、然后单击\*删除\*。

3. 单击 \* 是 \* 确认删除请求。

## 警报窗口和对话框的问题描述

您应使用添加警报对话框配置警报以接收有关事件的通知。您还可以从配置/警报页面查看警报列表。

### 配置/警报页面

配置/警报页面显示警报列表、并提供有关警报名称、状态、通知方法和通知频率的信息。您还可以从此页面添加，编辑，删除，启用或禁用警报。

您必须具有OnCommand 管理员或存储管理员角色。

#### 命令按钮

- \* 添加 \*。

显示添加警报对话框，在此可以添加新警报。

- \* 编辑 \*。

显示编辑警报对话框，在此可以编辑选定警报。

- \* 删除 \*。

删除选定警报。

- \* 启用 \*。

启用选定警报以发送通知。

- \* 禁用 \*。

如果要暂时停止发送通知，则禁用选定警报。

- \* 测试 \*。

添加或编辑选定警报后，将对其进行测试以验证其配置。

#### 列表视图

列表视图以表格形式显示有关已创建警报的信息。您可以使用列筛选器自定义显示的数据。您也可以选择警报，以便在详细信息区域中查看其详细信息。

- \* 状态 \*。

指定是否启用警报 () 或已禁用 ()。

- \* 警报 \*。

显示警报的名称。

- \* 问题描述 \*

显示警报的问题描述。

- \* 通知方法 \*

显示为警报选择的 notification 方法。您可以通过电子邮件或 SNMP 陷阱通知用户。

- \* 通知频率 \*

指定在事件被确认，解决或移至 " 已废弃 " 状态之前管理服务器继续发送通知的频率（以分钟为单位）。

## 详细信息区域

详细信息区域提供了有关选定警报的详细信息。

- \* 警报名称 \*

显示警报的名称。

- \* 警报问题描述 \*

显示警报的问题描述。

- \* 事件 \*

显示要触发警报的事件。

- \* 资源 \*

显示要触发警报的资源。

- \* 包括 \*

显示要触发警报的资源组。

- \* 不包括 \*

显示不希望触发警报的资源组。

- \* 通知方法 \*

显示警报的通知方法。

- \* 通知频率 \*

显示在事件被确认，解决或移至 " 已废弃 " 状态之前管理服务器继续发送警报通知的频率。

- \* 脚本名称 \*

显示与选定警报关联的脚本的名称。此脚本会在生成警报时执行。

- \* 电子邮件收件人 \*

显示接收警报通知的用户的电子邮件地址。

## 添加警报对话框

您可以创建警报，以便在生成特定事件时向您发出通知，从而快速解决问题描述问题，从而最大限度地减少对环境的影响。您可以为单个资源或一组资源以及特定严重性类型的事件创建警报。您还可以指定警报的通知方法和频率。

您必须具有OnCommand 管理员或存储管理员角色。

### Name

使用此区域可以指定警报的名称和问题描述：

- \* 警报名称 \*

用于指定警报名称。

- \* 警报问题描述 \*

用于指定警报的问题描述。

### Resources

通过此区域，您可以根据要触发警报的动态规则选择单个资源或对资源进行分组。*dynamic rule* 是根据您指定的文本字符串筛选的一组资源。您可以通过从下拉列表中选择资源类型来搜索资源，也可以指定确切的资源名称来显示特定资源。

如果您从任何存储对象详细信息页面创建警报，则此存储对象将自动包含在警报中。

- \* 包括 \*

用于包括要触发警报的资源。您可以指定一个文本字符串，以便对与该字符串匹配的资源进行分组，并选择要包含在警报中的此组。例如、您可以对名称包含"abc"字符串的所有卷进行分组。

- \* 排除 \*

用于排除不希望触发警报的资源。例如，您可以排除名称包含 "xyz" 字符串的所有卷。

只有在选择特定资源类型的所有资源时、才会显示排除选项卡：例如、[\[All Volumes\]](#) 或 [\[All Volumes whose name contains 'xyz'\]](#)。

