正在配置 Active IQ Unified Manager

Active IQ Unified Manager 9.12

NetApp
December 18, 2023

目录

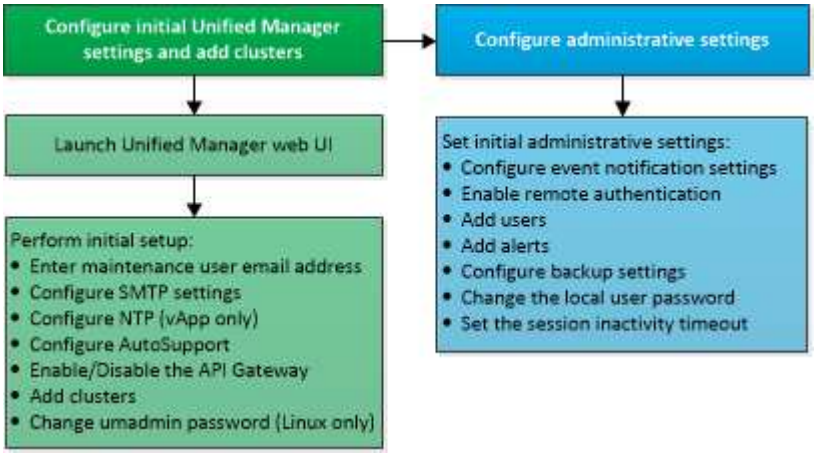
正在配置 Active IQ Unified Manager

安装 Active IQ Unified Manager （以前称为 OnCommand 统一管理器）后，您必须完成初始设置（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。

要完成 Unified Manager 实例的初始设置，需要执行本手册中所述的某些过程。其他过程包括建议的配置设置，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 系统之前最好了解这些设置。

配置顺序概述

配置工作流介绍了在使用 Unified Manager 之前必须执行的任务。



访问 Unified Manager Web UI

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

- 您需要的内容 *
- 如果这是首次访问 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完全限定域名（ FQDN ）或 IP 地址访问 Unified Manager ，则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一条警告，指示此证书不可信。您可以确认继续访问的风险，也可以安装证书颁发机构（ CA ）签名的数字证书以进行服务器身份验证。

