执行配置和管理任务

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

目录

执行配置和管理任务

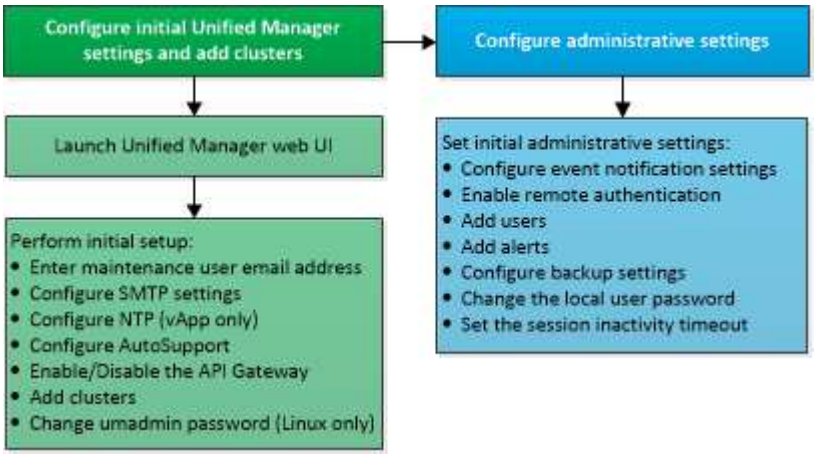
正在配置 **Active IQ Unified Manager**

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

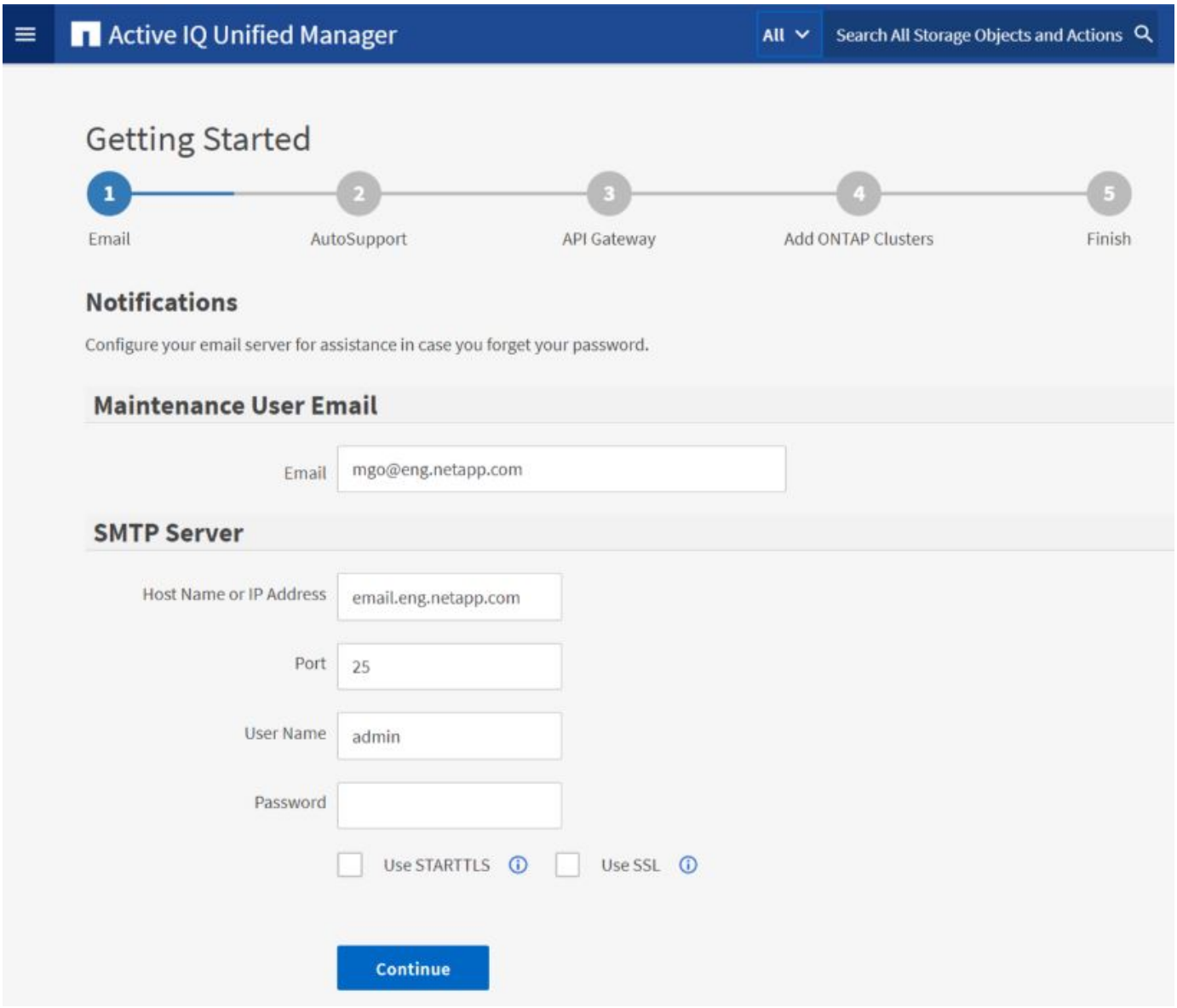
要使用 Unified Manager ，必须先配置初始设置选项，包括 NTP 服务器，维护用户电子邮件地址， SMTP 服务器主机以及添加 ONTAP 集群。

- 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：
  - Unified Manager支持内部ONTAP 集群、ONTAP Select 、Cloud Volumes ONTAP。
  - 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 ）
  - 您具有所需的证书：
- SSL (HTTPS)证书*：此证书归Unified Manager所有。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"。

  EMS证书：此证书归Unified Manager所有。它用于身份验证期间从ONTAP 收到的EMS通知。

  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。

如果要更新旧版本的Unified Manager、则不会自动为集群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"。

- 您可以从Web UI添加集群、系统会自动启用基于证书的身份验证。
- 您可以通过Unified Manager命令行界面添加集群、但默认情况下不会启用基于证书的身份验证。如果要使用Unified Manager命令行界面添加集群、则需要使用Unified Manager界面编辑此集群。您可以看到 "支持的 Unified Manager 命令行界面命令" 使用Unified Manager命令行界面添加集群。
- 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"。

集群证书：此证书归ONTAP 所有。您不能将证书已过期的集群添加到Unified Manager中、如果证书已过期、则应在添加集群之前重新生成该集群。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 * 。

   保存集群详细信息后、您可以看到用于集群相互TLS通信的证书。

   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。

配置 Unified Manager 备份

您可以通过一组配置步骤在 Unified Manager 上配置备份功能，这些配置步骤将通过维护控制台在主机系统和上执行。

有关配置步骤的信息，请参见 "管理备份和还原操作"。

管理功能设置

通过功能设置页面，您可以在 Active IQ Unified Manager 中启用和禁用特定功能。其中包括根据策略创建和管理存储对象，启用 API 网关和登录横幅，上传用于管理警报的脚本，根据非活动时间超时 Web UI 会话以及禁用接收 Active IQ 平台事件。

" 功能设置 " 页面仅适用于具有应用程序管理员角色的用户。

有关脚本上传的信息，请参见 "启用和禁用脚本上传"。

启用基于策略的存储管理

通过 * 基于策略的存储管理 * 选项，可以根据服务级别目标（ Service Level Objective ， SLO ）进行存储管理。默认情况下，此选项处于启用状态。

激活此功能后，您可以在添加到 Active IQ Unified Manager 实例的 ONTAP 集群上配置存储工作负载，并根据分配的性能服务级别和存储效率策略管理这些工作负载。

您可以从 * 常规 * > * 功能设置 * > * 基于策略的存储管理 * 中选择激活或停用此功能。激活此功能后，可以使用以下页面进行操作和监控：

- 配置（存储工作负载配置）
- * 策略 * > * 性能服务级别 *
- * 策略 * > * 存储效率 *
- 集群设置页面上的 " 通过性能服务级别管理的工作负载 " 列
- * 信息板 * 上的工作负载性能面板

您可以使用这些屏幕创建性能服务级别和存储效率策略，以及配置存储工作负载。您还可以监控符合分配的性能服务级别的存储工作负载以及不符合的存储工作负载。您还可以通过工作负载性能和工作负载 IOPS 面板根据数据中心中配置的存储工作负载评估集群的总容量和性能，可用容量和性能以及已用容量和性能（ IOPS ）。

激活此功能后，您可以通过 * 菜单栏 * > * 帮助按钮 * > * API Documentation* > * 存储提供程序 * 类别运行 Unified Manager REST API 来执行其中某些功能。或者、您也可以按+https：//API/docs/API/+格式输入主机名或IP地址以及用于访问REST <hostname>页面的URL

