配置通知

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/active-iq-unified-manager-918/config/task_configure_unified_manager_to_send_alert_notifications.html on November 13, 2026. Always check docs.netapp.com for the latest.

目录

配置通知 . . . 1
- 配置 Active IQ Unified Manager 以发送警报通知 . . . 1
- 在 Active IQ Unified Manager 中配置事件通知设置 . . . 1
- 在 Active IQ Unified Manager 中启用远程身份验证 . . . 2
- 在 Active IQ Unified Manager 中禁用远程身份验证中的嵌套组 . . . 3
- 在 Active IQ Unified Manager 中设置身份验证服务 . . . 4
- 向 Active IQ Unified Manager 添加身份验证服务器 . . . 5
- 测试 Active IQ Unified Manager 中身份验证服务器的配置 . . . 6
- 在 Active IQ Unified Manager 中添加警报 . . . 6
  - 添加警报的示例 . . . 7

配置通知

配置 Active IQ Unified Manager 以发送警报通知

您可以将 Unified Manager 配置为发送通知，提醒您环境中的事件。在发送通知之前，必须配置多个其他 Unified Manager 选项。

开始之前

您必须具有应用程序管理员角色。

部署 Unified Manager 并完成初始配置后，应考虑配置环境以触发警报，并根据接收到的事件生成通知电子邮件或 SNMP 陷阱。

步骤

1. "配置事件通知设置"。

   如果要在环境中发生某些事件时发送警报通知，则必须配置 SMTP 服务器并提供用于发送警报通知的电子邮件地址。如果要使用 SNMP 陷阱，可以选择该选项并提供必要的信息。

2. "启用远程身份验证"。

   如果希望远程 LDAP 或 Active Directory 用户访问 Unified Manager 实例并接收警报通知，则必须启用远程身份验证。

3. "添加身份验证服务器"。

   您可以添加身份验证服务器，以便身份验证服务器中的远程用户可以访问 Unified Manager。

4. "添加用户"。

   您可以添加几种不同类型的本地或远程用户并分配特定角色。在您创建警报时，您需要指定一个用户来接收警报通知。

5. "添加警报"。

   添加发送通知的电子邮件地址，添加接收通知的用户，配置网络设置，以及配置环境所需的 SMTP 和 SNMP 选项后，即可分配警报。

在 Active IQ Unified Manager 中配置事件通知设置

您可以将 Unified Manager 配置为在生成事件或将事件分配给用户时发送警报通知。您可以配置用于发送警报的 SMTP 服务器，也可以设置各种通知机制——例如，警报通知可以作为电子邮件或 SNMP 陷阱发送。

开始之前

您必须具有下列信息：

- 发送警报通知的电子邮件地址

电子邮件地址显示在发送的警报通知中的“From”字段中。如果由于任何原因无法发送电子邮件，此电子邮件地址也将用作无法投递邮件的收件人。

- SMTP 服务器主机名，以及访问服务器的用户名和密码
- 将接收 SNMP 陷阱的陷阱目标主机的主机名或 IP 地址，以及 SNMP 版本、出站陷阱端口、团体和其他必需的 SNMP 配置值

  要指定多个陷阱目标，请使用逗号分隔每个主机。在这种情况下，所有其他 SNMP 设置（例如版本和出站陷阱端口）必须对于此列表中的所有主机都相同。

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*常规* > 通知。
2. 在“通知”页面中，配置适当的设置。

   备注：

   - 如果发件人地址预先填写了地址“ActiveIQUnifiedManager@localhost.com”，则应将其更改为真实有效的电子邮件地址，以确保所有电子邮件通知都能成功发送。
   - 如果无法解析 SMTP 服务器的主机名，则可以指定 SMTP 服务器的 IP 地址（IPv4 或 IPv6）而不是主机名。
3. 单击 **Save**。
4. 如果您选择了 使用 **STARTTLS** 或 使用 **SSL** 选项，则单击 保存 按钮后会显示证书页面。验证证书详细信息并接受证书以保存通知设置。

   您可以单击*查看证书详细信息*按钮以查看证书详细信息。如果现有证书已过期，请取消选中*使用 STARTTLS*或*使用 SSL*复选框，保存通知设置，然后再次选中*使用 STARTTLS*或*使用 SSL*复选框以查看新证书。

在 **Active IQ Unified Manager** 中启用远程身份验证

您可以启用远程身份验证，以便 Unified Manager 服务器可以与您的身份验证服务器通信。身份验证服务器的用户可以访问 Unified Manager 图形界面来管理存储对象和数据。

开始之前

您必须具有应用程序管理员角色。

Unified Manager 服务器必须直接连接到身份验证服务器。您必须禁用任何本地 LDAP 客户端，例如 SSSD（系统安全服务后台程序）或 NSLCD（名称服务 LDAP 缓存后台程序）。