步骤

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

   此链接的格式如下： `https://URL`。

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

如果您连续三次尝试在一小时内登录到 Web UI 失败，则系统将锁定您，并需要联系您的系统管理员。这仅适用于本地用户。

执行 Unified Manager Web UI 的初始设置

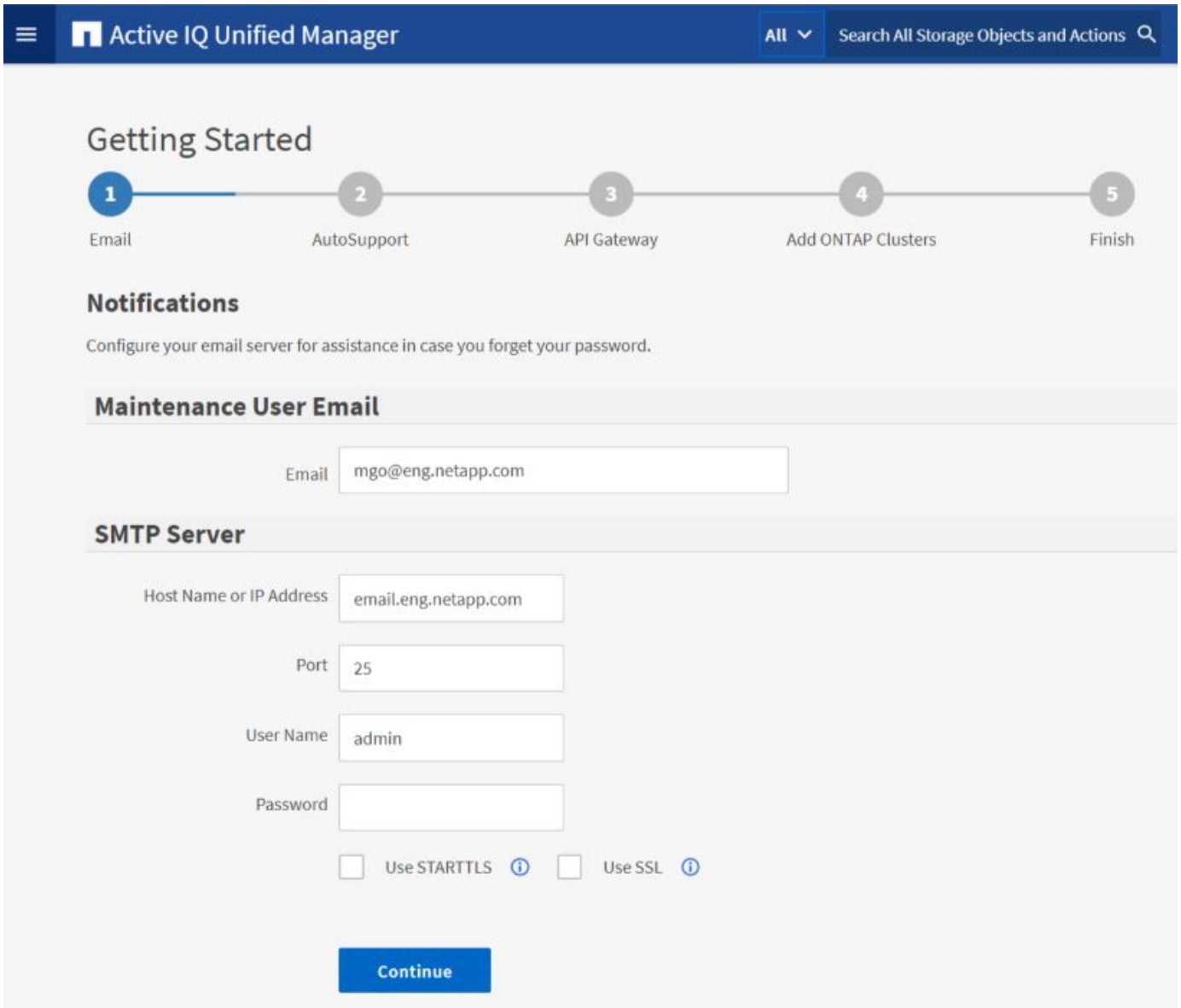
要使用 Unified Manager ，必须先配置初始设置选项，包括 NTP 服务器，维护用户电子邮件地址， SMTP 服务器主机以及添加 ONTAP 集群。

- 您需要的内容 *

您必须已执行以下操作：

- 已使用安装后提供的 URL 启动 Unified Manager Web UI
- 使用安装期间创建的维护用户名和密码（适用于 Linux 安装的 umadmin 用户）登录

只有在首次访问 Web UI 时，才会显示 Active IQ Unified Manager 的 " 设置开始 " 页面。以下页面来自 VMware 上的安装。



如果稍后要更改其中任何一个选项，您可以从 Unified Manager 左侧导航窗格中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 * 。

   > 如果选择了*使用STARTT*或*使用SSL*选项、则在单击*继续*按钮后、将显示证书页面。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 * 同意并继续 * 以启用从 Unified Manager 向 NetAppActive IQ 发送 AutoSupport 消息的功能。

   如果您需要指定一个代理来提供 Internet 访问以发送 AutoSupport 内容，或者要禁用 AutoSupport ，请使用 Web UI 中的 * 常规 * > * AutoSupport * 选项。

3. 在Red Hat和CentOS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. 在设置 API 网关页面中，选择是否要使用 API 网关功能，以便 Unified Manager 能够管理计划使用 ONTAP REST API 监控的 ONTAP 集群。然后单击 * 继续 * 。

   您可以稍后在 Web UI 中通过 * 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。稍后可以从 * 存储管理 * > * 集群设置 * 在 Web UI 中添加集群。

6. 在摘要页面中，验证所有设置是否正确，然后单击 * 完成 * 。

此时将关闭 Getting Started 页面，并显示 Unified Manager Dashboard 页面。

添加集群

您可以将集群添加到 Active IQ Unified Manager 中，以便监控集群。这包括能够获取集群的运行状况，容量，性能和配置等集群信息，以便您可以发现并解决可能发生的任何问题。