有关API的详细信息、请参见 "Active IQ Unified Manager REST API入门"。

启用 **API** 网关

通过 API 网关功能，可以将 Active IQ Unified Manager 作为一个控制平面来管理多个 ONTAP 集群，而无需单独登录到这些集群。

您可以从首次登录到 Unified Manager 时显示的配置页面启用此功能。或者，您也可以通过 * 常规 * > * 功能设置 * > * API 网关 * 启用或禁用此功能。

Unified Manager REST API 与 ONTAP REST API 不同，并非所有 ONTAP REST API 功能都可通过 Unified Manager REST API 来使用。但是，如果您在访问 ONTAP API 以管理未公开给 Unified Manager 的特定功能方面有特定业务要求，则可以启用 API 网关功能并执行 ONTAP API 。网关充当一个代理，通过保持标头和正文请求的格式与 ONTAP API 中的格式相同来对 API 请求进行通道化。您可以使用 Unified Manager 凭据并执行特定 API 来访问和管理 ONTAP 集群，而无需传递各个集群凭据。Unified Manager 可作为一个管理点在 Unified Manager 实例管理的 ONTAP 集群中运行 API 。API 返回的响应与直接从 ONTAP 执行的相应 ONTAP REST API 返回的响应相同。

启用此功能后，您可以从 * 菜单栏 * > * 帮助按钮 * > * API 文档 * > * 网关 * 类别执行 Unified Manager REST API 。或者、您也可以按格式输入主机名或IP地址以及URL来访问REST API页面 `https://<hostname>/docs/api/`

有关API的详细信息、请参见 "Active IQ Unified Manager REST API入门"。

指定非活动超时

您可以为 Active IQ Unified Manager 指定非活动超时值。在指定时间处于非活动状态后，应用程序将自动注销。默认情况下，此选项处于启用状态。

您可以停用此功能或从 * 常规 * > * 功能设置 * > * 非活动超时 * 中修改时间。激活此功能后，您应在 * 注销时间 * 字段中指定非活动的时间限制（以分钟为单位），超过此时间限制后，系统将自动注销。默认值为 4320 分钟（ 72 小时）。

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。

启用 **Active IQ** 门户事件

您可以指定是要启用还是禁用 Active IQ 门户事件。此设置允许 Active IQ 门户发现和显示有关系统配置，布线等的其他事件。默认情况下，此选项处于启用状态。

启用此功能后， Active IQ Unified Manager 将显示 Active IQ 门户发现的事件。这些事件是通过对从所有受监控存储系统生成的 AutoSupport 消息运行一组规则来创建的。这些事件与其他 Unified Manager 事件不同，它们可识别与系统配置，布线，最佳实践和可用性问题相关的意外事件或风险。

您可以从 * 常规 * > * 功能设置 * > * Active IQ 门户事件 * 中选择激活或停用此功能。在无法访问外部网络的站点中，您必须从 * 存储管理 * > * 事件设置 * > * 上传规则 * 手动上传规则。

默认情况下，此功能处于启用状态。禁用此功能将停止在 Unified Manager 上发现或显示 Active IQ 事件。如果禁用此功能，则 Unified Manager 可以在预定义的时间 00： 15 接收集群上该集群时区的 Active IQ 事件。

为合规性启用和禁用安全设置

通过使用功能设置页面的 * 安全信息板 * 面板上的 * 自定义 * 按钮，您可以在 Unified Manager 上启用或禁用合规性监控的安全参数。

此页面中启用或禁用的设置将控制 Unified Manager 上集群和 Storage VM 的整体合规状态。根据所做的选择，相应的列将显示在集群清单页面的 * 安全性：所有集群 * 视图和 Storage VM 清单页面的 * 安全性：所有 Storage VM* 视图中。

只有具有管理员角色的用户才能编辑这些设置。

系统会根据中定义的建议评估 ONTAP 集群， Storage VM 和卷的安全标准 "《 NetApp ONTAP 9 安全强化指南》"。信息板上的 " 安全 " 面板和 " 安全 " 页面将显示集群， Storage VM 和卷的默认安全合规状态。此外，还会为存在安全违规的集群和 Storage VM 生成安全事件并启用管理操作。

自定义安全设置

要根据您的 ONTAP 环境自定义合规性监控设置，请执行以下步骤：

步骤

1. 单击 * 常规 > 功能设置 > 安全信息板 > 自定义 * 。此时将显示 * 自定义安全信息板设置 * 弹出窗口。

   启用或禁用的安全合规性参数可能会直接影响集群和 Storage VM 屏幕上的默认安全视图，报告和计划报告。如果您在修改安全参数之前已从这些屏幕上传了 Excel 报告，则下载的 Excel 报告可能会出现故障。

2. 要启用或禁用 ONTAP 集群的自定义设置，请在 * 集群 * 下选择所需的常规设置。有关用于自定义集群合规性的选项的信息，请参见 "集群合规性类别"。
3. 要为Storage VM启用或禁用自定义设置、请在* Storage VM*下选择所需的常规设置。有关用于自定义 Storage VM 合规性的选项的信息，请参见 "Storage VM 合规性类别"。

自定义 **AutoSupport** 和身份验证设置

在 * HTTPS 设置 * 部分中，您可以指定是否使用 AutoSupport 传输从 ONTAP 发送 AutoSupport 消息。

在 * 身份验证设置 * 部分中，您可以为默认 ONTAP 管理员用户启用 Unified Manager 警报。

启用和禁用脚本上传

默认情况下，可以将脚本上传到 Unified Manager 并运行这些脚本。如果您的组织出于安全原因不希望允许此活动，您可以禁用此功能。

- 您需要的内容 *

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 * > * 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脚本：

如果您要 ...	然后执行此操作 ...
禁用脚本	在 * 脚本上传 * 面板中，将滑块按钮移至左侧。
启用脚本	在 * 脚本上传 * 面板中，将滑块按钮移至右侧。

正在添加登录横幅

通过添加登录横幅，您的组织可以显示任何信息，例如，允许谁访问系统以及登录和注销期间的使用条款和条件。

任何用户，例如存储操作员或管理员，都可以在登录，注销和会话超时期间查看此登录横幅弹出窗口。

使用维护控制台

您可以使用维护控制台配置网络设置，配置和管理安装了 Unified Manager 的系统，以及执行其他维护任务来帮助您防止可能出现的问题并对其进行故障排除。

维护控制台提供的功能

通过 Unified Manager 维护控制台，您可以维护 Unified Manager 系统上的设置，并进行任何必要的更改以防止出现问题。

根据安装 Unified Manager 的操作系统，维护控制台可提供以下功能：

- 对虚拟设备的任何问题进行故障排除，尤其是在 Unified Manager Web 界面不可用时
- 升级到较新版本的 Unified Manager
- 生成要发送给技术支持的支持包
- 配置网络设置
- 更改维护用户密码
- 连接到外部数据提供程序以发送性能统计信息
- 在内部更改性能数据收集
- 从先前备份的版本还原 Unified Manager 数据库和配置设置。

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。

诊断用户功能

诊断访问的目的是使技术支持能够帮助您进行故障排除，您只能在技术支持的指导下使用它。

诊断用户可以在技术支持的指导下执行操作系统级别的命令，以便进行故障排除。

访问维护控制台

如果 Unified Manager 用户界面未运行，或者您需要执行用户界面中不可用的功能，则可以访问维护控制台来管理 Unified Manager 系统。

- 您需要的内容 *

您必须已安装并配置 Unified Manager 。

处于非活动状态 15 分钟后，维护控制台会将您注销。

安装在 VMware 上后，如果您已通过 VMware 控制台以维护用户身份登录，则无法使用安全 Shell 同时登录。

步骤

1. 按照以下步骤访问维护控制台：

在此操作系统上 ...	请按照以下步骤操作 ...
VMware	a. 使用安全 Shell 连接到 Unified Manager 虚拟设备的 IP 地址或完全限定域名。 b. 使用您的维护用户名和密码登录到维护控制台。
Linux	a. 使用安全 Shell 连接到 Unified Manager 系统的 IP 地址或完全限定域名。 b. 使用维护用户（ umadmin ）名称和密码登录到系统。 c. 输入命令 ... `maintenance_console` 然后按Enter键。
Windows	a. 使用管理员凭据登录到 Unified Manager 系统。 b. 以 Windows 管理员身份启动 PowerShell 。 c. 输入命令 ... `maintenance_console` 然后按Enter键。

此时将显示 Unified Manager 维护控制台菜单。

使用 **vSphere VM** 控制台访问维护控制台

如果 Unified Manager 用户界面未运行，或者您需要执行用户界面中不可用的功能，则可以访问维护控制台以重新配置虚拟设备。

- 您需要的内容 *
- 您必须是维护用户。
- 要访问维护控制台，必须打开虚拟设备的电源。

步骤

1. 在 vSphere Client 中，找到 Unified Manager 虚拟设备。
2. 单击 * 控制台 * 选项卡。
3. 单击控制台窗口内部以登录。
4. 使用您的用户名和密码登录到维护控制台。

