管理用户访问

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_add_users.html on November 13, 2026. Always check docs.netapp.com for the latest.

目录

管理用户访问 . . . 1
添加用户 . . . 1
在 Active IQ Unified Manager 中添加用户 . . . 1
在 Active IQ Unified Manager 中创建数据库用户 . . . 1
在 Active IQ Unified Manager 中编辑用户设置 . . . 2
在 Active IQ Unified Manager 中查看用户 . . . 2
删除 Active IQ Unified Manager 中的用户或组 . . . 3
了解 Active IQ Unified Manager 中基于角色的访问控制 . . . 3
了解 Active IQ Unified Manager 中的用户类型 . . . 3
了解 Active IQ Unified Manager 中的用户角色 . . . 4
了解 Active IQ Unified Manager 中的用户角色和功能 . . . 5

管理用户访问

添加用户

在 **Active IQ Unified Manager** 中添加用户

您可以使用“用户”页面添加本地用户或数据库用户。您还可以添加属于身份验证服务器的远程用户或组。您可以为这些用户分配角色，并且根据角色的权限，用户可以使用 Unified Manager 管理存储对象和数据，或查看数据库中的数据。

开始之前

- 您必须具有应用程序管理员角色。
- 要添加远程用户或组，您必须启用远程身份验证并配置身份验证服务器。
- 如果您计划配置 SAML 身份验证，以便身份提供程序（IdP）对访问图形界面的用户进行身份验证，请确保将这些用户定义为 “remote” 用户。

  启用 SAML 身份验证时，不允许类型为“`local`”或“`maintenance`”的用户访问 UI。

如果从 Windows Active Directory 添加组，则所有直接成员和嵌套子组都可以向 Unified Manager 进行身份验证，除非嵌套子组被禁用。如果从 OpenLDAP 或其他身份验证服务添加组，则只有该组的直接成员才能向 Unified Manager 进行身份验证。

步骤

1. 在左侧导航窗格中，单击 常规 > 用户。
2. 在“用户”页面上，单击*添加*。
3. 在“添加用户”对话框中，选择要添加的用户类型，然后输入所需信息。

   输入所需的用户信息时，您必须指定该用户唯一的电子邮件地址。您必须避免指定由多个用户共享的电子邮件地址。

4. 单击 **Add**。

在 **Active IQ Unified Manager** 中创建数据库用户

若要支持 Workflow Automation 和 Unified Manager 之间的连接或访问数据库视图，必须首先在 Unified Manager Web UI 中创建具有“集成架构”或“报告架构”角色的数据库用户。

开始之前

您必须具有应用程序管理员角色。

数据库用户提供与 Workflow Automation 的集成以及对特定于报表的数据库视图的访问。数据库用户无权访问 Unified Manager Web UI 或维护控制台，并且无法执行 API 调用。

步骤

1. 在左侧导航窗格中，单击 常规 > 用户。

2. 在用户页面中，单击*添加*。
3. 在添加用户对话框中，在*类型*下拉列表中选择*数据库用户*。
4. 键入此数据库用户的名称和密码。
5. 在*角色*下拉列表中，选择相应的角色。

如果您是……	选择此角色
将 Unified Manager 与 Workflow Automation 连接	集成架构
访问报告和其他数据库视图	报告架构

6. 单击 **Add**。

在 Active IQ Unified Manager 中编辑用户设置

您可以编辑为每个用户指定的用户设置（例如电子邮件地址和角色）。例如，您可能希望更改存储操作员用户的角色，并将存储管理员权限分配给该用户。

开始之前

您必须具有应用程序管理员角色。

当您修改分配给用户的角色时，会在发生以下任一操作时应用更改：

- 用户注销并重新登录到 Unified Manager。
- 已达到 24 小时的会话超时。

步骤

1. 在左侧导航窗格中，单击 常规 > 用户。
2. 在用户页面中，选择要编辑设置的用户，然后单击*编辑*。
3. 在编辑用户对话框中，编辑为此用户指定的相应设置。
4. 单击 **Save**。

在 Active IQ Unified Manager 中查看用户

您可以使用“用户”页面查看使用 Unified Manager 管理存储对象和数据的用户列表。您可以查看有关用户的详细信息，例如用户名、用户类型、电子邮件地址以及分配给用户的角色。

开始之前

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 > 用户。

删除 **Active IQ Unified Manager** 中的用户或组

您可以从管理服务器数据库中删除一个或多个用户，以防止特定用户访问 Unified Manager。您还可以删除组，以便组中的所有用户都无法再访问管理服务器。

开始之前

- 删除远程组时，必须重新分配已分配给远程组用户的事件。

  如果要删除本地用户或远程用户，则分配给这些用户的事件将自动取消分配。

- 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 > 用户。
2. 在“用户”页面中，选择要删除的用户或组，然后单击 删除。
3. 单击 是 确认删除。

