配置 Active IQ Unified Manager

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

目录

配置 Active IQ Unified Manager . . . 1
- 了解有关配置 Active IQ Unified Manager 的信息 . . . 1
- 了解 Active IQ Unified Manager 中的配置顺序 . . . 1
- 访问 Active IQ Unified Manager 中的 Web UI . . . 1
- 执行 Active IQ Unified Manager Web UI 的初始设置 . . . 2
- 向 Active IQ Unified Manager 添加集群 . . . 4
- 配置通知 . . . 6
  - 配置 Active IQ Unified Manager 以发送警报通知 . . . 6
  - 在 Active IQ Unified Manager 中配置事件通知设置 . . . 7
  - 在 Active IQ Unified Manager 中启用远程身份验证 . . . 7
  - 在 Active IQ Unified Manager 中禁用远程身份验证中的嵌套组 . . . 8
  - 在 Active IQ Unified Manager 中设置身份验证服务 . . . 9
  - 向 Active IQ Unified Manager 添加身份验证服务器 . . . 10
  - 测试 Active IQ Unified Manager 中身份验证服务器的配置 . . . 11
  - 在 Active IQ Unified Manager 中添加警报 . . . 12
- 在 Active IQ Unified Manager 中更改本地用户密码 . . . 13
- 在 Active IQ Unified Manager 中设置会话非活动超时 . . . 14
- 使用 Active IQ Unified Manager 中的 CLI 设置会话超时 . . . 14
- 更改 Unified Manager 主机名 . . . 15
  - 更改 Active IQ Unified Manager 虚拟设备主机名 . . . 15
  - 在 Active IQ Unified Manager 中生成 HTTPS 安全证书 . . . 15
  - 重新启动 Active IQ Unified Manager 虚拟机 . . . 17
  - 在 Linux 系统上更改 Active IQ Unified Manager 主机名 . . . 17
- 在 Active IQ Unified Manager 中启用和禁用基于策略的存储管理 . . . 18

配置 Active IQ Unified Manager

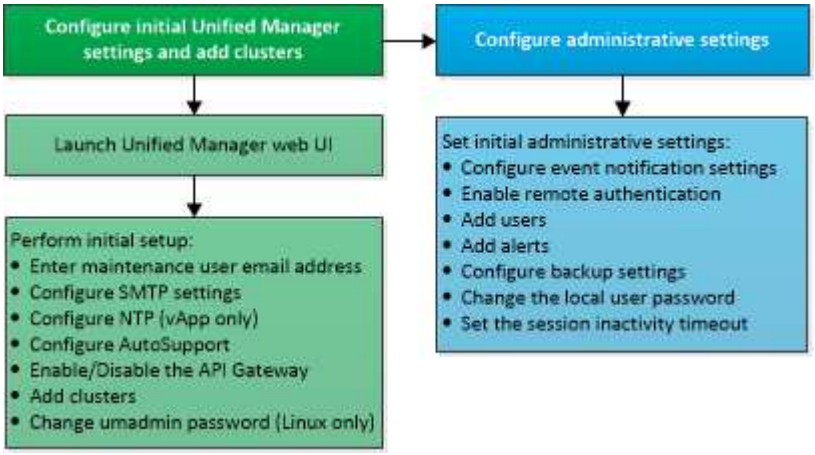
了解有关配置 Active IQ Unified Manager 的信息

安装 Active IQ Unified Manager（以前称为 OnCommand Unified Manager）后，必须完成初始设置（也称为首次体验向导）才能访问 Web UI。然后，您可以执行其他配置任务，例如添加集群、配置远程身份验证、添加用户和添加警报。

完成 Unified Manager 实例的初始设置需要执行本手册中描述的部分步骤。其他步骤是推荐的配置设置，这些设置有助于在新实例上进行设置，或者在开始定期监控 ONTAP 系统之前最好能有所了解。