   处于非活动状态 15 分钟后，维护控制台会将您注销。

维护控制台菜单

维护控制台包含多个不同的菜单，可用于维护和管理 Unified Manager 服务器的特殊功能和配置设置。

根据安装 Unified Manager 的操作系统，维护控制台包含以下菜单：

- 升级 Unified Manager （仅限 VMware ）
- 网络配置（仅限 VMware ）
- 系统配置（仅限 VMware ）
  a. 支持/诊断
  b. 重置服务器证书
  c. 外部数据提供程序
  d. 备份还原
  e. 性能轮询间隔配置
  f. 禁用 SAML 身份验证
  g. 查看/更改应用程序端口
  h. 调试日志配置
  i. 控制对MySQL端口3306的访问
  j. 退出

您可以从列表中选择用于访问特定菜单选项的编号。例如、对于备份和还原、请选择_4_。

通过网络配置菜单，您可以管理网络设置。如果 Unified Manager 用户界面不可用，则应使用此菜单。

如果 Unified Manager 安装在 Red Hat Enterprise Linux ， CentOS 或 Microsoft Windows 上，则此菜单不可用。

可以使用以下菜单选项。

- * 显示 IP 地址设置 *

  显示虚拟设备的当前网络设置，包括 IP 地址，网络，广播地址，网络掩码，网关， 和 DNS 服务器。

- * 更改 IP 地址设置 *

  用于更改虚拟设备的任何网络设置，包括 IP 地址，网络掩码，网关或 DNS 服务器。如果使用维护控制台将网络设置从 DHCP 切换到静态网络，则无法编辑主机名。要进行更改，必须选择 * 提交更改 * 。

- * 显示域名搜索设置 *

  显示用于解析主机名的域名搜索列表。

- * 更改域名搜索设置 *

  用于更改解析主机名时要搜索的域名。要进行更改，必须选择 * 提交更改 * 。

- * 显示静态路由 *

  显示当前静态网络路由。

- * 更改静态路由 *

  用于添加或删除静态网络路由。要进行更改，必须选择 * 提交更改 * 。

  - * 添加路由 *

    用于添加静态路由。

  - * 删除路由 *

    用于删除静态路由。

  - * 返回 *

    返回到 * 主菜单 * 。

  - * 退出 *

    退出维护控制台。

- * 禁用网络接口 *

禁用任何可用的网络接口。如果只有一个网络接口可用，则无法将其禁用。要进行更改，必须选择 * 提交更改 * 。

- * 启用网络接口 *

  启用可用网络接口。要进行更改，必须选择 * 提交更改 * 。

- * 提交更改 *

  应用对虚拟设备的网络设置所做的任何更改。您必须选择此选项才能实施所做的任何更改，否则不会发生更改。

- 对主机执行 Ping 操作 *

  对目标主机执行 Ping 操作以确认 IP 地址更改或 DNS 配置。

- * 还原为默认设置 *

  将所有设置重置为出厂默认值。要进行更改，必须选择 * 提交更改 * 。

- * 返回 *

  返回到 * 主菜单 * 。

- * 退出 *

  退出维护控制台。

System Configuration 菜单

通过 System Configuration 菜单，您可以通过提供各种选项来管理虚拟设备，例如查看服务器状态以及重新启动和关闭虚拟机。

如果 Unified Manager 安装在 Linux 或 Microsoft Windows 系统上，则此菜单仅提供 "`Restore from a Unified Manager Backup` " 选项。

可以使用以下菜单选项：

- * 显示服务器状态 *

  显示当前服务器状态。状态选项包括 " 正在运行 " 和 " 未运行 " 。

  如果服务器未运行，您可能需要联系技术支持。

- * 重新启动虚拟机 *

  重新启动虚拟机，停止所有服务。重新启动后，虚拟机和服务将重新启动。

- * 关闭虚拟机 *

  关闭虚拟机，停止所有服务。

您只能从虚拟机控制台选择此选项。

- * 更改 < 登录用户 > 用户密码 *

  更改当前登录的用户的密码，该用户只能是维护用户。

- * 增加数据磁盘大小 *

  增加虚拟机中数据磁盘（磁盘 3 ）的大小。

- * 增加交换磁盘大小 *

  增加虚拟机中交换磁盘（磁盘 2 ）的大小。

- * 更改时区 *

  将时区更改为您所在的位置。

- * 更改 NTP 服务器 *

  更改 NTP 服务器设置，例如 IP 地址或完全限定域名（ FQDN ）。

- * 更改 NTP 服务 *

  在之间切换 `ntp` 和 `systemd-timesyncd` 服务。

- * 从 Unified Manager 备份还原 *

  从先前备份的版本还原 Unified Manager 数据库和配置设置。

- * 重置服务器证书 *

  重置服务器安全证书。

- * 更改主机名 *

  更改安装虚拟设备的主机的名称。

- * 返回 *

  退出 System Configuration 菜单并返回 Main Menu 。

- * 退出 *

  退出维护控制台菜单。

支持和诊断菜单

通过 " 支持和诊断 " 菜单，您可以生成一个支持包，您可以将该支持包发送给技术支持以获得故障排除帮助。

可以使用以下菜单选项：

- * 生成轻型支持包 *

  用于生成一个轻型支持包，该支持包只包含 30 天的日志和配置数据库记录，它不包括性能数据，采集记录文件和服务器堆转储。

- * 生成支持包 *

  用于在诊断用户的主目录中创建包含诊断信息的完整支持包（ 7-Zip 文件）。如果您的系统已连接到 Internet ，则还可以将支持包上传到 NetApp 。

  此文件包含 AutoSupport 消息生成的信息， Unified Manager 数据库的内容，有关 Unified Manager 服务器内部的详细数据以及通常不包含在 AutoSupport 消息或轻型支持包中的详细级别日志。

其他菜单选项

您可以使用以下菜单选项在 Unified Manager 服务器上执行各种管理任务。

可以使用以下菜单选项：

- * 重置服务器证书 *

  重新生成 HTTPS 服务器证书。

  您可以通过单击 * 常规 * > * HTTPS 证书 * > * 重新生成 HTTPS 证书 * 在 Unified Manager 图形用户界面中重新生成服务器证书。

- * 禁用 SAML 身份验证 *

  禁用 SAML 身份验证，以便身份提供程序（ IdP ）不再为访问 Unified Manager 图形用户界面的用户提供登录身份验证。如果具有 IdP 服务器或 SAML 配置的问题描述阻止用户访问 Unified Manager 图形用户界面，则通常会使用此控制台选项。

- * 外部数据提供程序 *

  提供了将 Unified Manager 连接到外部数据提供程序的选项。建立连接后，性能数据将发送到外部服务器，以便存储性能专家可以使用第三方软件绘制性能指标图表。此时将显示以下选项：

  - * 显示服务器配置 * - 显示外部数据提供程序的当前连接和配置设置。
  - * 添加 / 修改服务器连接 * —用于输入外部数据提供程序的新连接设置或更改现有设置。
  - * 修改服务器配置 * —用于输入外部数据提供程序的新配置设置或更改现有设置。
  - * 删除服务器连接 * —删除与外部数据提供程序的连接。

    删除此连接后， Unified Manager 将断开与外部服务器的连接。

- 备份还原

  有关信息、请参见下的主题 "管理备份和还原操作"。

- * 性能轮询间隔配置 *

  提供了一个选项，用于配置 Unified Manager 从集群收集性能统计数据的频率。默认收集间隔为 5 分钟。

如果您发现从大型集群收集的操作未按时完成，可以将此间隔更改为 10 或 15 分钟。

- * 查看 / 更改应用程序端口 *

  提供了一个选项，可根据安全要求更改 Unified Manager 用于 HTTP 和 HTTPS 协议的默认端口。对于 HTTP ，默认端口为 80 ，对于 HTTPS ，默认端口为 443 。

- *控制对MySQL端口3306*的访问

  控制主机对默认MySQL端口3306的访问。出于安全原因、在Linux、Windows和VMware vSphere系统上全新安装Unified Manager期间、通过此端口的访问仅限于本地主机。使用此选项可以在本地主机和远程主机之间切换此端口的可见性、也就是说、如果仅在您的环境中为本地主机启用了此端口、则也可以使此端口对远程主机可用。或者、如果为所有主机启用了、则只能将此端口的访问限制为本地主机。如果之前在远程主机上启用了访问、则在升级情形中会保留此配置。您应在更改端口可见性后检查Windows系统上的防火墙设置、如果将防火墙设置配置为限制对MySQL端口3306的访问、则应禁用这些设置。