- 您需要的内容 *
- 您必须具有应用程序管理员或存储管理员角色。
- 您必须具有以下信息：
  - 主机名或集群管理 IP 地址

    主机名是 Unified Manager 用于连接到集群的 FQDN 或简称。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 Storage Virtual Machine （ SVM ）的集群管理 LIF 。如果使用节点管理 LIF ，则操作将失败。

  - 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、并且应用程序访问权限设置为_ontapi_、*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。Unified Manager在添加集群时安装安全证书：

    服务器证书：此证书属于Unified Manager。全新安装的Unified Manager将生成默认的自签名SSL (HTTPS)证书。NetApp建议您将其升级到CA签名证书、以提高安全性。如果服务器证书到期、您应重新生成该证书并重新启动Unified Manager、以便服务加入新证书。有关重新生成SSL证书的详细信息、请参见 "生成 HTTPS 安全证书"。

    用于相互**TLS**通信的证书：在Unified Manager和ONTAP 之间进行相互TLS通信期间使用。系统将根据ONTAP 版本为集群启用基于证书的身份验证。如果运行ONTAP 版本的集群低于9.5、则不会启用基于证书的身份验证。

    如果要将旧版本的Unified Manager更新到Unified Manager 9.12、则集群不会自动启用基于证书的身份

验证。但是、您可以通过修改和保存集群详细信息来启用此功能。如果证书过期、则应重新生成证书以加入新证书。有关查看和重新生成证书的详细信息、请参见 "编辑集群"。

> ◦ 如果您从Web UI添加集群、则基于证书的身份验证将自动启用。如果从维护控制台添加集群、则不会启用基于证书的身份验证。
>
> ◦ 如果为集群启用了基于证书的身份验证、并且您从服务器备份Unified Manager并还原到另一个Unified Manager服务器、其中主机名或IP地址发生了更改、则监控集群可能会失败。要避免失败、请编辑并保存集群详细信息。有关编辑集群详细信息的详细信息、请参见 "编辑集群"。

+ 客户端证书：在对从ONTAP 收到的EMS消息进行身份验证期间使用。此证书属于ONTAP 、在将ONTAP 集群添加到Unified Manager时需要此证书。您不能将证书已过期的集群添加到 Unified Manager 中，如果客户端证书已过期，则应在添加集群之前重新生成该集群。但是，如果已添加且 Unified Manager 正在使用的集群的此证书到期，则 EMS 消息传送功能将在证书过期后继续运行。有关生成证书的信息、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"。

- Unified Manager 服务器上必须有足够的空间。如果数据库目录中已占用的空间超过 90% ，则系统将阻止您向服务器添加集群。

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

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 集群设置 * 。
2. 在 Cluster Setup 页面上，单击 * 添加 * 。
3. 在添加集群对话框中，指定所需的值，例如集群的主机名或 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 或从 IPv4 更改为 IPv6 。下一个监控周期完成后，新 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. 在授权主机对话框中，单击 * 查看证书 * 以查看有关集群的证书信息。
6. 单击 * 是 * 。

   在Unified Manager 9.12中、保存集群详细信息后、您可以查看集群的相互TLS通信证书。

   如果未启用基于证书的身份验证、则Unified Manager仅在首次添加集群时才会检查证书。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 将开始收集过去 15 天的历史性能数据。这些统计信息是使用数据连续性收集功能收集的。添加集群后，此功能会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，系统会默认每五分钟收集一次实时集群性能数据。

> 由于收集 15 天的性能数据需要占用大量 CPU 资源，因此建议您错开添加新集群的时间，以便不会在太多集群上同时运行数据连续性收集轮询。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，并且性能图表中会显示缺少的时间范围。

> 如果您收到一条错误消息，指出无法添加集群，请检查两个系统上的时钟是否未同步，以及 Unified Manager HTTPS 证书的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 Unified Manager 以发送警报通知

您可以将 Unified Manager 配置为发送通知，以便就环境中的事件向您发出警报。在发送通知之前，您必须配置其他几个 Unified Manager 选项。

- 您需要的内容 *

您必须具有应用程序管理员角色。

在部署 Unified Manager 并完成初始配置后，您应考虑将环境配置为触发警报，并根据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"。