您可以使用 Open LDAP 或 Active Directory 启用远程身份验证。如果禁用远程身份验证，远程用户将无法访问 Unified Manager。

支持通过 LDAP 和 LDAPS（安全 LDAP）进行远程身份验证。Unified Manager 使用 389 作为非安全通信的默认端口，636 作为安全通信的默认端口。

用于对用户进行身份验证的证书必须符合 X.509 格式。

步骤

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 选中*启用远程身份验证……*的复选框。
3. 在身份验证服务字段中，选择服务类型并配置身份验证服务。

对于身份验证类型……	输入以下信息……
Active Directory	• 以下格式之一的身份验证服务器管理员名称： ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` （使用适当的 LDAP 表示法） • 管理员密码 • 基本可分辨名称（使用适当的 LDAP 表示法）
打开 LDAP	• 绑定可分辨名称（使用适当的 LDAP 表示法） • 绑定密码 • 基本可分辨名称

如果 Active Directory 用户的身份验证需要很长时间或超时，则身份验证服务器可能需要很长时间才能响应。在 Unified Manager 中禁用对嵌套组的支持可能会缩短身份验证时间。

如果为身份验证服务器选择使用安全连接选项，则 Unified Manager 将使用安全套接字层（SSL）协议与身份验证服务器进行通信。

4. 可选： 添加身份验证服务器，并测试身份验证。
5. 单击 **Save**。

在 Active IQ Unified Manager 中禁用远程身份验证中的嵌套组

如果启用了远程身份验证，则可以禁用嵌套组身份验证，以便只有单个用户（而不是组成员）可以对 Unified Manager 进行远程身份验证。如果要改善 Active Directory 身份验证响应时间，则可以禁用嵌套组。

开始之前

- 您必须具有应用程序管理员角色。
- 禁用嵌套组仅适用于使用 Active Directory 时。

禁用对 Unified Manager 中嵌套组的支持可能会缩短身份验证时间。如果禁用嵌套组支持，并且将远程组添加到 Unified Manager，则单个用户必须是远程组的成员才能向 Unified Manager 进行身份验证。

步骤

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 选中*禁用嵌套组查找*复选框。
3. 单击 **Save**。

在 Active IQ Unified Manager 中设置身份验证服务

身份验证服务在向身份验证服务器中的远程用户或远程组提供对 Unified Manager 的访问权限之前对其进行身份验证。可以通过使用预定义的身份验证服务（如 Active Directory 或 OpenLDAP）或配置自己的身份验证机制来对用户进行身份验证。

开始之前

- 您必须已启用远程身份验证。
- 您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 从下列身份验证服务中选择一项：

如果选择.....	操作
Active Directory	a. 输入管理员名称和密码。 b. 指定身份验证服务器的基本可分辨名称。 例如，如果身份验证服务器的域名为+ou@domain.com+，则基本可分辨名称为*cn=ou,dc=domain,dc=com*。
OpenLDAP	a. 输入绑定可分辨名称和绑定密码。 b. 指定身份验证服务器的基本可分辨名称。 例如，如果身份验证服务器的域名为+ou@domain.com+，则基本可分辨名称为*cn=ou,dc=domain,dc=com*。
其他	a. 输入绑定可分辨名称和绑定密码。 b. 指定身份验证服务器的基本可分辨名称。 例如，如果身份验证服务器的域名为+ou@domain.com+，则基本可分辨名称为*cn=ou,dc=domain,dc=com*。 c. 指定身份验证服务器支持的 LDAP 协议版本。 d. 输入用户名、组成员身份、用户组和成员属性。

如果要修改身份验证服务，则必须删除所有现有的身份验证服务器，然后添加新的身份验证服务器。

3. 单击 **Save**。

向 **Active IQ Unified Manager** 添加身份验证服务器

可以在管理服务器上添加身份验证服务器并启用远程身份验证，以便身份验证服务器中的远程用户可以访问 Unified Manager。

开始之前

- 必须提供以下信息：
  - 身份验证服务器的主机名或 IP 地址
  - 身份验证服务器的端口号
- 必须已启用远程身份验证并配置身份验证服务，以便管理服务器可以对身份验证服务器中的远程用户或组进行身份验证。
- 您必须具有应用程序管理员角色。

如果要添加的身份验证服务器是高可用性（HA）对的一部分（使用相同的数据库），则还可以添加配对身份验证服务器。这样，当其中一个身份验证服务器无法访问时，管理服务器便可以与配对服务器进行通信。