- * 退出 *

  退出维护控制台菜单。

在 **Windows** 上更改维护用户密码

您可以根据需要更改 Unified Manager 维护用户密码。

步骤

1. 在 Unified Manager Web UI 登录页面中，单击 * 忘记密码 * 。

   此时将显示一个页面，提示您输入要重置其密码的用户的名称。

2. 输入用户名并单击 * 提交 * 。

   将向为此用户名定义的电子邮件地址发送一封包含密码重置链接的电子邮件。

3. 单击电子邮件中的 * 重置密码链接 * 并定义新密码。
4. 返回到 Web UI 并使用新密码登录到 Unified Manager 。

在 **Linux** 系统上更改 **umadmin** 密码

出于安全原因，您必须在完成安装过程后立即更改 Unified Manager umadmin 用户的默认密码。如有必要，您可以随时再次更改密码。

- 您需要的内容 *
- Unified Manager 必须安装在 Red Hat Enterprise Linux 或 CentOS Linux 系统上。
- 您必须具有安装 Unified Manager 的 Linux 系统的 root 用户凭据。

步骤

1. 以 root 用户身份登录到运行 Unified Manager 的 Linux 系统。
2. 更改 umadmin 密码：

```
passwd umadmin
```

系统将提示您输入 umadmin 用户的新密码。

更改 **Unified Manager** 用于 **HTTP** 和 **HTTPS** 协议的端口

为了确保安全， Unified Manager 用于 HTTP 和 HTTPS 协议的默认端口可以在安装后进行更改。对于 HTTP ，默认端口为 80 ，对于 HTTPS ，默认端口为 443 。

- 您需要的内容 *

您必须拥有有权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。

使用 Mozilla Firefox 或 Google Chrome 浏览器时，某些端口被视为不安全。在为 HTTP 和 HTTPS 流量分配新端口号之前，请先咨询浏览器。选择不安全的端口可能会使系统无法访问，这需要您联系客户支持以解决问题。

更改端口后， Unified Manager 实例将自动重新启动，因此请确保现在是关闭系统一小段时间的好时机。

1. 以维护用户身份使用 SSH 登录到 Unified Manager 主机。

   此时将显示 Unified Manager 维护控制台提示符。

2. 键入标有 * 查看 / 更改应用程序端口 * 的菜单选项编号，然后按 Enter 键。
3. 如果出现提示，请再次输入维护用户密码。
4. 键入 HTTP 和 HTTPS 端口的新端口号，然后按 Enter 键。

   如果将端口号留空，则会为此协议分配默认端口。

   系统会提示您是否要更改端口并立即重新启动 Unified Manager 。

5. 键入 * 。 * 以更改端口并重新启动 Unified Manager 。
6. 退出维护控制台。

执行此更改后、用户必须在URL中包含新端口号才能访问Unified Manager Web UI、例如https://host.company.com:1234+, 2001:db8:0:1:2123+.

添加网络接口

如果需要分隔网络流量，可以添加新的网络接口。

- 您需要的内容 *

您必须已使用 vSphere 将网络接口添加到虚拟设备。

必须打开虚拟设备的电源。

如果 Unified Manager 安装在 Red Hat Enterprise Linux 或 Microsoft Windows 上，则无法执行此操作。

步骤

1. 在 vSphere 控制台主菜单中，选择 * 系统配置 * > * 重新启动操作系统 * 。

   重新启动后，维护控制台可以检测新添加的网络接口。

2. 访问维护控制台
3. 选择 * 网络配置 * > * 启用网络接口 * 。
4. 选择新的网络接口并按 * 输入 * 。

   选择 * eth1* 并按 * 输入 * 。

5. 键入 * 。 * 以启用网络接口。
6. 输入网络设置。

   如果使用静态接口或未检测到 DHCP ，系统会提示您输入网络设置。

   输入网络设置后，您将自动返回到 * 网络配置 * 菜单。

7. 选择 * 提交更改 * 。

   您必须提交更改才能添加网络接口。

向 **Unified Manager** 数据库目录添加磁盘空间

Unified Manager 数据库目录包含从 ONTAP 系统收集的所有运行状况和性能数据。在某些情况下，可能需要增加数据库目录的大小。

例如，如果 Unified Manager 从每个集群都有多个节点的大量集群中收集数据，则数据库目录可能已满。当数据库目录已满 90% 时，您将收到警告事件；当目录已满 95% 时，您将收到严重事件。

目录已满 95% 后，不会从集群收集其他数据。

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，向数据目录添加容量所需的步骤会有所不同。

向 **Linux** 主机的数据目录添加空间

分配给的磁盘空间不足 `/opt/netapp/data` 目录以支持Unified Manager最初设置Linux主机并安装Unified Manager时、您可以在安装后通过增加上的磁盘空间来添加磁盘空间 `/opt/netapp/data` 目录。

- 您需要的内容 *

您必须对安装了 Unified Manager 的 Red Hat Enterprise Linux 或 CentOS Linux 计算机具有 root 用户访问权限。

建议您在增加数据目录大小之前备份 Unified Manager 数据库。

步骤

1. 以 root 用户身份登录到要添加磁盘空间的 Linux 计算机。
2. 按所示顺序停止 Unified Manager 服务和关联的 MySQL 软件：

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. 创建临时备份文件夹(例如、 `/backup-data`)、并具有足够的磁盘空间来容纳当前数据 `/opt/netapp/data` 目录。
4. 复制现有的内容和权限配置 `/opt/netapp/data` 目录到备份数据目录：

   ```
   cp -arp /opt/netapp/data/* /backup-data
   ```

5. 如果启用了 SE Linux ：

   a. 为现有上的文件夹获取SE Linux类型 `/opt/netapp/data` 文件夹：

      ```
      se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
      head -1
      ```

      系统将返回类似于以下内容的确认消息：

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. 运行 chcon 命令为备份目录设置 SE Linux 类型：

      ```
      chcon -R --type=mysqld_db_t /backup-data
      ```

6. 删除的内容 `/opt/netapp/data` 目录：

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. 扩展的大小 `/opt/netapp/data` 通过LVM命令或通过添加额外磁盘将目录设置为至少150 GB。

   > 如果已创建 `/opt/netapp/data` 然后、您不应尝试从磁盘挂载 `/opt/netapp/data` 作为NFS或CIFS共享。因为在这种情况下、如果您尝试扩展磁盘空间、则会使用一些LVM命令、例如 `resize` 和 `extend` 可能无法按预期工作。

8. 确认 `/opt/netapp/data` 目录所有者(mysql)和组(root)保持不变：

   ```
   ls -ltr /opt/netapp/ | grep data
   ```

   系统将返回类似于以下内容的确认消息：

```
drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
```

9. 如果启用了SE Linux、请确认的上下文 `/opt/netapp/data` 目录仍设置为mysqld_db_t：

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

   系统将返回类似于以下内容的确认消息：

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. 删除文件 abc ，以便此无关文件将来不发生原因会出现数据库错误。
11. 将备份数据中的内容复制回扩展后的 `/opt/netapp/data` 目录：

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. 如果启用了 SE Linux ，请运行以下命令：

```
chcon -R --type=mysqld_db_t /opt/netapp/data
```

13. 启动 MySQL 服务：

```
systemctl start mysqld
```

14. 启动 MySQL 服务后，按所示顺序启动 ocie 和 ocieau 服务：

```
systemctl start ocie ocieau
```

15. 启动所有服务后、删除备份文件夹 `/backup-data`：

```
rm -rf /backup-data
```

向 **VMware** 虚拟机的数据磁盘添加空间

如果需要增加 Unified Manager 数据库的数据磁盘空间量，则可以在安装后通过使用 Unified Manager 维护控制台增加磁盘空间来添加容量。

- 您需要的内容 *
- 您必须有权访问 vSphere Client 。
- 虚拟机不能在本地存储任何快照。
- 您必须具有维护用户凭据。

建议您在增加虚拟磁盘大小之前备份虚拟机。

步骤

1. 在vSphere客户端中、选择Unified Manager虚拟机、然后向数据添加更多磁盘容量 `disk 3`。有关详细信息，请参见 VMware 文档。

   在极少数情况下， Unified Manager 部署会对数据磁盘使用 "`Hard Disk 2` " ，而不是 "`Hard Disk 3` " 。如果在部署中发生这种情况，请增加较大磁盘的空间。数据磁盘的空间始终会多于另一个磁盘。

2. 在 vSphere 客户端中，选择 Unified Manager 虚拟机，然后选择 * 控制台 * 选项卡。
3. 单击控制台窗口中的，然后使用您的用户名和密码登录到维护控制台。
4. 在主菜单中，输入 * 系统配置 * 选项的编号。
5. 在 System Configuration Menu 中，为 * 增加数据磁盘大小 * 选项输入数字。