了解 Active IQ Unified Manager 中的配置顺序

配置工作流描述了在使用 Unified Manager 之前必须执行的任务。



访问 Active IQ Unified Manager 中的 Web UI

安装 Unified Manager 后，您可以访问 Web UI 以设置 Unified Manager，以便开始监控 ONTAP 系统。

开始之前

- 如果这是您第一次访问 Web UI，则必须以维护用户（或 Linux 安装的 umadmin 用户）身份登录。
- 如果您计划允许用户使用短名称而不是使用完全限定的域名（FQDN）或 IP 地址访问 Unified Manager，则您的网络配置必须将此短名称解析为有效的 FQDN。
- 如果服务器使用自签名数字证书，则浏览器可能会显示警告，指示该证书不受信任。您可以确认风险并继续访问，也可以安装用于服务器身份验证的证书颁发机构（CA）签名的数字证书。

步骤

1. 请使用安装结束时显示的 URL 从浏览器启动 Unified Manager Web UI。该 URL 是 Unified Manager 服务器的 IP 地址或完全限定域名（FQDN）。

   链接的格式如下： `https://URL`。

2. 使用维护用户凭据登录到 Unified Manager Web UI。

> 如果您在一小时内连续三次尝试登录 Web UI 失败，您将被系统锁定，并且需要联系您的系统管理员。这仅适用于本地用户。

执行 **Active IQ Unified Manager Web UI** 的初始设置

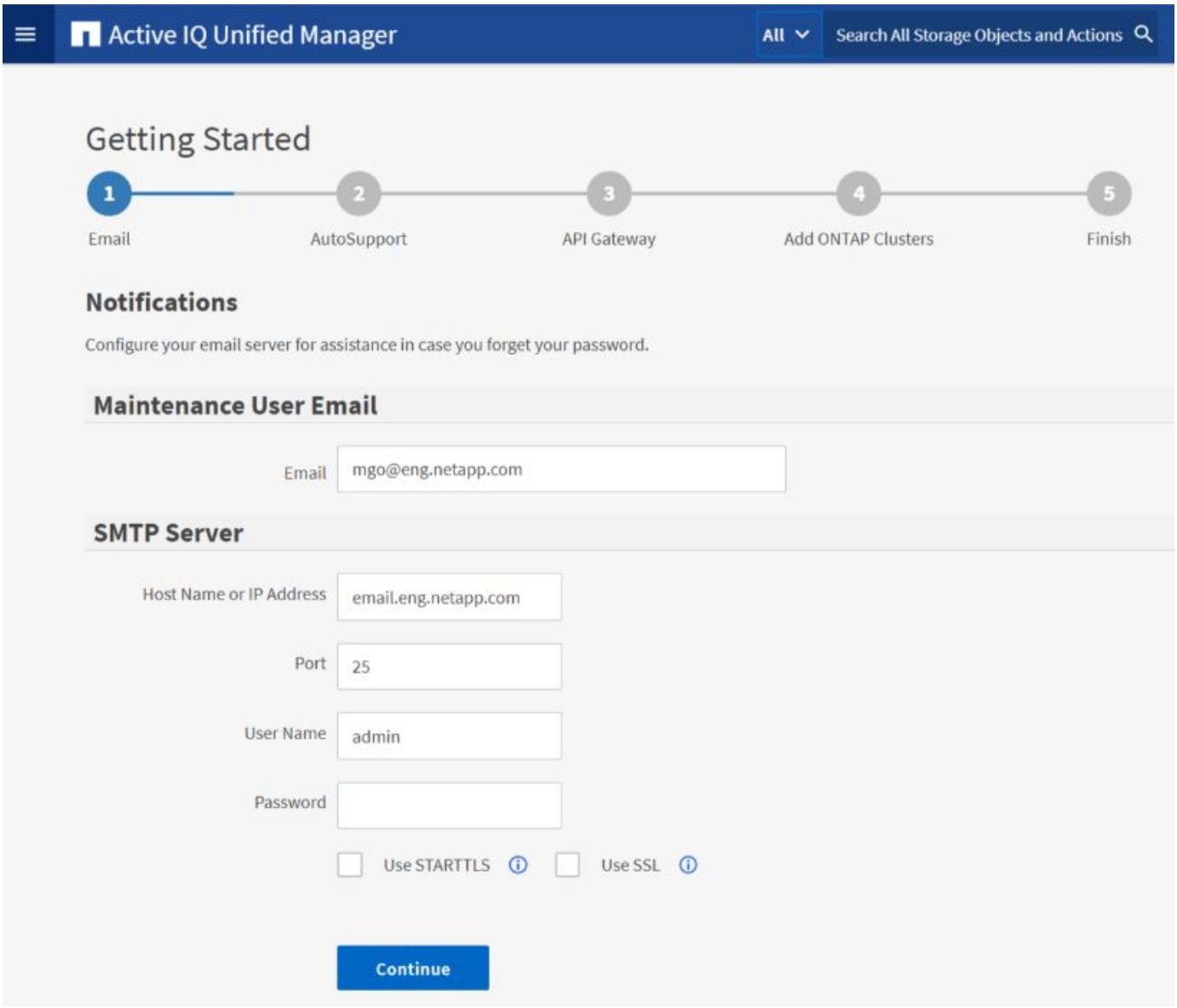
要使用 Unified Manager，必须首先配置初始设置选项，包括 NTP 服务器、维护用户电子邮件地址、SMTP 服务器主机和添加 ONTAP 群集。