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

2. "启用远程身份验证"。

   如果您希望远程 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"。

   您可以添加多种不同类型的本地或远程用户并分配特定角色。创建警报时，您需要分配一个用户以接收警报通知。

5. "添加警报"。

   添加用于发送通知的电子邮件地址，添加用于接收通知的用户，配置网络设置以及配置环境所需的 SMTP 和 SNMP 选项后，您可以分配警报。

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，警报通知可以通

过电子邮件或 SNMP 陷阱发送。

- 您需要的内容 *

您必须具有以下信息：

- 发送警报通知的电子邮件地址

  电子邮件地址将显示在已发送警报通知的 "`from` " 字段中。如果由于任何原因无法传送此电子邮件，则此电子邮件地址也会用作无法传送的邮件的收件人。

- 用于访问服务器的 SMTP 服务器主机名以及用户名和密码
- 要接收 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，社区和其他所需的 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，列表中所有主机的所有其他 SNMP 设置（例如版本和出站陷阱端口）都必须相同。

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、配置相应的设置。
   - 注： *
     - 如果 " 发件人地址 " 已预先填充地址 "+ActiveIQUnifiedManager@localhost.com +" ，则应将其更改为实际有效的电子邮件地址，以确保所有电子邮件通知均已成功传送。
     - 如果无法解析 SMTP 服务器的主机名，您可以指定 SMTP 服务器的 IP 地址（ IPv4 或 IPv6 ），而不是主机名。
3. 单击 * 保存 * 。
4. 如果选择了*使用STARTT*或*使用SSL*选项、则在单击*保存*按钮后、将显示证书页面。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STARTT*或*使用SSL*复选框、保存通知设置、然后再次选中*使用STARTT*或*使用SSL*复选框以查看新证书。

启用远程身份验证

您可以启用远程身份验证，以便 Unified Manager 服务器可以与身份验证服务器进行通信。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。

- 您需要的内容 *

您必须具有应用程序管理员角色。

> Unified Manager 服务器必须直接与身份验证服务器连接。您必须禁用任何本地 LDAP 客户端，例如 SSSD （系统安全服务守护进程）或 NSLCD （名称服务 LDAP 缓存守护进程）。

您可以使用 Open LDAP 或 Active Directory 启用远程身份验证。如果禁用了远程身份验证，则远程用户无法访问 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，使用 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 …* 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。

身份验证类型 …	输入以下信息 …
Active Directory	• 身份验证服务器管理员名称采用以下格式之一： ◦ `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（采用适当的 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 * 保存 * 。

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）可以远程向 Unified Manager 进行身份验证。如果要缩短 Active Directory 身份验证响应时间，可以禁用嵌套组。

- 您需要的内容 *
- 您必须具有应用程序管理员角色。

- 只有在使用 Active Directory 时，禁用嵌套组才适用。

在 Unified Manager 中禁用对嵌套组的支持可能会缩短身份验证时间。如果禁用嵌套组支持，并且将远程组添加到 Unified Manager 中，则各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 * 保存 * 。

设置身份验证服务

通过身份验证服务，可以先对身份验证服务器中的远程用户或远程组进行身份验证，然后再为其提供对 Unified Manager 的访问权限。您可以使用预定义的身份验证服务（例如 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。

- 您需要的内容 *
- 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. 选择以下身份验证服务之一：

如果选择	然后执行此操作 ...
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	然后执行此操作 ...
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，组成员资格，用户组和成员属性。

> 如果要修改身份验证服务，必须删除任何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 * 保存 * 。

正在添加身份验证服务器

您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 。

- 您需要的内容 *
- 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
- 您必须已启用远程身份验证并配置身份验证服务，以便管理服务器能够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属于高可用性（ HA ）对（使用同一数据库），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：

如果您要 ...	然后执行此操作 ...
启用它	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. 在授权主机对话框中，单击查看证书。 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 * 是 * 。 启用 * 使用安全连接身份验证 * 选项后， 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，使用端口号 389 进行非安全通信。
请将其禁用	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 * 添加 * 。