向 **Microsoft Windows** 服务器的逻辑驱动器添加空间

如果需要增加 Unified Manager 数据库的磁盘空间量，可以向安装 Unified Manager 的逻辑驱动器添加容量。

- 您需要的内容 *

您必须具有 Windows 管理员权限。

建议您在添加磁盘空间之前备份 Unified Manager 数据库。

步骤

1. 以管理员身份登录到要添加磁盘空间的 Windows 服务器。
2. 按照要用于添加更多空间的方法对应的步骤进行操作：

选项	**Description**
在物理服务器上，向安装 Unified Manager 服务器的逻辑驱动器添加容量。	按照 Microsoft 主题中的步骤进行操作： "扩展基本卷"
在物理服务器上，添加硬盘驱动器。	按照 Microsoft 主题中的步骤进行操作： "添加硬盘驱动器"
在虚拟机上，增加磁盘分区的大小。	按照 VMware 主题中的步骤进行操作： "增加磁盘分区的大小"

管理用户访问

您可以创建角色并分配功能来控制用户对Active IQ Unified Manager 的访问。您可以确定具有访问Unified Manager中选定对象所需功能的用户。只有具有这些角色和功能的用户才能在Unified Manager中管理对象。

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。

- 您需要的内容 *
- 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 。

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 * 。

创建数据库用户

要支持在 Workflow Automation 和 Unified Manager 之间建立连接或访问数据库视图，您必须先在 Unified Manager Web UI 中创建一个具有集成架构或报告架构角色的数据库用户。

- 您需要的内容 *

您必须具有应用程序管理员角色。

数据库用户可与 Workflow Automation 集成并访问特定于报告的数据库视图。数据库用户无权访问 Unified Manager Web UI 或维护控制台，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. 在添加用户对话框的 * 类型 * 下拉列表中选择 * 数据库用户 * 。
4. 键入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 ...	选择此角色
将 Unified Manager 与 Workflow Automation 连接起来	集成架构
访问报告和其他数据库视图	报告架构

6. 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。

- 您需要的内容 *

您必须具有应用程序管理员角色。

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。

- 您需要的内容 *

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。

- 您需要的内容 *
- 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。

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		•	•		

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
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				•	
计划并保存报告		•	•		
从管理操作执行 "`修复` " 操作		•	•		
提供对数据库视图的只读访问权限					•

管理 SAML 身份验证设置

配置远程身份验证设置后，您可以启用安全断言标记语言（ Security Assertion Markup Language ， SAML ）身份验证，以便远程用户先通过安全身份提供程序（ IdP ）进行身份验证，然后才能访问 Unified Manager Web UI 。

请注意，启用 SAML 身份验证后，只有远程用户才能访问 Unified Manager 图形用户界面。本地用户和维护用户将无法访问此 UI 。此配置不会影响访问维护控制台的用户。

身份提供程序要求

在将 Unified Manager 配置为使用身份提供程序（ Identity Provider ， IdP ）对所有远程用户执行 SAML 身份验证时，您需要了解一些必需的配置设置，以便成功连接到 Unified Manager 。

您必须在 IdP 服务器中输入 Unified Manager URI 和元数据。您可以从 Unified ManagerSAML 身份验证页面复制此信息。在安全断言标记语言（ SAML ）标准中， Unified Manager 被视为服务提供商（ Service Provider ， SP ）。

支持的加密标准

- 高级加密标准（ AES ）： AES-128 和 AES-256

- 安全哈希算法（ Secure Hash Algorithm ， SHA ）： SHA-1 和 SHA-256

经过验证的身份提供程序

- Shibboleth
- Active Directory 联合身份验证服务（ ADFS ）

ADFS 配置要求

- 您必须按以下顺序定义 Unified Manager 解析此依赖方信任条目的 ADFS SAML 响应所需的三个声明规则。

声明规则	价值
sam 帐户名称	名称 ID
sam 帐户名称	urn： OID： 0.9.2342.19200300.100.1.1
令牌组—非限定名称	urn： OID： 1.3.6.1.4.1.5923.1.5.1.1

- 您必须将身份验证方法设置为 "`Forms Authentication` " ，否则用户可能会在注销 Unified Manager 时收到错误。请按照以下步骤操作：
  a. 打开 ADFS 管理控制台。
  b. 单击左侧树视图中的身份验证策略文件夹。
  c. 在右侧的 "Actions" 下，单击 Edit Global Primary Authentication Policy 。
  d. 将 "Intranet Authentication Method" （内部网身份验证方法）设置为 "`Forms Authentication` " ，而不是默认值 "`Windows Authentication` " 。
- 在某些情况下，如果 Unified Manager 安全证书是 CA 签名的，则通过 IdP 登录将被拒绝。要解决此问题描述，可以使用两种解决方法：
  - 按照链接中的说明在 ADFS 服务器上禁用对链接的 CA 证书关联依赖方进行的撤消检查：

    "禁用每个依赖方信任的撤消检查"

  - 将 CA 服务器驻留在 ADFS 服务器中，以便对 Unified Manager 服务器证书请求进行签名。

其他配置要求

- Unified Manager 时钟偏差设置为 5 分钟，因此 IdP 服务器和 Unified Manager 服务器之间的时间差不能超过 5 分钟，否则身份验证将失败。

启用 **SAML** 身份验证

您可以启用安全断言标记语言（ SAML ）身份验证，以便远程用户在访问 Unified Manager Web UI 之前先通过安全身份提供程序（ IdP ）进行身份验证。

- 您需要的内容 *

- 您必须已配置远程身份验证并验证它是否成功。
- 您必须已至少创建一个具有应用程序管理员角色的远程用户或远程组。
- Unified Manager 必须支持身份提供程序（ IdP ），并且必须对其进行配置。
- 您必须具有 IdP URL 和元数据。
- 您必须有权访问 IdP 服务器。

从 Unified Manager 启用 SAML 身份验证后，只有在为 IdP 配置了 Unified Manager 服务器主机信息之后，用户才能访问图形用户界面。因此，在开始配置过程之前，您必须准备好完成连接的两个部分。可以在配置 Unified Manager 之前或之后配置 IdP 。

启用 SAML 身份验证后，只有远程用户才能访问 Unified Manager 图形用户界面。本地用户和维护用户将无法访问此 UI 。此配置不会影响访问维护控制台， Unified Manager 命令或 ZAPI 的用户。

在此页面上完成 SAML 配置后， Unified Manager 将自动重新启动。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * SAML 身份验证 * 。
2. 选中 * 启用 SAML 身份验证 * 复选框。

   此时将显示配置 IdP 连接所需的字段。
3. 输入将 Unified Manager 服务器连接到 IdP 服务器所需的 IdP URI 和 IdP 元数据。

   如果可以直接从 Unified Manager 服务器访问 IdP 服务器，则可以在输入 IdP URI 后单击 * 提取 IdP 元数据 * 按钮以自动填充 IdP 元数据字段。
4. 复制 Unified Manager 主机元数据 URI ，或者将主机元数据保存到 XML 文本文件中。

   此时，您可以使用此信息配置 IdP 服务器。
5. 单击 * 保存 * 。

   此时将显示一个消息框，确认您要完成配置并重新启动 Unified Manager 。
6. 单击 * 确认并注销 * ， Unified Manager 将重新启动。

授权远程用户下次尝试访问 Unified Manager 图形界面时，他们将在 IdP 登录页面而不是 Unified Manager 登录页面中输入凭据。

如果尚未完成，请访问 IdP 并输入 Unified Manager 服务器 URI 和元数据以完成配置。

使用 ADFS 作为身份提供程序时， Unified Manager 图形用户界面不会遵守 ADFS 超时要求，它将继续工作，直到达到 Unified Manager 会话超时为止。您可以通过单击 * 常规 * > * 功能设置 * > * 非活动超时 * 来更改 GUI 会话超时。

更改用于 SAML 身份验证的身份提供程序

您可以更改 Unified Manager 用于对远程用户进行身份验证的身份提供程序（ IdP ）。

- 您需要的内容 *
- 您必须具有 IdP URL 和元数据。
- 您必须有权访问 IdP 。

可以在配置 Unified Manager 之前或之后配置新的 IdP 。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * SAML 身份验证 * 。
2. 输入将 Unified Manager 服务器连接到 IdP 所需的新 IdP URI 和 IdP 元数据。

   如果 IdP 可直接从 Unified Manager 服务器访问，则在输入 IdP URL 后，您可以单击 * 提取 IdP 元数据 * 按钮以自动填充 IdP 元数据字段。

