执行配置和管理任务

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

执行配置和管理任务 1
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
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 13
使用 Active IQ Unified Manager 中的 CLI 设置会话超时 14
更改 Unified Manager 主机名 14
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 备份 18
管理功能设置 19
了解 Active IQ Unified Manager 中的功能设置 19
在 Active IQ Unified Manager 中启用基于策略的存储管理 19
了解 Active IQ Unified Manager 中的 API Gateway 功能 19
在 Active IQ Unified Manager 中指定非活动超时 20
在 Active IQ Unified Manager 中启用 Active IQ 门户事件 20
在 Active IQ Unified Manager 中启用和禁用合规性安全设置 20
在 Active IQ Unified Manager 中启用和禁用脚本上传 21
在 Active IQ Unified Manager 中添加登录横幅 21
使用维护控制台 22
了解 Active IQ Unified Manager 中的维护控制台 22
了解 Active IQ Unified Manager 中的维护用户 22
Active IQ Unified Manager 中的诊断用户功能 22
访问 Active IQ Unified Manager 中的维护控制台 22
使用 Active IQ Unified Manager 中的 vSphere VM 控制台访问维护控制台 23
维护控制台菜单 24
在 Windows 中更改 Active IQ Unified Manager 的维护用户密码 29
在 Linux 系统上更改 Active IQ Unified Manager umadmin 密码 29
更改 Active IQ Unified Manager 用于 HTTP 和 HTTPS 协议的端口 29
向 Active IQ Unified Manager 添加网络接口 30
在 Active IQ Unified Manager 中重新生成客户端证书 31
添加磁盘空间 31
管理用户访问 34
添加用户 34
在 Active IQ Unified Manager 中编辑用户设置 35

在 Active IQ Unified Manager 中查看用户 36
删除 Active IQ Unified Manager 中的用户或组 36
了解 Active IQ Unified Manager 中基于角色的访问控制 37
了解 Active IQ Unified Manager 中的用户类型 37
了解 Active IQ Unified Manager 中的用户角色 37
了解 Active IQ Unified Manager 中的用户角色和功能 38
管理 SAML 身份验证设置 39
在 Active IQ Unified Manager 中启用 SAML 身份验证 39
在 Active IQ Unified Manager 中使用身份提供程序 40
在 Active IQ Unified Manager 中启用 SAML 身份验证 41
在 Active IQ Unified Manager 中更改 SAML 身份验证标识提供程序 42
在 Active IQ Unified Manager 安全证书更改后更新 SAML 身份验证设置 42
在 Active IQ Unified Manager 中禁用 SAML 身份验证 43
从 Active IQ Unified Manager 维护控制台禁用 SAML 身份验证 44
使用 Active IQ Unified Manager 中的 SAML 身份验证页面 44
管理身份验证 45
在 Active IQ Unified Manager 中编辑身份验证服务器 45
删除 Active IQ Unified Manager 中的身份验证服务器 46
在 Active IQ Unified Manager 中使用 Active Directory 或 OpenLDAP 进行身份验证 46
审核日志记录 46
使用 Active IQ Unified Manager 中的远程身份验证页面 49
管理安全证书 52
在 Active IQ Unified Manager 中查看 HTTPS 安全证书 52
在 Active IQ Unified Manager 中下载 HTTPS 证书签名请求 52
在 Active IQ Unified Manager 中安装 CA 签名的 HTTPS 证书 52
了解在 Active IQ Unified Manager Unified Manager 中使用外部工具生成的 HTTPS 证书 53
证书管理的页面描述 55