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您可以在添加的身份验证服务器中对用户进行身份验证。

测试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这些服务器进行通信。您可以通过从身份验证服务器中搜索远程用户或远程组并使用已配置的设置对其进行身份验证来验证配置。

- 您需要的内容 *
- 您必须已启用远程身份验证并配置身份验证服务，以便 Unified Manager 服务器能够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 ，并且您要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. 在测试用户对话框中，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 * 测试 * 。

   如果要对远程组进行身份验证，则不能输入密码。

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。

- 您需要的内容 *
- 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。
- 您必须了解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，则必须已使用脚本页面将脚本添加到 Unified Manager 中。
- 您必须具有应用程序管理员或存储管理员角色。

除了从 "Alert Setup" 页面创建警报之外，您还可以在收到事件后直接从 "Event Details" 页面创建警报，如下所述。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 警报设置 * 。
2. 在 "Alert Setup" 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，如果您从用户页面修改了选定用户的电子邮件地址，则不会为选定用户更新修改后的电子邮件地址。

您也可以选择通过 SNMP 陷阱通知用户。

7. 单击 * 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：

步骤

1. 单击 * 名称 * ，然后在 * 警报名称 * 字段中输入 * 运行状况测试 * 。
2. 单击 * 资源 * ，然后在包括选项卡中，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. 选择 * +[All Volumes whose name contains 'abc']从 "Available Resources" 区域中选择 +* ，然后将其移动到 "Selected Resources" 区域。
   c. 单击 * 排除 * ，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 * 所有严重事件 * ，然后将其移动到选定事件区域。
5. 单击 * 操作 * ，然后在警报这些用户字段中输入 * sample@domain.com * 。
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 Select Script to Execute 菜单中，选择 * 测试 * 脚本。
8. 单击 * 保存 * 。

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。

- 您需要的内容 *

您必须以本地用户身份登录。

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 "使用维护控制台"。

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 * 。

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。

设置会话非活动超时

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

- 您需要的内容 *

您必须具有应用程序管理员角色。

此设置会影响所有已登录的用户会话。

> 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，选择以下选项之一以指定非活动超时：

如果您要 ...	然后执行此操作 ...
未设置超时，会话永远不会自动关闭	在 * 非活动超时 * 面板中，将滑块按钮移至左侧（关闭），然后单击 * 应用 * 。
将特定分钟数设置为超时值	在 * 非活动超时 * 面板中，将滑块按钮移至右侧（打开），以分钟为单位指定非活动超时值，然后单击 * 应用 * 。

更改 Unified Manager 主机名

有时，您可能需要更改已安装 Unified Manager 的系统的主机名。例如，您可能希望重命名主机，以便按类型，工作组或受监控集群组更轻松地识别 Unified Manager 服务器。

根据 Unified Manager 是在 VMware ESXi 服务器， Red Hat 或 CentOS Linux 服务器上还是在 Microsoft Windows 服务器上运行，更改主机名所需的步骤会有所不同。

更改 **Unified Manager** 虚拟设备主机名

首次部署 Unified Manager 虚拟设备时，系统会为网络主机分配一个名称。您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。

- 您需要的内容 *

要执行这些任务，您必须以维护用户身份登录到 Unified Manager 或分配有应用程序管理员角色。

您可以使用主机名（或主机 IP 地址）访问 Unified Manager Web UI 。如果您在部署期间为网络配置了静态 IP 地址，则应指定网络主机的名称。如果使用 DHCP 配置网络，则应从 DNS 中获取主机名。如果 DHCP 或 DNS 配置不正确，系统会自动分配主机名 "`Unified Manager` " 并将其与安全证书关联。

无论主机名的分配方式如何，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。

如果您使用服务器的 IP 地址而不是主机名访问 Web UI ，则在更改主机名后不必生成新证书。但是，最好更新证书，使证书中的主机名与实际主机名匹配。

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。主机名不会在 WFA 中自动更新。

新证书在 Unified Manager 虚拟机重新启动后才会生效。

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 证书才能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。

生成 **HTTPS** 安全证书

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

- 您需要的内容 *

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，例如您希望为可分辨名称（ Distinguished Name ， DN ）设置更好的值，或者您希望增加密钥大小或延长到期期限，或者当前证书已过期。