3. 复制 Unified Manager 元数据 URI ，或将元数据保存到 XML 文本文件。
4. 单击 * 保存配置 * 。

   此时将显示一个消息框，确认您要更改配置。

5. 单击 * 确定 * 。

访问新 IdP 并输入 Unified Manager 服务器 URI 和元数据以完成配置。

授权远程用户下次尝试访问 Unified Manager 图形界面时，他们将在新的 IdP 登录页面中输入凭据，而不是在旧的 IdP 登录页面中输入凭据。

更改 **Unified Manager** 安全证书后更新 **SAML** 身份验证设置

对 Unified Manager 服务器上安装的 HTTPS 安全证书进行任何更改都需要更新 SAML 身份验证配置设置。如果您重命名主机系统，为主机系统分配新的 IP 地址或手动更改系统的安全证书，则此证书将更新。

更改安全证书并重新启动 Unified Manager 服务器后， SAML 身份验证将无法正常运行，用户将无法访问 Unified Manager 图形界面。您必须同时更新 IdP 服务器和 Unified Manager 服务器上的 SAML 身份验证设置，才能重新启用对用户界面的访问。

步骤

1. 登录到维护控制台。
2. 在 * 主菜单 * 中，输入 * 禁用 SAML 身份验证 * 选项的编号。

   此时将显示一条消息，确认您要禁用 SAML 身份验证并重新启动 Unified Manager 。

3. 使用更新后的 FQDN 或 IP 地址启动 Unified Manager 用户界面，接受更新后的服务器证书并使用维护用户凭据登录。
4. 在 * 设置 / 身份验证 * 页面中，选择 * SAML 身份验证 * 选项卡并配置 IdP 连接。
5. 复制 Unified Manager 主机元数据 URI ，或者将主机元数据保存到 XML 文本文件中。
6. 单击 * 保存 * 。

此时将显示一个消息框，确认您要完成配置并重新启动 Unified Manager 。

7. 单击 * 确认并注销 * ， Unified Manager 将重新启动。
8. 访问 IdP 服务器并输入 Unified Manager 服务器 URI 和元数据以完成配置。

身份提供程序	配置步骤
ADFS	a. 在 ADFS 管理 GUI 中删除现有的依赖方信任条目。 b. 使用添加新的依赖方信任条目 `saml_sp_metadata.xml` 从更新后的Unified Manager服务器。 c. 定义 Unified Manager 解析此依赖方信任条目的 ADFS SAML 响应所需的三个声明规则。 d. 重新启动 ADFS Windows 服务。
Shibboleth	a. 将Unified Manager服务器的新FQDN更新到中 `attribute-filter.xml` 和 `relying-party.xml` 文件。 b. 重新启动 Apache Tomcat Web 服务器并等待端口 8005 联机。

9. 登录到 Unified Manager 并验证 SAML 身份验证是否可通过 IdP 按预期工作。

禁用 **SAML** 身份验证

如果要在远程用户登录到 Unified Manager Web UI 之前停止通过安全身份提供程序（ IdP ）进行身份验证，则可以禁用 SAML 身份验证。禁用 SAML 身份验证后，配置的目录服务提供程序（例如 Active Directory 或 LDAP ）将执行登录身份验证。

禁用 SAML 身份验证后，除了配置的远程用户之外，本地用户和维护用户还可以访问图形用户界面。

如果您无法访问图形用户界面，也可以使用 Unified Manager 维护控制台禁用 SAML 身份验证。

禁用 SAML 身份验证后， Unified Manager 将自动重新启动。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * SAML 身份验证 * 。
2. 取消选中 * 启用 SAML 身份验证 * 复选框。
3. 单击 * 保存 * 。

   此时将显示一个消息框，确认您要完成配置并重新启动 Unified Manager 。

4. 单击 * 确认并注销 * ， Unified Manager 将重新启动。

下次远程用户尝试访问 Unified Manager 图形界面时，他们将在 Unified Manager 登录页面而不是 IdP 登录页面

中输入凭据。

访问 IdP 并删除 Unified Manager 服务器 URI 和元数据。

从维护控制台禁用 **SAML** 身份验证

如果无法访问 Unified Manager 图形用户界面，则可能需要从维护控制台禁用 SAML 身份验证。如果配置不当或 IdP 不可访问，则可能会发生这种情况。

- 您需要的内容 *

您必须以维护用户身份访问维护控制台。

禁用 SAML 身份验证后，配置的目录服务提供程序（例如 Active Directory 或 LDAP ）将执行登录身份验证。除了配置的远程用户之外，本地用户和维护用户还可以访问图形用户界面。

您还可以从 UI 的设置 / 身份验证页面禁用 SAML 身份验证。

禁用 SAML 身份验证后， Unified Manager 将自动重新启动。

步骤

1. 登录到维护控制台。
2. 在 * 主菜单 * 中，输入 * 禁用 SAML 身份验证 * 选项的编号。

   此时将显示一条消息，确认您要禁用 SAML 身份验证并重新启动 Unified Manager 。

3. 键入 * 。 y* ，然后按 Enter 键， Unified Manager 将重新启动。

下次远程用户尝试访问 Unified Manager 图形界面时，他们将在 Unified Manager 登录页面而不是 IdP 登录页面中输入凭据。

如果需要，请访问 IdP 并删除 Unified Manager 服务器 URL 和元数据。

SAML 身份验证页面

您可以使用 "SAML 身份验证 " 页面配置 Unified Manager ，以便在远程用户登录到 Unified Manager Web UI 之前使用 SAML 通过安全身份提供程序（ IdP ）对其进行身份验证。

- 要创建或修改 SAML 配置，您必须具有应用程序管理员角色。
- 您必须已配置远程身份验证。
- 您必须已至少配置一个远程用户或远程组。

配置远程身份验证和远程用户后，您可以选中启用 SAML 身份验证复选框以使用安全身份提供程序启用身份验证。

- * IdP URI*

  从 Unified Manager 服务器访问 IdP 的 URI 。下面列出了示例 URI 。

ADFS 示例 URI：

```
https://win2016-dc.ntap2016.local/federationmetadata/2007-
06/federationmetadata.xml
```

Shibboleth 示例 URI：

```
https://centos7.ntap2016.local/idp/shibboleth
```

- * IdP 元数据 *

  XML 格式的 IdP 元数据。

  如果可以从 Unified Manager 服务器访问 IdP URL ，则可以单击 * 提取 IdP 元数据 * 按钮以填充此字段。

- * 主机系统（ FQDN ） *

  安装期间定义的 Unified Manager 主机系统的 FQDN 。如有必要，您可以更改此值。

- 主机**URI**

  用于从 IdP 访问 Unified Manager 主机系统的 URI 。

- * 主机元数据 *

  XML 格式的主机系统元数据。

管理身份验证

您可以在 Unified Manager 服务器上使用 LDAP 或 Active Directory 启用身份验证，并将其配置为与服务器配合使用以对远程用户进行身份验证。

有关启用远程身份验证，设置身份验证服务以及添加身份验证服务器的信息，请参见前面有关 * 配置 Unified Manager 以发送警报通知 * 的章节。

编辑身份验证服务器

您可以更改 Unified Manager 服务器用于与身份验证服务器通信的端口。

- 您需要的内容 *

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. 选中 * 禁用嵌套组查找 * 框。
3. 在 * 身份验证服务器 * 区域中，选择要编辑的身份验证服务器，然后单击 * 编辑 * 。
4. 在 * 编辑身份验证服务器 * 对话框中，编辑端口详细信息。

5. 单击 * 保存 * 。

删除身份验证服务器

如果要阻止 Unified Manager 服务器与身份验证服务器通信，可以删除身份验证服务器。例如，如果要更改管理服务器正在与其通信的身份验证服务器，则可以删除此身份验证服务器并添加新的身份验证服务器。

- 您需要的内容 *

您必须具有应用程序管理员角色。

删除身份验证服务器后，身份验证服务器的远程用户或组将无法再访问 Unified Manager 。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 远程身份验证 * 。
2. 选择要删除的一个或多个身份验证服务器，然后单击 * 删除 * 。
3. 单击 * 是 * 确认删除请求。

   如果启用了 * 使用安全连接 * 选项，则与身份验证服务器关联的证书将与身份验证服务器一起删除。

使用 **Active Directory** 或 **OpenLDAP** 进行身份验证

您可以在管理服务器上启用远程身份验证，并将管理服务器配置为与身份验证服务器进行通信，以便身份验证服务器中的用户可以访问 Unified Manager 。

您可以使用以下预定义的身份验证服务之一，也可以指定自己的身份验证服务：

- Microsoft Active Directory

  您不能使用 Microsoft 轻型目录服务。

- OpenLDAP

您可以选择所需的身份验证服务并添加相应的身份验证服务器，以使身份验证服务器中的远程用户能够访问 Unified Manager 。远程用户或组的凭据由身份验证服务器维护。管理服务器使用轻型目录访问协议（ Lightweight Directory Access Protocol ， LDAP ）对配置的身份验证服务器中的远程用户进行身份验证。