执行配置和管理任务

配置 Active IQ Unified Manager

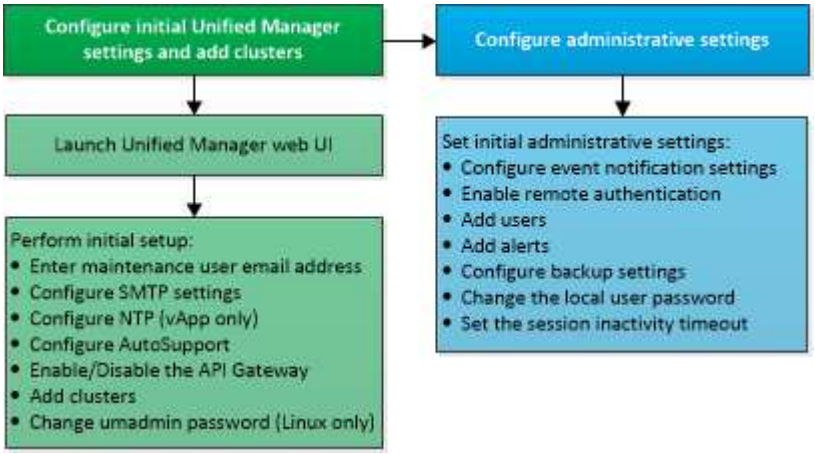
了解有关配置 Active IQ Unified Manager 的信息

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

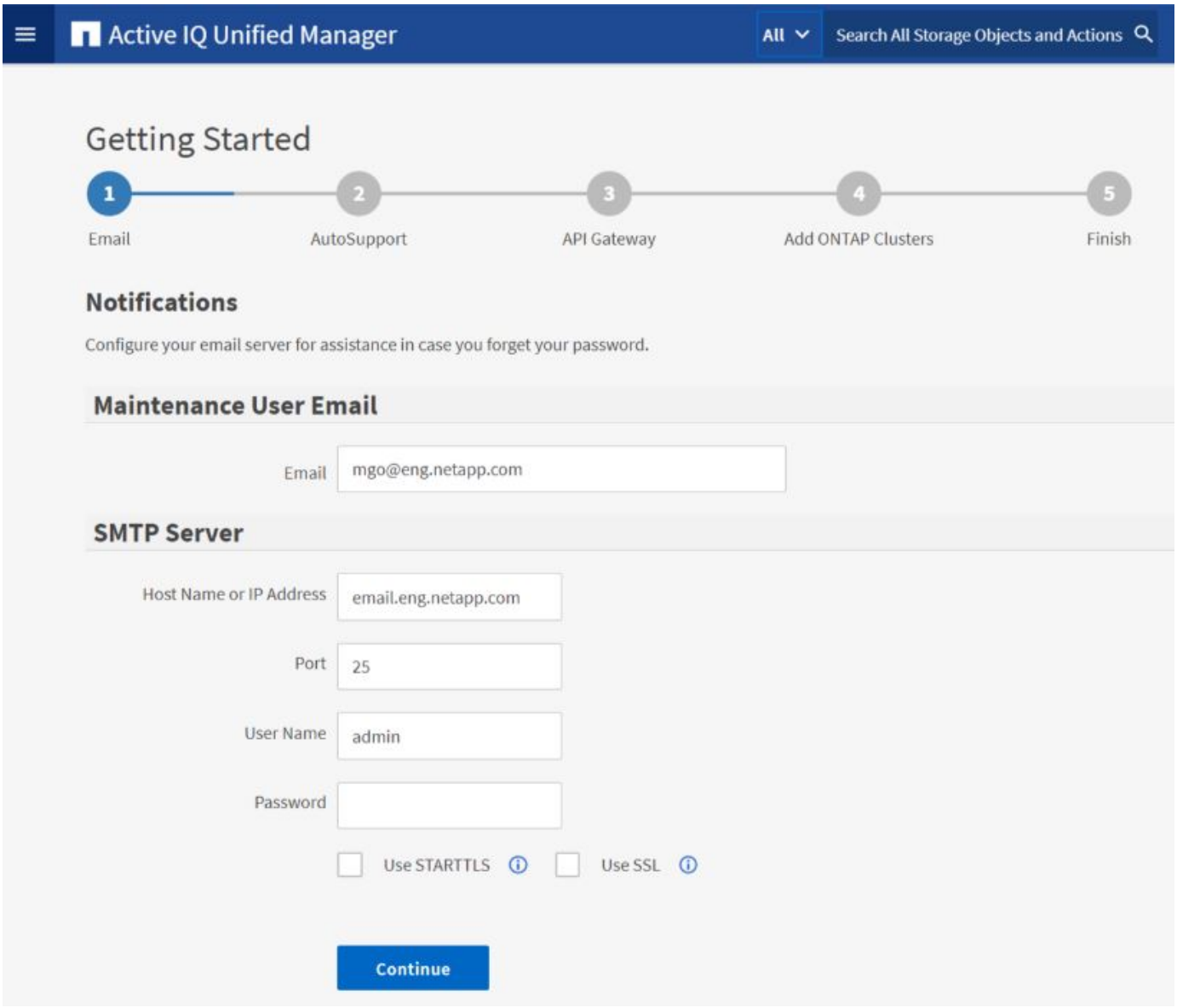
要使用 Unified Manager，必须首先配置初始设置选项，包括 NTP 服务器、维护用户电子邮件地址、SMTP 服务器主机和添加 ONTAP 群集。