如果您无法访问 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。如果您使用 `Reset Server Certificate` 选项、则会创建一个新的HTTPS证书、此证书的有效期为397天。此证书的 RSA 密钥大小为 2048 位。

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. 根据要生成证书的方式，选择以下选项之一：

如果您要 ...	执行此操作 ...
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。
使用不同的值生成证书	单击 * 更新当前证书属性 * 选项。 如果不输入新值， " 公用名 " 和 " 备用名称 " 字段将使用现有证书中的值。应将 "`Common Name` " 设置为主机的 FQDN 。其他字段不需要值，但您可以输入电子邮件，公司，部门， 城市，省 / 自治区 / 直辖市和国家 / 地区，以便在证书中填充这些值。您也可以从可用密钥大小（密钥算法为 "`RSA` " ）和有效期中进行选择。 • 允许的密钥大小值为 2048，3072 和 4096。 • 有效期至少为 1 天，最多为 36500 天。 即使允许使用 36500 天的有效期，建议您使用的有效期不超过 397 天或 13 个月。由于如果您选择的有效期超过 397 天，并计划导出此证书的 CSR 并使其由知名 CA 签名，则此 CA 返回给您的签名证书的有效期将缩短为 397 天。 • 如果要从证书的 " 备用名称 " 字段中删除本地标识信息，可以选中 " 排除本地标识信息（例如本地主机） " 复选框。选中此复选框后，备用名称字段将仅使用您在字段中输入的内容。如果留空，则生成的证书将根本没有备用名称字段。

4. 单击 * 是 * 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 证书来验证新证书信息。

重新启动 **Unified Manager** 虚拟机

您可以从 Unified Manager 的维护控制台重新启动虚拟机。生成新的安全证书或虚拟机出现问题时，必须重新启动。

- 您需要的内容 *

虚拟设备已启动。

您以维护用户身份登录到维护控制台。

您也可以使用 * 重新启动来宾 * 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 * > * 重新启动虚拟机 * 。

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

有时，您可能需要更改已安装 Unified Manager 的 Red Hat Enterprise Linux 或 CentOS 计算机的主机名。例如，您可能希望重命名主机，以便在列出 Linux 计算机时更容易按类型，工作组或受监控集群组来识别 Unified Manager 服务器。

- 您需要的内容 *

您必须对安装了 Unified Manager 的 Linux 系统具有 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 。如果您在部署期间为网络配置了静态 IP 地址，则应指定网络主机的名称。如果使用 DHCP 配置网络，则应从 DNS 服务器获取主机名。

无论主机名的分配方式如何，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。

如果您使用服务器的 IP 地址而不是主机名访问 Web UI ，则在更改主机名后不必生成新证书。但是，最好更新证书，以便证书中的主机名与实际主机名匹配。新证书在 Linux 计算机重新启动后才会生效。

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。主机名不会在 WFA 中自动更新。

步骤

1. 以 root 用户身份登录到要修改的 Unified Manager 系统。
2. 输入以下命令以停止 Unified Manager 软件和关联的 MySQL 软件：

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. 使用Linux更改主机名 `hostnamectl` 命令：

   ```
   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：

   ```
   service network restart
   ```

6. 重新启动服务后，验证新主机名是否能够对自身执行 ping 操作：

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   此命令应返回先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，输入以下命令重新启动 Unified Manager：

   ```
   systemctl start mysqld ocie ocieau
   ```

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，但如果使用 Unified Manager 应用此功能，则可以在 Unified Manager 实例监控的所有集群之间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：

新内容	位置
用于配置新工作负载的页面	可从 * 常见任务 * > * 配置 * 获取
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 * 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 * 获取
用于描述当前工作负载性能和工作负载 IOPS 的面板	可从信息板获取

有关这些页面以及此功能的详细信息，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：

如果您要 ...	然后执行此操作 ...
禁用基于策略的存储管理	在 * 基于策略的存储管理 * 面板中，将滑块按钮移至左侧。
启用基于策略的存储管理	在 * 基于策略的存储管理 * 面板中，将滑块按钮移至右侧。