了解 **Active IQ Unified Manager** 中基于角色的访问控制

RBAC（基于角色的访问控制）提供了控制谁有权访问 Active IQ Unified Manager 服务器中的各种功能和资源的功能。RBAC 使管理员能够通过定义角色来管理用户组。如果需要将特定功能的访问权限限制为选定管理员，则必须为其设置管理员帐户。如果要限制管理员可以查看的信息及其可以执行的操作，则必须将角色应用于创建的管理员帐户。

管理服务器使用 RBAC 进行用户登录和角色权限管理。如果您没有更改管理服务器的管理用户访问默认设置，则无需登录即可查看它们。

当您启动需要特定权限的操作时，管理服务器会提示您登录。例如，要创建管理员帐户，必须使用应用程序管理员帐户访问权限登录。

了解 **Active IQ Unified Manager** 中的用户类型

用户类型指定用户持有的帐户类型，包括远程用户、远程组、本地用户、数据库用户和维护用户。每种类型都有自己的角色，由具有管理员角色的用户分配。

Unified Manager 用户类型如下：

- 维护用户

  在 Unified Manager 的初始配置期间创建。然后，维护用户创建其他用户并分配角色。维护用户也是唯一有权访问维护控制台的用户。在 Red Hat Enterprise Linux 系统上安装 Unified Manager 时，维护用户将被赋予用户名 “umadmin.”

- 本地用户

  访问 Unified Manager UI 并根据维护用户或具有应用程序管理员角色的用户赋予的角色执行功能。

- 远程组

  使用存储在身份验证服务器上的凭据访问 Unified Manager UI 的一组用户。此帐户的名称应与存储在身份验证服务器上的组的名称相匹配。远程组中的所有用户都可以使用其个人用户凭据访问 Unified Manager UI。远程组可以根据其分配的角色执行功能。

- 远程用户

  使用存储在身份验证服务器上的凭据访问 Unified Manager UI。远程用户根据维护用户或具有应用程序管理员角色的用户赋予的角色执行功能。

- 数据库用户

  对 Unified Manager 数据库中的数据具有只读访问权限，无权访问 Unified Manager Web 界面或维护控制台，并且无法执行 API 调用。

了解 Active IQ Unified Manager 中的用户角色

维护用户或应用程序管理员为每个用户分配一个角色。每个角色都包含某些特权。您可以在 Unified Manager 中执行的活动范围取决于分配给您的角色以及该角色包含的权限。

Unified Manager 包括以下预定义的用户角色：

- 操作员

  查看存储系统信息以及 Unified Manager 收集的其他数据，包括历史记录和容量趋势。此角色使存储操作员能够查看、分配、确认、解决事件并为事件添加备注。

- 存储管理员

  在 Unified Manager 中配置存储管理操作。此角色使存储管理员能够配置阈值并创建警报和其他特定于存储管理的选项和策略。

- 应用程序管理员

  配置与存储管理无关的设置。此角色允许管理用户、安全证书、数据库访问和管理选项，包括身份验证、SMTP、网络和 AutoSupport。

  在 Linux 系统上安装 Unified Manager 时，具有应用程序管理员角色的初始用户将自动命名为“umadmin”。

- 集成架构

  此角色允许对 Unified Manager 数据库视图进行只读访问，以便将 Unified Manager 与 OnCommand Workflow Automation （WFA） 集成。

- 报告架构

  此角色可直接从 Unified Manager 数据库以只读方式访问报告和其他数据库视图。可查看的数据库包括：

  - netapp_model_view

- netapp_performance
- ocum
- ocum_report
- ocum_report_birt
- opm
- scalemonitor

了解 Active IQ Unified Manager 中的用户角色和功能

根据您分配的用户角色，您可以确定可以在 Unified Manager 中执行哪些操作。

下表显示了每个用户角色可以执行的功能：

功能	运算符	存储管理员	应用程序管理员	集成架构	报告架构
查看存储系统信息	•	•	•	•	•
查看其他数据，例如历史记录和容量趋势	•	•	•	•	•
查看、分配和解决事件	•	•	•		
查看存储服务对象，例如 SVM 关联和资源池	•	•	•		
查看阈值策略	•	•	•		
管理存储服务对象，例如 SVM 关联和资源池		•	•		
定义警报		•	•		
管理存储管理选项		•	•		
管理存储管理策略		•	•		
管理用户			•		
管理管理选项			•		
定义阈值策略			•		
管理数据库访问			•		
管理与 WFA 的集成并提供对数据库视图的访问				•	
安排并保存报告		•	•		

功能	运算符	存储管理员	应用程序管理员	集成架构	报告架构
从管理操作执行“Fix It” 操作		•	•		
提供对数据库视图的只读访问权限					•

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。