开始之前

您必须已执行以下操作：

- 使用安装后提供的 URL 启动 Unified Manager Web UI
- 使用在安装期间创建的维护用户名和密码（对于 Linux 安装，为 umadmin 用户）登录

仅当您首次访问 Web UI 时，才会显示 Active IQ Unified ManagerGetting Started 页面。下面的页面来自 VMware 上的安装。



如果稍后要更改其中任何选项，您可以从 Unified Manager 左侧导航窗格的常规选项中进行选择。请注意，NTP 设置仅适用于 VMware 安装，稍后可以使用 Unified Manager 维护控制台进行更改。

步骤

1. 在“Active IQ Unified Manager 初始设置”页面中，输入维护用户电子邮件地址、SMTP 服务器主机名和任何其他 SMTP 选项，以及 NTP 服务器（仅限 VMware 安装）。然后单击 继续。

   如果您选择了 使用 **STARTTLS** 或 使用 **SSL** 选项，则单击 继续 按钮后会显示证书页面。验证证书详细信息并接受证书以继续进行 Web UI 的初始设置。

2. 在 AutoSupport 页面中，单击 **Agree and Continue** 以启用从 Unified Manager 向 NetAppActive IQ 发送 AutoSupport 消息的功能。

   如果需要指定代理来提供 Internet 访问以发送 AutoSupport 内容，或者如果要禁用 AutoSupport，请使用 Web UI 中的 **General** > **AutoSupport** 选项。

3. 在 Red Hat 系统上，将 umadmin 用户密码从默认的“`admin`”字符串更改为个性化字符串。

4. 在 Set up API Gateway 页面中，选择是否要使用 API Gateway 功能，该功能允许 Active IQ Unified Manager 使用 ONTAP REST API 管理您计划监控的 ONTAP 集群。然后单击 **Continue**。

   您可以稍后在 Web UI 中从 常规 > 功能设置 > **API** 网关 启用或禁用此设置。有关 API 的详细信息，请参见 "Active IQ Unified Manager REST API 入门"。

5. 添加您希望 Unified Manager 管理的集群，然后单击 下一步。对于您计划管理的每个集群，您必须具有主机名或集群管理 IP 地址（IPv4 或 IPv6）以及用户名和密码凭据——用户必须具有“admin”角色。

   此步骤为可选步骤。您可以稍后在 Web UI 中从 存储管理 > 集群设置 添加集群。

6. 在“摘要”页面中，验证所有设置是否正确，然后单击 完成。

“入门”页面关闭并显示“Unified Manager 仪表板”页面。

向 Active IQ Unified Manager 添加集群

您可以将集群添加到 Active IQ Unified Manager 以便可以监视该集群。这包括能够获取集群信息，例如集群的运行状况、容量、性能和配置，以便您可以查找并解决可能发生的任何问题。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须具有下列信息：
  - Unified Manager 支持本地 ONTAP 集群、ONTAP Select、Cloud Volumes ONTAP。
  - 主机名或集群管理 IP 地址