如果某个资源同时符合您指定的包含和排除规则，则排除规则优先于包含规则，并且不会为此事件生成警报。

## 事件

通过此区域，您可以选择要为其创建警报的事件。您可以根据特定严重性为事件创建警报，也可以为一组事件创建警报。

要选择多个事件，应在选择时按住 Ctrl 键。

- \* 事件严重性 \*

用于根据严重性类型选择事件，可以是 " 严重 " ， " 错误 " 或 " 警告 " 。

- \* 事件名称包含 \*

用于选择名称包含指定字符的事件。

## 操作

通过此区域，您可以指定要在触发警报时通知的用户。您还可以指定通知方法和通知频率。

- \* 向这些用户发送警报 \*

用于指定接收通知的用户的电子邮件地址或用户名。

如果修改为用户指定的电子邮件地址并重新打开警报进行编辑，则 " 名称 " 字段将显示为空，因为修改后的电子邮件地址不再映射到先前选择的用户。此外、如果您已从 " 管理 / 用户 " 页面修改选定用户的电子邮件地址、则修改后的电子邮件地址不会针对选定用户进行更新。

- \* 通知频率 \*

用于指定在事件被确认，解决或移至已废弃状态之前管理服务器发送通知的频率。

您可以选择以下通知方法：

- 仅通知一次
- 按指定频率通知
- 在指定时间范围内以指定频率通知

- \* 问题描述 SNMP 陷阱 \*

选中此框可指定是否应将 SNMP 陷阱发送到全局配置的 SNMP 主机。

- \* 执行脚本 \*

用于将自定义脚本添加到警报。此脚本会在生成警报时执行。

## 命令按钮

- \* 保存 \*

创建警报并关闭对话框。

- \* 取消 \*

丢弃所做的更改并关闭对话框。

## 编辑警报对话框

您可以编辑警报属性，例如与警报关联的资源，事件，脚本和通知选项。

### Name

通过此区域，您可以编辑警报的名称和问题描述。

- \* 警报名称 \*

用于编辑警报名称。

- \* 警报问题描述 \*

用于指定警报的问题描述。

- \* 警报状态 \*

用于启用或禁用警报。

### Resources

通过此区域，您可以根据要触发警报的动态规则选择单个资源或对资源进行分组。您可以通过从下拉列表中选择资源类型来搜索资源，也可以指定确切的资源名称来显示特定资源。

- \* 包括 \*

用于包括要触发警报的资源。您可以指定一个文本字符串，以便对与该字符串匹配的资源进行分组，并选择要包含在警报中的此组。例如，您可以对名称包含 "vol0" 字符串的所有卷进行分组。

- \* 排除 \*

用于排除不希望触发警报的资源。例如，您可以排除名称包含 "xyz" 字符串的所有卷。



只有在选择特定资源类型的所有资源时、才会显示排除选项卡、例如 [\[All Volumes\]](#) 或 [\[All Volumes whose name contains 'xyz'\]](#)。

### 事件

通过此区域，您可以选择要触发警报的事件。您可以根据特定严重性为事件触发警报，也可以针对一组事件触发警报。

- \* 事件严重性 \*

用于根据严重性类型选择事件，可以是 "严重"，"错误" 或 "警告"。

- \* 事件名称包含 \*

用于选择名称包含指定字符的事件。

## 操作

此区域用于指定通知方法和通知频率。

- \* 向这些用户发送警报 \*

用于编辑电子邮件地址或用户名，或者指定新的电子邮件地址或用户名以接收通知。

- \* 通知频率 \*

用于编辑管理服务器发送通知的频率，直到事件被确认，解决或移至已废弃状态为止。

您可以选择以下通知方法：

- 仅通知一次
- 按指定频率通知
- 在指定时间范围内以指定频率通知

- \* 问题描述 SNMP 陷阱 \*

用于指定是否应将 SNMP 陷阱发送到全局配置的 SNMP 主机。

- \* 执行脚本 \*

用于将脚本与警报关联。此脚本会在生成警报时执行。

## 命令按钮

- \* 保存 \*

保存更改并关闭对话框。

- \* 取消 \*

丢弃所做的更改并关闭对话框。

## 版权信息

版权所有 © 2024 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。