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*。
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。

目的	操作
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。

目的	操作
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。

配置 **Active IQ Unified Manager** 备份

您可以通过在主机系统上和通过维护控制台执行的一组配置步骤，在 Unified Manager 上配置备份功能。

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

了解 **Active IQ Unified Manager** 中的功能设置

“功能设置”页面允许您在 Active IQ Unified Manager 中启用和禁用特定功能。这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、根据非活动时间使 Web UI 会话超时，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"。

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

*基于策略的存储管理*选项允许基于服务级别目标（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，以下页面可用于操作和监控：

- 配置（存储工作负载配置）
- 策略 > 性能服务级别
- 策略 > 存储效率
- “群集设置”页面上的“通过性能服务级别管理的工作负载”列
- *仪表板*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，并配置存储工作负载。您还可以监控符合已分配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。工作负载性能和工作负载 IOPS 面板还可让您根据在集群上配置的存储工作负载，评估数据中心内各集群的总容量、可用容量和已用容量以及性能 （IOPS）。

激活此功能后，您可以运行 Unified Manager REST API，以执行 菜单栏 > 帮助按钮 > **API** 文档 > **storage-provider** 类别中的某些功能。或者，您可以输入主机名或 IP 地址以及用于访问 REST API 页面的 URL，格式为 https://<hostname>/docs/api/

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

了解 **Active IQ Unified Manager** 中的 **API Gateway** 功能

API 网关功能使 Active IQ Unified Manager 成为单一控制平面，您可以从中管理多个 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，您可以从 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，并且并非 ONTAP REST API 的所有功能都可以通过使用 Unified Manager REST API 来实现。但是，如果您有访问 ONTAP API 以管理未向 Unified Manager 公开的特定功能的特定业务需求，则可以启用 API 网关功能并执行 ONTAP API。网关充当代理，通过以与 ONTAP API 相同的格式维护标头和正文请求来隧道传输 API 请求。您可以使用 Unified Manager 凭据并执行特定 API 以访问和管理 ONTAP 集群，而无需传递各个集群凭据。Unified Manager 作为单点管理，用于在由您的 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，您可以按以下格式输入主机名或 IP 地址以及用于访问 REST API 页面的 URL `https://<hostname>/docs/api/`

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

在 **Active IQ Unified Manager** 中指定非活动超时

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。

您可以在 常规 > 功能设置 > 非活动超时 中停用此功能或修改时间。激活此功能后，应在 **LOGOUT AFTER** 字段中指定非活动时间限制（以分钟为单位），之后系统会自动注销。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。

在 **Active IQ Unified Manager** 中启用 **Active IQ** 门户事件

您可以指定是否要启用或禁用 Active IQ 门户事件。此设置允许 Active IQ 门户发现并显示有关系统配置、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。这些事件是通过针对所有受监视的存储系统生成的 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事件或风险。

您可以从 **General** > **Feature Settings** > **Active IQ Portal Events** 选择激活或停用此功能。在没有外部网络访问的站点中，您必须从 **Storage Management** > **Event Setup** > **Upload Rules** 手动上传规则。

此功能默认处于启用状态。禁用此功能将停止在 Unified Manager 上发现或显示 Active IQ 事件。禁用后，启用此功能可使 Unified Manager 在该集群时区的预定义时间 00:15 接收集群上的 Active IQ 事件。

在 **Active IQ Unified Manager** 中启用和禁用合规性安全设置

通过使用功能设置页面*安全仪表板*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。

从此页面启用或禁用的设置控制 Unified Manager 上集群和存储虚拟机的整体合规性状态。根据选择，相应的列在集群清单页面的*安全：所有集群*视图和存储虚拟机清单页面的*安全：所有存储虚拟机*视图中可见。