    主机名是 FQDN 或 Unified Manager 用来连接集群的简称。主机名必须解析为集群管理 IP 地址。

    集群管理 IP 地址必须是管理存储虚拟机（SVM）的集群管理 LIF。如果使用节点管理 LIF，则操作会失败。

  - 此集群必须运行 ONTAP 9.1 或更高版本的软件。
  - ONTAP 管理员用户名和密码

    此帐户必须具有 *admin* 角色，应用程序访问权限设置为 *ontapi*、*amqp*、*console* 和 *http*。

  - 使用 HTTPS 协议连接到集群的端口号（通常为端口 443）
  - 您拥有所需的证书：

    SSL (HTTPS) 证书：此证书由 Unified Manager 拥有。全新安装 Unified Manager 时，会生成默认的自签名 SSL (HTTPS) 证书。NetApp 建议将其升级为 CA 签名证书，以获得更好的安全性。如果服务器证书过期，您应重新生成该证书并重新启动 Unified Manager，以便服务采用新证书。有关重新生成 SSL 证书的详细信息，请参见 "生成 HTTPS 安全证书"。

    EMS 证书：此证书归 Unified Manager 所有。它在对从 ONTAP 接收的 EMS 通知进行身份验证时使用。

双向 **TLS** 通信证书：在 Unified Manager 和 ONTAP 之间的双向 TLS 通信期间使用。系统会根据 ONTAP 版本为集群启用基于证书的身份验证。如果集群运行的 ONTAP 版本低于 9.5，则不会启用基于证书的身份验证。

如果您要更新早期版本的 Unified Manager，则不会为集群自动启用基于证书的身份验证。但是，您可以通过修改并保存集群详细信息来启用它。如果证书过期，您应重新生成证书以整合新证书。有关查看和重新生成证书的详细信息，请参见"编辑集群"。

- 您可以从 Web UI 添加集群，并自动启用基于证书的身份验证。
- 您可以通过 Unified Manager CLI 添加集群，默认情况下不会启用基于证书的身份验证。如果使用 Unified Manager CLI 添加集群，则需要使用 Unified Manager UI 编辑集群。您可以查看 "支持的 Unified Manager CLI 命令" 了解如何使用 Unified Manager CLI 添加集群。
- 如果为集群启用了基于证书的身份验证，并且您从服务器获取 Unified Manager 的备份并还原到主机名或 IP 地址已更改的另一台 Unified Manager 服务器，则对集群的监控可能会失败。为避免失败，请编辑并保存集群详细信息。有关编辑集群详细信息的更多信息，请参见 "编辑集群"。

+ 集群证书：此证书归 ONTAP 所有。您无法将证书已过期的集群添加到 Unified Manager，如果证书已过期，则应在添加集群之前重新生成该证书。有关证书生成的信息，请参见知识库（KB）文章 "如何在 System Manager 用户界面中续订 ONTAP 自签名证书"。

- 您必须在 Unified Manager 服务器上有足够的空间。当数据库目录中超过 90% 的空间已被占用时，您将无法向服务器添加集群。

对于 MetroCluster 配置，必须同时添加本地和远程集群，并且必须正确配置集群。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 集群设置。
2. 在“集群设置”页面上，单击*添加*。
3. 在添加群集对话框中，指定所需的值，例如群集的主机名或 IP 地址、用户名、密码和端口号。

   您可以将集群管理 IP 地址从 IPv6 更改为 IPv4，或者从 IPv4 更改为 IPv6。下一个监控周期完成后，新的 IP 地址将反映在集群网格和集群配置页面中。

4. 单击*提交*。
5. 在 Authorize Host 对话框中，单击 **View Certificate** 可查看集群的证书信息。
6. 单击 **Yes**。

