# 管理用户访问

## Active IQ Unified Manager 9.7

NetApp
April 17, 2024

# 目录

# 管理用户访问

您可以创建角色并分配功能，以控制用户对选定集群对象的访问。您可以确定具有访问集群中选定对象所需功能的用户。仅向这些用户提供管理集群对象的访问权限。

## 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，并且根据这些角色的权限，用户可以使用 Unified Manager 管理存储对象和数据，或者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，必须已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（ Identity Provider ， 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 身份验证后，类型为 "`local` " 或 " m维护 " 的用户不允许访问此 UI 。

### 关于此任务

如果从 Windows Active Directory 添加组，则所有直接成员和嵌套子组都可以通过 Unified Manager 的身份验证，除非禁用嵌套子组。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 * 添加 * 。

# 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，并为该用户分配存储管理员权限。

### 开始之前

您必须具有应用程序管理员角色。

### 关于此任务

修改分配给用户的角色时，将在执行以下任一操作时应用所做的更改：

- 用户注销并重新登录到 Unified Manager 。
- 会话已达到 24 小时超时。

### 步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 用户 * 。
2. 在*用户*页面中、选择要编辑其设置的用户、然后单击*编辑*。
3. 在*编辑用户*对话框中、编辑为用户指定的相应设置。
4. 单击 * 保存 * 。

# 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，必须已重新分配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。

# 更改本地用户密码

您可以更改本地用户登录密码，以防止潜在的安全风险。

### 开始之前

您必须以本地用户身份登录。

### 关于此任务

维护用户和远程用户的密码不能使用以下步骤进行更改。要更改远程用户密码，请与密码管理员联系。要更改维护用户密码，请参见 "正在配置 Active IQ Unified Manager"。

### 步骤

1. 登录到 Unified Manager 。
2. 从顶部菜单栏中，单击用户图标，然后单击 * 更改密码 * 。

   如果您是远程用户，则不会显示 * 更改密码 * 选项。

3. 在*更改密码*对话框中、输入当前密码和新密码。
4. 单击 * 保存 * 。

### 完成后

如果 Unified Manager 是在高可用性配置中配置的，则必须更改设置中第二个节点上的密码。两个实例必须具有相同的密码。

# 维护用户执行的操作

维护用户是在 Red Hat Enterprise Linux 或 CentOS 系统上安装 Unified Manager 期间创建的。维护用户名为 "`umadmin` " 用户。维护用户在 Web UI 中具有应用程序管理员角色，该用户可以创建后续用户并为其分配角色。

维护用户或 umadmin 用户也可以访问 Unified Manager 维护控制台。

# 什么是 **RBAC**

RBAC （基于角色的访问控制）可以控制谁有权访问 Active IQ Unified Manager 服务器中

的各种功能和资源。

# 基于角色的访问控制的作用

通过基于角色的访问控制（ Role-Based Access Control ， RBAC ），管理员可以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您创建的管理员帐户。

管理服务器使用 RBAC 来访问用户登录和角色权限。如果您尚未更改管理用户访问的管理服务器默认设置，则无需登录即可查看这些设置。

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，您必须使用应用程序管理员帐户访问权限登录。

# 用户类型的定义

用户类型指定用户持有的帐户类型，其中包括远程用户，远程组，本地用户，数据库用户和维护用户。其中每种类型都有自己的角色，该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。如果 Unified Manager 安装在 Red Hat Enterprise Linux 或 CentOS 系统上，维护用户将获得用户名 "`umadmin.` "

- * 本地用户 *

  访问 Unified Manager 用户界面并根据维护用户或具有应用程序管理员角色的用户提供的角色执行功能。

- * 远程组 *

  使用身份验证服务器上存储的凭据访问 Unified Manager UI 的一组用户。此帐户的名称应与身份验证服务器上存储的组的名称匹配。远程组中的所有用户均可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 *

  使用身份验证服务器上存储的凭据访问 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提供的角色执行功能。

- * 数据库用户 *

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

# 用户角色的定义

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：

- * 运算符 *

  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。通过此角色，存储操作员可以查看，分配，确认，解决和添加事件注释。

- * 存储管理员 *

  在 Unified Manager 中配置存储管理操作。通过此角色，存储管理员可以配置阈值并创建警报和其他存储管理专用选项和策略。

- * 应用程序管理员 *

  配置与存储管理无关的设置。此角色可用于管理用户，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 。

  如果 Unified Manager 安装在 Linux 系统上，则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 *