对于在 Unified Manager 中创建的本地用户，管理服务器会维护自己的用户名和密码数据库。管理服务器执行身份验证，不使用 Active Directory 或 OpenLDAP 进行身份验证。

审核日志记录

您可以使用审核日志来检测审核日志是否受到影响。系统会监控用户执行的所有活动，并将其记录在审核日志中。对 Active IQ Unified Manager 的所有用户界面和公开发布的 API` ' 功能执行审核。

您可以使用*审核日志：文件视图*查看和访问Active IQ Unified Manager 中可用的所有审核日志文件。审核日志

：文件视图中的文件将根据其创建日期列出。此视图显示从安装或升级到系统中的现有时捕获的所有审核日志的信息。无论何时在 Unified Manager 中执行操作，此信息都会更新，并可在日志中查看。每个日志文件的状态均使用 "`File Integrity Status` " 属性捕获，该属性会受到主动监控，以检测日志文件的篡改或删除情况。如果审核日志在系统中可用，则审核日志可能具有以下状态之一：

State	Description
活动	当前正在记录日志的文件。
正常	文件，该文件处于非活动状态，已进行压缩并存储在系统中。
已被篡改	手动编辑文件的用户已损坏的文件。
manual_delete	已被授权用户删除的文件。
lover_delete	由于根据滚动配置策略进行回滚而被删除的文件。
unexpected 删除	由于未知原因而被删除的文件。

审核日志页面包含以下命令按钮：

- 配置
- 删除
- 下载

使用 * 删除 * 按钮可以删除 " 审核日志 " 视图中列出的任何审核日志。您可以删除审核日志，也可以提供删除此文件的原因，以帮助将来确定有效的删除。原因列列出原因以及执行删除操作的用户的名称。

删除日志文件将从发生原因中删除系统中的文件，但不会删除数据库表中的条目。

您可以使用审核日志部分中的 * 下载 * 按钮从 Active IQ Unified Manager 下载审核日志，并导出审核日志文件。标记为"`normal`"或"`篡改`"的文件将下载到压缩的中 `.gzip` 格式。

审核日志文件会定期归档并保存到数据库中以供参考。在归档之前、审核日志会进行数字签名、以保持安全性和完整性。

生成完整的AutoSupport 包后、支持包将同时包含归档和活动的审核日志文件。但是，在生成轻型支持包时，它仅包含活动的审核日志。不包括归档的审核日志。

配置审核日志

您可以使用审核日志部分中的 * 配置 * 按钮为审核日志文件配置滚动策略，并为审核日志启用远程日志记录。

您可以根据要存储在系统中的所需数据量和频率设置 * 最大文件大小 * 和 * 审核日志保留天数 * 中的值。字段 * 审核日志总大小 * 中的值是系统中存在的审核日志总数据的大小。回滚策略由 * 审核日志保留天数 * ， * 最大文件大小 * 和 * 审核日志总大小 * 字段中的值决定。当审核日志备份的大小达到在 * 审核日志总大小 * 中配置的值

时，首先归档的文件将被删除。这意味着删除最旧的文件。但是，此文件条目在数据库中仍然可用，并标记为"`Rollover Delete` "。审核日志保留天数 * 值用于保留审核日志文件的天数。超过此字段中设置的值的任何文件都会进行回滚。

步骤

1. 单击 * 审核日志 * >> * 配置 * 。
2. 输入 * 最大文件大小 * ， * 审核日志总大小 * 和 * 审核日志保留天数 * 中的值。

   如果要启用远程日志记录，则应选择 * 启用远程日志记录 * 。

启用审核日志的远程日志记录

您可以在配置审核日志对话框中选中 * 启用远程日志记录 * 复选框以启用远程审核日志记录。您可以使用此功能将审核日志传输到远程系统日志服务器。这样，当存在空间限制时，您可以管理审核日志。

远程记录审核日志可提供防篡改备份，以防 Active IQ Unified Manager 服务器上的审核日志文件被篡改。

步骤

1. 在 * 配置审核日志 * 对话框中，选中 * 启用远程日志记录 * 复选框。

   此时将显示用于配置远程日志记录的其他字段。

2. 输入要连接到的远程服务器的 * HOSTNAME* 和 * 端口 * 。
3. 在 * 服务器 CA 证书 * 字段中，单击 * 浏览 * 以选择目标服务器的公有证书。

   此证书应上传到中 `.pem` 格式。此证书应从目标系统日志服务器获取，并且不应过期。此证书应包含选定的"`hostname`"作为的一部分 `SubjectAltName` (SAN)属性。

4. 输入以下字段的值： * 连接超时 * ， * 重新连接延迟 * 。

   这些字段的值应以毫秒为单位。

5. 在 * 格式 * 和 * 协议 * 字段中选择所需的系统日志格式和 TLS 协议版本。
6. 如果目标系统日志服务器需要基于证书的身份验证，请选中 * 启用客户端身份验证 * 复选框。

   在保存审核日志配置之前，您需要下载客户端身份验证证书并将其上传到系统日志服务器，否则连接将失败。根据系统日志服务器的类型，您可能需要为客户端身份验证证书创建哈希。

   示例：syslog-ng要求使用命令创建证书的<hash> `openssl x509 -noout -hash -in cert.pem`、然后、您应以符号方式将客户端身份验证证书链接到以<hash>.0命名的文件。

7. 单击 * 保存 * 以配置与服务器的连接并启用远程日志记录。

   您将重定向到 " 审核日志 " 页面。

> “连接超时”值可能会影响配置。如果配置响应所需时间超过定义的值、则可能会因连接错误而导致配置失败。要建立成功的连接，请增加*连接超时*值，然后重试配置。

远程身份验证页面

您可以使用 " 远程身份验证 " 页面配置 Unified Manager ，使其能够与身份验证服务器进行通信，以便对尝试登录到 Unified Manager Web UI 的远程用户进行身份验证。

您必须具有应用程序管理员或存储管理员角色。

选中启用远程身份验证复选框后，您可以使用身份验证服务器启用远程身份验证。

- * 身份验证服务 *

  用于将管理服务器配置为在 Active Directory ， OpenLDAP 等目录服务提供程序中对用户进行身份验证，或者指定您自己的身份验证机制。只有在启用了远程身份验证后，才能指定身份验证服务。

  - * Active Directory*
    - 管理员名称

      指定身份验证服务器的管理员名称。

    - Password

      指定用于访问身份验证服务器的密码。

    - 基本可分辨名称

      指定远程用户在身份验证服务器中的位置。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* 。

    - 禁用嵌套组查找

      指定是启用还是禁用嵌套组查找选项。默认情况下，此选项处于禁用状态。如果使用 Active Directory ，则可以通过禁用对嵌套组的支持来加快身份验证速度。

    - 使用安全连接

      指定用于与身份验证服务器通信的身份验证服务。

  - * OpenLDAP*
    - 绑定可分辨名称

      指定用于在身份验证服务器中查找远程用户的绑定可分辨名称以及基本可分辨名称。

    - 绑定密码

      指定用于访问身份验证服务器的密码。

    - 基本可分辨名称

      指定远程用户在身份验证服务器中的位置。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* 。

    - 使用安全连接

指定使用安全LDAP与LDAP身份验证服务器进行通信。

- * 其他 *
  - 绑定可分辨名称

    指定与基本可分辨名称一起使用的绑定可分辨名称，以便在您配置的身份验证服务器中查找远程用户。

  - 绑定密码

    指定用于访问身份验证服务器的密码。

  - 基本可分辨名称

    指定远程用户在身份验证服务器中的位置。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* 。

  - 协议版本

    指定身份验证服务器支持的轻型目录访问协议（ LDAP ）版本。您可以指定是否必须自动检测协议版本，或者将版本设置为 2 或 3 。

  - 用户名属性

    指定身份验证服务器中包含要由管理服务器进行身份验证的用户登录名的属性名称。

  - 组成员资格属性

    指定一个值，用于根据用户的身份验证服务器中指定的属性和值将管理服务器组成员资格分配给远程用户。

  - UGID

    如果远程用户包括在身份验证服务器中作为 groupOfuniqueNames 对象的成员，则可以使用此选项根据该 groupOfuniqueNames 对象中的指定属性将管理服务器组成员资格分配给远程用户。

  - 禁用嵌套组查找

    指定是启用还是禁用嵌套组查找选项。默认情况下，此选项处于禁用状态。如果使用 Active Directory ，则可以通过禁用对嵌套组的支持来加快身份验证速度。

  - 成员

    指定身份验证服务器用于存储有关组中各个成员的信息的属性名称。

  - 用户对象类

    指定远程身份验证服务器中用户的对象类。

  - 组对象类

    指定远程身份验证服务器中所有组的对象类。

为_Member_、_User Object Class_和_Group Object Class_属性输入的值应与在Active Directory、OpenLDAP和LDAP配置中添加的值相同。否则、身份验证可能会失败。