   保存集群详细信息后，可以查看集群的 Mutual TLS 通信证书。

   如果未启用基于证书的身份验证，Unified Manager 仅在最初添加集群时检查证书。Unified Manager 不会检查对 ONTAP 的每次 API 调用的证书。

发现新集群的所有对象后，Unified Manager 将开始收集前 15 天的历史性能数据。这些统计数据通过数据连续性收集功能进行收集。此功能可在集群添加后立即为您提供超过两周的集群性能信息。数据连续性收集周期完成后，将默认每五分钟收集一次实时集群性能数据。

由于收集 15 天的性能数据是 CPU 密集型的，因此建议您错开添加新集群，以便数据连续性收集

轮询不会同时在太多集群上运行。此外，如果您在数据连续性收集期间重新启动 Unified Manager，则收集将暂停，您将看到缺失时间范围内的性能图表中的缺口。

如果收到无法添加集群的错误消息，请检查两个系统上的时钟是否未同步，以及 Unified Manager HTTPS 证书开始日期是否晚于集群上的日期。您必须确保时钟使用 NTP 或类似服务进行同步。

相关信息

"安装 CA 签名并返回的 HTTPS 证书"

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*。

如果选择.....	操作
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。
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**。

在 Active IQ Unified Manager 中更改本地用户密码

您可以更改本地用户登录密码，以避免出现可能的安全风险。

开始之前

必须以本地用户身份登录。

无法使用这些步骤更改维护用户和远程用户的密码。要更改远程用户密码，请联系您的密码管理员。要更改维护用户密码，请参阅 "使用维护控制台"。

步骤

1. 登录到 Unified Manager。
2. 在顶部菜单栏中，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 **Save**。

如果在高可用性配置中配置了 Unified Manager，则必须在设置的第二个节点上更改密码。两个实例必须具有相同的密码。

在 Active IQ Unified Manager 中设置会话非活动超时

您可以为 Unified Manager 指定非活动超时值，以便在一段时间非活动后自动终止会话。默认情况下，超时设置为 4,320 分钟（72 小时）。

开始之前

您必须具有应用程序管理员角色。

此设置会影响所有登录的用户会话。

如果已启用安全断言标记语言（SAML）身份验证，则此选项不可用。

步骤

1. 在左侧导航窗格中，单击*常规* > 功能设置。
2. 在*功能设置*页面中，通过选择以下选项之一指定非活动超时：

目的	操作
未设置超时，因此会话永远不会自动关闭	在*非活动超时*面板中，将滑块按钮向左移动（关闭），然后单击*应用*。
设置特定的分钟数作为超时值	在*非活动超时*面板中，将滑块按钮向右移动（开启），以分钟为单位指定非活动超时值，然后单击*应用*。

使用 Active IQ Unified Manager 中的 CLI 设置会话超时

您可以使用 CLI 为 Unified Manager 设置最大会话超时值，以便在一段时间后自动终止会话。默认情况下，您的会话超时设置为最大值，即 4,320 分钟（72 小时）。这意味着您的会话将在 72 小时后自动结束，即使您已登录并正在积极使用 Unified Manager 也是如此。

关于此任务

您必须具有应用程序管理员角色。

会话超时设置会影响所有登录的用户会话。

步骤

1. 输入 `um cli login`命令登录到 Unified Manager CLI。使用有效的用户名和密码进行身份验证。
2. 输入 `um option set max.session.timeout.value=<in mins>`命令以修改会话超时值。

更改 Unified Manager 主机名

更改 Active IQ Unified Manager 虚拟设备主机名

首次部署 Unified Manager 虚拟设备时，将为网络主机分配一个名称。可以在部署后更改主机名。如果更改主机名，则还必须重新生成 HTTPS 证书。

开始之前

您必须以维护用户身份登录到 Unified Manager，或者拥有应用程序管理员角色，才能执行这些任务。

您可以使用主机名（或主机 IP 地址）访问 Unified Manager Web UI。如果在部署期间为网络配置了静态 IP 地址，则会为网络主机指定名称。如果使用 DHCP 配置网络，则主机名应取自 DNS。如果未正确配置 DHCP 或 DNS，则会自动分配主机名“`Unified Manager`”，并将其与安全证书相关联。