步骤

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 启用或禁用*使用安全连接*选项：

目的	操作
启用	a. 选择*使用安全连接*选项。 b. 在身份验证服务器区域中，单击 添加。 c. 在“添加身份验证服务器”对话框中，输入服务器的身份验证名称或 IP 地址（IPv4 或 IPv6）。 d. 在 Authorize Host 对话框中，单击 View Certificate。 e. 在查看证书对话框中，验证证书信息，然后单击*关闭*。 f. 在 Authorize Host 对话框中，单击 **Yes**。 启用 使用安全连接身份验证 选项时，Unified Manager 将与身份验证服务器通信并显示证书。Unified Manager 使用 636 作为安全通信的默认端口，端口号 389 用于非安全通信。

目的	操作
禁用	a. 清除*使用安全连接*选项。 b. 在身份验证服务器区域中，单击 添加。 c. 在“添加身份验证服务器”对话框中，指定服务器的主机名或 IP 地址（IPv4 或 IPv6）以及端口详细信息。 d. 单击 **Add**。

已添加的身份验证服务器将显示在“服务器”区域中。

3. 执行测试身份验证以确认可以对添加的身份验证服务器中的用户进行身份验证。

测试 **Active IQ Unified Manager** 中身份验证服务器的配置

您可以验证身份验证服务器的配置，以确保管理服务器能够与其通信。您可以通过从身份验证服务器搜索远程用户或远程组并使用配置的设置对其进行身份验证来验证配置。

开始之前

- 必须已启用远程身份验证并配置身份验证服务，以便 Unified Manager 服务器可以对远程用户或远程组进行身份验证。
- 您必须已添加身份验证服务器，以便管理服务器可以从这些服务器中搜索远程用户或远程组并对其进行身份验证。
- 您必须具有应用程序管理员角色。

如果身份验证服务设置为 Active Directory，并且正在验证属于身份验证服务器主组的远程用户的身份验证，则身份验证结果中不会显示有关主组的信息。

步骤

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 单击*测试身份验证*。
3. 在 Test User 对话框中，指定远程用户的用户名和密码或远程组的用户名，然后单击 **Test**。

   如果要对远程组进行身份验证，则不得输入密码。

在 **Active IQ Unified Manager** 中添加警报

您可以配置警报，以便在生成特定事件时通知您。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。您可以指定要收到通知的频率，并将脚本关联到警报。

开始之前

- 您必须配置通知设置（如用户电子邮件地址、SMTP 服务器和 SNMP 陷阱主机），以使 Active IQ Unified Manager 服务器能够在生成事件时使用这些设置向用户发送通知。
- 您必须知道要触发警报的资源和事件，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，则必须使用“脚本”页面将脚本添加到 Unified Manager。
- 您必须具有应用程序管理员或存储管理员角色。

除了从“警报设置”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，如此处所述。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 警报设置。
2. 在警报设置页面中，单击*添加*。
3. 在添加警报对话框中，单击*名称*，并输入警报的名称和描述。
4. 单击*资源*，然后选择要包含在此警报中或从此警报中排除的资源。

   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。根据指定的文本字符串，可用资源列表仅显示与筛选规则匹配的资源。指定的文本字符串区分大小写。

   如果资源同时符合已指定的包含和排除规则，则排除规则优先于包含规则，并且不会为与排除资源相关的事件生成警报。

5. 单击*事件*，并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，请在进行选择时按 Ctrl 键。

6. 单击 操作，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器，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”字段将显示为空白，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，如果从“用户”页面修改了所选用户的电子邮件地址，则不会为所选用户更新已修改的电子邮件地址。

   您也可以选择通过 SNMP 陷阱通知用户。

7. 单击 **Save**。

添加警报的示例

此示例演示如何创建满足以下要求的警报：

- 警报名称：HealthTest
- 资源：包括名称中含有 “abc” 的所有卷，并排除名称中含有 “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"、一个 “Test” 脚本，并且必须每 15 分钟通知一次用户

请在添加警报对话框中执行以下步骤：

步骤

1. 单击*名称*，然后在*警报名称*字段中输入*HealthTest*。

2. 单击*资源*，然后在包含选项卡中，从下拉列表中选择*卷*。
   a. 在 名称包含 字段中输入 **abc** 以显示名称包含 “abc” 的卷。
   b. 从可用资源区域中选择 **<<All Volumes whose name contains 'abc'>>**，并将其移动到选定资源区域。
   c. 单击*排除*，然后在*名称包含*字段中输入*xyz*，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 **All Critical Events**，然后将其移动到"已选择事件"区域。
5. 单击 操作，并在提醒这些用户字段中输入 **sample@domain.com**。
6. 选择*每 15 分钟提醒一次*，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重复向收件人发送通知。您应确定警报的事件通知处于活动状态的时间。

7. 在“Select Script to Execute”菜单中，选择 **Test** 脚本。
8. 单击 **Save**。

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。