- 使用安全连接

  指定用于与身份验证服务器通信的身份验证服务。

如果要修改身份验证服务，请确保删除任何现有身份验证服务器并添加新的身份验证服务器。

身份验证服务器区域

" 身份验证服务器 " 区域显示管理服务器与之通信以查找远程用户并对其进行身份验证的身份验证服务器。远程用户或组的凭据由身份验证服务器维护。

- * 命令按钮 *

  用于添加，编辑或删除身份验证服务器。

  - 添加

    用于添加身份验证服务器。

  如果要添加的身份验证服务器属于高可用性对（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。

  - 编辑

    用于编辑选定身份验证服务器的设置。

  - 删除

    删除选定的身份验证服务器。

- * 名称或 IP 地址 *

  显示用于在管理服务器上对用户进行身份验证的身份验证服务器的主机名或 IP 地址。

- * 端口 *

  显示身份验证服务器的端口号。

- * 测试身份验证 *

  此按钮可通过对远程用户或组进行身份验证来验证身份验证服务器的配置。

  测试时，如果仅指定用户名，则管理服务器将在身份验证服务器中搜索远程用户，但不会对用户进行身份验证。如果同时指定用户名和密码，则管理服务器将搜索远程用户并对其进行身份验证。

  如果禁用了远程身份验证，则无法测试身份验证。

管理安全证书

您可以在 Unified Manager 服务器中配置 HTTPS ，以便通过安全连接监控和管理集群。

查看 **HTTPS** 安全证书

您可以将 HTTPS 证书详细信息与浏览器中检索到的证书进行比较，以确保浏览器与 Unified Manager 的加密连接不会被截获。

- 您需要的内容 *

您必须具有操作员，应用程序管理员或存储管理员角色。

通过查看证书，您可以验证重新生成的证书的内容，或者查看可用于访问 Unified Manager 的使用者替代名称（ SAN ）。

步骤

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

   HTTPS 证书将显示在页面顶部

如果您需要查看有关安全证书的详细信息，而不是 HTTPS 证书页面上显示的内容，则可以在浏览器中查看连接证书。

下载 **HTTPS** 证书签名请求

您可以下载当前 HTTPS 安全证书的证书签名请求，以便将文件提供给证书颁发机构进行签名。CA 签名证书有助于防止中间人攻击，并提供比自签名证书更好的安全保护。

- 您需要的内容 *

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 * > * HTTPS 证书 * 。
2. 单击 * 下载 HTTPS 证书签名请求 * 。
3. 保存 `<hostname>.csr` 文件

您可以将文件提供给证书颁发机构进行签名，然后安装签名证书。

安装 **CA** 签名并返回的 **HTTPS** 证书

您可以在证书颁发机构签名并返回安全证书后上传并安装该证书。您上传和安装的文件必须是现有自签名证书的签名版本。CA 签名证书有助于防止中间人攻击，并提供比自签名证书更好的安全保护。

- 您需要的内容 *

您必须已完成以下操作：

- 已下载证书签名请求文件并由证书颁发机构签名
- 已以 PEM 格式保存证书链
- 包括链中的所有证书，从 Unified Manager 服务器证书到根签名证书，包括存在的任何中间证书

您必须具有应用程序管理员角色。

如果创建了 CSR 的证书的有效期超过 397 天，则 CA 会将有效期缩短为 397 天，然后再签署并返回此证书

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * HTTPS 证书 * 。
2. 单击 * 安装 HTTPS 证书 * 。
3. 在显示的对话框中，单击 * 选择文件 …* 以找到要上传的文件。
4. 选择文件，然后单击 * 安装 * 以安装此文件。

有关信息，请参见 "安装使用外部工具生成的 HTTPS 证书"。

证书链示例

以下示例显示了证书链文件的显示方式：

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

安装使用外部工具生成的 **HTTPS** 证书

您可以安装自签名或 CA 签名的证书，这些证书是使用 OpenSSL ， BoringSSL ， LtsEncrypt 等外部工具生成的。

您应将私钥与证书链一起加载，因为这些证书是外部生成的公共 - 私有密钥对。允许的密钥对算法为 "`RSA` " 和 "`EC` " 。"* 安装 HTTPS 证书 * " 选项位于 "General " 部分的 "HTTPS Certificates" 页面中。上传的文件应采用以下输入格式。

1. 属于Active IQ Unified Manager 主机的服务器的专用密钥
2. 与私钥匹配的服务器证书
3. CA 的证书将反向添加到根证书，用于对上述证书进行签名

用于加载具有 **EC** 密钥对的证书的格式

允许的曲线为 "`prime256v1` " 和 " `secp384r1` " 。具有外部生成的 EC 对的证书示例：

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

使用**RSA**密钥对加载证书的格式

属于主机证书的 RSA 密钥对允许的密钥大小为 2048 ， 3072 和 4096 。具有外部生成的 * RSA 密钥对 * 的证书：

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

上传证书后，您应重新启动 Active IQ Unified Manager 实例，以使更改生效。

上传外部生成的证书时检查

系统会在上传使用外部工具生成的证书时执行检查。如果任何检查失败，则证书将被拒绝。此外，还会对产品中的 CSR 生成的证书以及使用外部工具生成的证书进行验证。

- 输入中的私钥将根据输入中的主机证书进行验证。
- 系统会根据主机的 FQDN 检查主机证书中的公用名（ Common Name ， CN ）。
- 主机证书的公用名（ Common Name ， CN ）不应为空或空白，不应设置为 localhost 。
- 有效开始日期不应是未来的，证书的有效到期日期不应是过去的。
- 如果存在中间 CA 或 CA ，则证书的有效期开始日期不应是未来的，而有效期到期日期不应是过去的。

输入中的私钥不应加密。如果存在任何已加密的私钥，则系统会拒绝这些私钥。

示例 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

示例 2.

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

示例3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

证书管理的页面说明

您可以使用 HTTPS 证书页面查看当前安全证书并生成新的 HTTPS 证书。

HTTPS 证书页面

您可以通过"HTTPS证书"页面查看当前安全证书、下载证书签名请求、生成新的自签名HTTPS证书或安装新的HTTPS证书。

如果您尚未生成新的自签名HTTPS证书、则此页面上显示的证书是在安装期间生成的证书。

命令按钮

命令按钮可用于执行以下操作：

- * 下载 HTTPS 证书签名请求 *

  下载当前安装的 HTTPS 证书的认证请求。您的浏览器会提示您保存 <hostname>.csr 文件，以便您可以将此文件提供给证书颁发机构进行签名。

- * 安装 HTTPS 证书 *

  用于在证书颁发机构签名并返回安全证书后上传并安装该证书。新证书将在您重新启动管理服务器后生效。

- * 重新生成 HTTPS 证书 *

  用于生成新的自签名HTTPS证书、此证书将替换当前安全证书。新证书将在重新启动 Unified Manager 后生效。

重新生成 **HTTPS** 证书对话框

通过重新生成 HTTPS 证书对话框，您可以自定义安全信息，然后使用该信息生成新的 HTTPS 证书。

当前证书信息将显示在此页面上。

通过 "`使用当前证书属性重新生成` " 和 "`更新当前证书属性` " 选项，您可以使用当前信息重新生成证书或使用新信息生成证书。

- * 公用名 *

  Required要保护的完全限定域名（ FQDN ）。

  在 Unified Manager 高可用性配置中，使用虚拟 IP 地址。

- * 电子邮件 *

  可选。用于联系您的组织的电子邮件地址；通常是证书管理员或 IT 部门的电子邮件地址。

- * 公司 *

  可选。通常是贵公司的注册名称。

- * 部门 *

  可选。贵公司部门的名称。

- * 城市 *

  可选。公司所在的城市位置。

- * 状态 *

  可选。贵公司所在的州或省 / 自治区 / 直辖市位置，而不是缩写。

- * 国家 / 地区 *

  可选。贵公司所在的国家或地区位置。这通常是国家 / 地区的两个字母的 ISO 代码。

- * 备用名称 *

  Required除了现有本地主机或其他网络地址之外，还可以使用其他非主域名来访问此服务器。使用逗号分隔每个备用名称。

  如果要从证书的 " 备用名称 " 字段中删除本地标识信息，请选中 "`exclude local Identifying information （ e.go localhost ）` " 复选框。如果选中此复选框，则 " 备用名称 " 字段仅会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。

- * 密钥大小（密钥算法： RSA ） *

  密钥算法设置为 RSA 。您可以选择以下密钥大小之一： 2048 ， 3072 或 4096 位。默认密钥大小设置为 2048 位。

- * 有效期 *

  默认有效期为 397 天。如果您已从先前版本升级，则可能会看到先前的证书有效期未更改。

有关详细信息，请参见 "正在生成HTTPS证书"。