无论主机名是如何分配的，如果更改主机名并打算使用新主机名访问 Unified Manager Web UI，则必须生成新的安全证书。

如果使用服务器的 IP 地址而不是主机名访问 Web UI，那么在更改主机名时，无需生成新证书。但是，最佳做法是更新证书，使证书中的主机名与实际主机名相匹配。

如果在 Unified Manager 中更改主机名，则必须在 OnCommand Workflow Automation (WFA) 中手动更新主机名。WFA 中的主机名不会自动更新。

在重新启动 Unified Manager 虚拟机之前，新证书不会生效。

步骤

1. 生成 HTTPS 安全证书

   如果要使用新主机名访问 Unified Manager Web UI，则必须重新生成 HTTPS 证书以将其与新主机名关联。

2. 重新启动 Unified Manager 虚拟机

   重新生成 HTTPS 证书后，必须重新启动 Unified Manager 虚拟机。

在 Active IQ Unified Manager 中生成 HTTPS 安全证书

首次安装 Active IQ Unified Manager 时，将安装默认 HTTPS 证书。您可能会生成一个新的 HTTPS 安全证书来替换现有证书。

开始之前

您必须具有应用程序管理员角色。

重新生成证书的原因可能有多种，例如希望为可分辨名称 （DN） 设置更好的值、希望使用更大的密钥大小、更长的有效期，或者当前证书已过期。

如果无权访问 Unified Manager Web UI，则可以使用维护控制台使用相同的值重新生成 HTTPS 证书。在重新生成证书时，您可以定义密钥大小和密钥的有效期。如果使用维护控制台中的 `Reset Server Certificate`选项，则会创建一个有效期为 397 天的新 HTTPS 证书。此证书将具有大小为 2048 位的 RSA 密钥。

步骤

1. 在左侧导航窗格中，单击 常规 > **HTTPS** 证书。
2. 单击 重新生成 **HTTPS** 证书。

   此时将显示重新生成 HTTPS 证书对话框。

3. 根据您要生成证书的方式选择以下选项之一：

目的	操作
使用当前值重新生成证书	单击*使用当前证书属性重新生成*选项。
使用其他值生成证书	单击*更新当前证书属性*选项。 如果不输入新值，Common Name 和 Alternative Names 字段将使用现有证书中的值。“Common Name”应设置为主机的 FQDN。其他字段不需要值，但如果希望在证书中填充这些值，则可以输入值，例如 EMAIL、COMPANY、DEPARTMENT、City 、State 和 Country 的值。您还可以从可用的 KEY SIZE（密钥算法为“RSA”。）和 VALIDITY PERIOD 中进行选择。 • 密钥大小的允许值为 2048、3072`和 `4096。 • 有效期为最少 1 天至最多 36500 天。 即使允许 36500 天的有效期，也建议您使用不超过 397 天或 13 个月的有效期。因为如果您选择了超过 397 天的有效期，并计划导出此证书的 CSR 并由知名的 CA 签名，则 CA 退还给您的签名证书的有效期将缩短至 397 天。 • 如果要从证书的 Alternative Names 字段中删除本地标识信息，可以选中“排除本地标识信息（例如 localhost）”复选框。选中此复选框时，Alternative Names 字段中将仅使用您在该字段中输入的内容。如果留空，生成的证书将完全没有 Alternative Names 字段。