  通过此角色，可以对 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 *

  通过此角色，可以直接从 Unified Manager 数据库对报告和其他数据库视图进行只读访问。可以查看的数据库包括：

  - netapp_model_view
  - netapp_performance
  - ocum
  - ocum_report
  - ocum_report_BIRT
  - OPM
  - scalemonitor

# Unified Manager 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 中执行的操作。

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权限 | | | | • | |
| 提供对数据库视图的只读访问权限 | | | | | • |

| 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 |
| --- | --- | --- | --- | --- | --- |
| 计划并保存报告 | | • | • | | |

# 用户访问窗口和对话框的问题描述

根据RBAC设置、您可以从"用户"页面添加用户、并为这些用户分配适当的角色以访问和监控集群。

## 用户页面

"用户"页面显示用户和组的列表、并提供名称、用户类型和电子邮件地址等信息。您也可以使用此页面执行添加、编辑、删除和测试用户等任务。

### 命令按钮

命令按钮可用于对选定用户执行以下任务：

- * 添加 * 。

  显示添加用户对话框、在此可以添加本地用户、远程用户、远程组或数据库用户。

  只有在启用并配置了身份验证服务器后、才能添加远程用户或组。

- * 编辑 * 。

  显示编辑用户对话框、在此可以编辑选定用户的设置。

- * 删除 *

  从管理服务器数据库中删除选定用户。

- * 测试 *

  用于验证身份验证服务器中是否存在远程用户或组。

  只有在启用并配置了身份验证服务器后、才能执行此任务。

### 列表视图

列表视图以表格形式显示有关已创建用户的信息。您可以使用列筛选器自定义显示的数据。

- * 名称 *

  显示用户或组的名称。

- * 类型 *

  显示用户的类型：本地用户、远程用户、远程组、数据库用户或维护用户。

- * 电子邮件 *

  显示用户的电子邮件地址。

- * 角色 *

  显示分配给用户的角色类型：操作员、存储管理员、应用程序管理员、集成架构或报告架构。

## 添加用户对话框

您可以创建本地用户或数据库用户、或者添加远程用户或远程组并分配角色、以便这些用户可以使用Unified Manager管理存储对象和数据。

您可以通过填写以下字段来添加用户：

- * 类型 *

  用于指定要创建的用户类型。

- * 名称 *

  用于指定用户可用于登录到Unified Manager的用户名。

- * 密码 *

  用于为指定用户名指定密码。只有在添加本地用户或数据库用户时、才会显示此字段。

- 确认密码

  用于重新输入密码、以确保您在密码字段中输入的内容准确无误。只有在添加本地用户或数据库用户时、才会显示此字段。

- * 电子邮件 *

  用于指定用户的电子邮件地址；指定的电子邮件地址对于用户名必须是唯一的。只有在添加远程用户或本地用户时、才会显示此字段。

- * 角色 *

  用于为用户分配角色并定义用户可执行的活动范围。此角色可以是应用程序管理员、存储管理员、操作员、集成架构或报告架构。

命令按钮

命令按钮可用于执行以下任务：

- * 添加 * 。

  添加用户并关闭添加用户对话框。

- * 取消 *

取消所做的更改并关闭添加用户对话框。

## 编辑用户对话框

通过编辑用户对话框、您可以仅编辑特定设置、具体取决于选定用户。

### 详细信息

"详细信息"区域用于编辑有关选定用户的以下信息：

- * 类型 *

  无法编辑此字段。

- * 名称 *

  无法编辑此字段。

- * 密码 *

  用于在选定用户为数据库用户时编辑密码。

- 确认密码

  用于在选定用户为数据库用户时编辑已确认的密码。

- * 电子邮件 *

  用于编辑选定用户的电子邮件地址。如果选定用户是本地用户、LDAP用户或维护用户、则可以编辑此字段。

- * 角色 *

  用于编辑分配给用户的角色。如果选定用户是本地用户、远程用户或远程组、则可以编辑此字段。

### 命令按钮

命令按钮可用于执行以下任务：

- * 保存 *

  保存更改并关闭编辑用户对话框。

- * 取消 *

  取消所做的更改并关闭编辑用户对话框。