4. 单击*是*以重新生成证书。
5. 重新启动 Unified Manager 服务器以使新证书生效。
6. 通过查看 HTTPS 证书，可验证新证书的信息。

重新启动 **Active IQ Unified Manager** 虚拟机

您可以从 Unified Manager 的维护控制台重新启动虚拟机。在生成新的安全证书后，或者如果虚拟机出现问题，您必须重新启动。

开始之前

已打开虚拟设备的电源。

您以维护用户身份登录到维护控制台。

您还可以使用 **Restart Guest** 选项从 vSphere 重新启动虚拟机。有关详细信息，请参见 VMware 文档。

步骤

1. 访问维护控制台。
2. 选择*系统配置* > 重启虚拟机。

在 **Linux** 系统上更改 **Active IQ Unified Manager** 主机名

在某些时候，您可能需要更改已安装 Unified Manager 的 Red Hat Enterprise Linux 计算机的主机名。例如，您可能希望在列出 Linux 计算机时按类型、工作组或受监视的集群组重命名主机，以便更轻松地识别 Unified Manager 服务器。

开始之前

您必须具有对安装了 Unified Manager 的 Linux 系统的 root 用户访问权限。

您可以使用主机名（或主机 IP 地址）访问 Unified Manager web UI。如果在部署期间为网络配置了静态 IP 地址，则会为网络主机指定一个名称。如果使用 DHCP 配置网络，则应从 DNS 服务器获取主机名。

无论主机名是如何分配的，如果更改主机名并打算使用新主机名来访问 Unified Manager Web UI，则必须生成新的安全证书。

如果使用服务器的 IP 地址而不是主机名访问 web UI，则在更改主机名时无需生成新证书。但是，最佳做法是更新证书，以便证书中的主机名与实际主机名相匹配。重新启动 Linux 计算机之前，新证书不会生效。

如果在 Unified Manager 中更改主机名，则必须在 OnCommand Workflow Automation (WFA) 中手动更新主机名。WFA 中的主机名不会自动更新。

步骤

1. 以 root 用户身份登录到要修改的 Unified Manager 系统。
2. 通过输入以下命令停止 Unified Manager 软件和相关的 MySQL 软件：

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. 使用 Linux `hostnamectl` 命令更改主机名：

   ```
   hostnamectl set-hostname new_FQDN

   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. 重新生成服务器的 HTTPS 证书：

   ```
   /opt/netapp/essentials/bin/cert.sh create
   ```

5. 重新启动网络服务：

   ```
   systemctl restart NetworkManager.service
   ```

6. 服务重新启动后，验证新主机名是否能够 ping 通自己：

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   此命令应返回之前为原始主机名设置的相同 IP 地址。

7. 完成并验证主机名更改后，通过输入以下命令重新启动 Unified Manager：

   ```
   systemctl start mysqld ocie ocieau
   ```

在 Active IQ Unified Manager 中启用和禁用基于策略的存储管理

从 Unified Manager 9.7 开始，您可以在 ONTAP 集群上配置存储工作负载（卷和 LUN），并根据分配的性能服务级别管理这些工作负载。此功能类似于在 ONTAP System Manager 中创建工作负载并附加 QoS 策略，但使用 Unified Manager 应用时，您可以在 Unified Manager 实例正在监控的所有集群中配置和管理工作负载。

您必须具有应用程序管理员角色。

默认情况下，此选项处于启用状态，但如果您不想使用 Unified Manager 配置和管理工作负载，则可以将其禁用。

启用后，此选项将在用户界面中提供许多新项目：

新内容	位置
配置新工作负载的页面	可从 **Common Tasks** > **Provisioning** 获得
用于创建性能服务级别策略的页面	可从 设置 > 策略 > 性能服务级别 中获取
用于创建性能存储效率策略的页面	可从*设置* > 策略 > 存储效率
描述当前工作负载性能和工作负载 IOPS 的面板	可从信息板获得

有关这些页面和此功能的更多信息，请参见产品中的联机帮助。

步骤

1. 在左侧导航窗格中，单击*常规* > 功能设置。
2. 在*功能设置*页面中，通过选择以下选项之一禁用或启用基于策略的存储管理：

目的	操作
禁用基于策略的存储管理	在*基于策略的存储管理*面板中，向左移动滑块按钮。
启用基于策略的存储管理	在*基于策略的存储管理*面板中，将滑块按钮向右移动。

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。