只有具有管理员角色的用户才能编辑这些设置。

将根据 "NetApp ONTAP 9 安全强化指南" 中定义的建议评估您的 ONTAP 集群、存储虚拟机和卷的安全标准。仪表板上的安全面板和安全页面显示集群、存储虚拟机和卷的默认安全合规性状态。还会为存在安全违规的集群和存储虚拟机生成安全事件并启用管理操作。

自定义安全设置

要自定义适用于您的 ONTAP 环境的合规性监控设置，请执行以下步骤：

步骤

1. 单击*常规>功能设置>安全仪表板>自定义*。此时将显示*自定义安全仪表板设置*弹出窗口。

> 您启用或禁用的安全合规性参数会直接影响集群和 Storage VM 屏幕上的默认安全视图、报告和计划报告。如果在修改安全参数之前从这些屏幕上传了 Excel 报告，则下载的 Excel 报告可能会出错。

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. 要启用或禁用存储 VM 的自定义设置，请在 存储 **VM** 下选择所需的常规设置。有关自定义存储 VM 合规性选项的信息，请参见 "Storage VM 合规性类别"。

自定义 **AutoSupport** 和身份验证设置

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

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

在 **Active IQ Unified Manager** 中启用和禁用脚本上传

默认情况下，将脚本上传到 Unified Manager 并运行它们的功能处于启用状态。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。

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* > 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：

目的	操作
禁用脚本	在*脚本上传*面板中，将滑块按钮向左移动。
启用脚本	在*脚本上传*面板中，将滑块按钮向右移动。

在 **Active IQ Unified Manager** 中添加登录横幅

添加登录横幅使您的组织能够显示任何信息，例如登录和注销期间允许访问系统的人员以

及使用条款和条件。

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

了解 **Active IQ Unified Manager** 中的维护控制台

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。

根据已安装 Unified Manager 的操作系统，维护控制台提供以下功能：

- 对虚拟设备的任何问题进行故障诊断，尤其是在 Unified Manager Web 界面不可用时
- 升级到较新版本的 Unified Manager
- 生成支持包以发送给技术支持
- 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
- 更改内部性能数据收集
- 从以前备份的版本恢复 Unified Manager 数据库和配置设置。

了解 **Active IQ Unified Manager** 中的维护用户

维护用户是在 Red Hat Enterprise Linux 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，并且该用户可以创建后续用户并为其分配角色。

维护用户（即 umadmin 用户）也可以访问 Unified Manager 维护控制台。

Active IQ Unified Manager 中的诊断用户功能

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

诊断用户可以在技术支持人员的指导下执行操作系统级别的命令，以进行故障排除。

访问 **Active IQ Unified Manager** 中的维护控制台

如果 Unified Manager 用户界面未运行，或者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。

开始之前

您必须已安装并配置 Unified Manager。

15 分钟不活动后，维护控制台会将您注销。

> 在 VMware 上安装时，如果已经通过 VMware 控制台以维护用户身份登录，则不能同时使用 Secure Shell 登录。

步骤

1. 按照下面的步骤访问维护控制台：

在此操作系统上……	按照下面的步骤进行操作……
VMware	a. 使用 Secure Shell，连接到 Unified Manager 虚拟设备的 IP 地址或完全限定的域名。 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 Secure 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) 名称和密码登录到此系统。 c. 输入命令 `maintenance_console`并按 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`并按 Enter 键。

此时将显示 Unified Manager 维护控制台菜单。

使用 **Active IQ Unified Manager** 中的 **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。

开始之前

- 您必须是维护用户。
- 必须打开虚拟设备电源才能访问维护控制台。

步骤

1. 在 vSphere 客户端中，找到 Unified Manager 虚拟设备。
2. 单击 **Console** 选项卡。
3. 在控制台窗口内单击以登录。
4. 使用您的用户名和密码登录到维护控制台。

   15 分钟不活动后，维护控制台会将您注销。

维护控制台菜单

了解 **Active IQ Unified Manager** 中的维护控制台菜单

维护控制台由不同的菜单组成，使您可以维护和管理 Unified Manager 服务器的特殊功能和配置设置。

根据已安装 Unified Manager 的操作系统，维护控制台包括以下菜单：

- 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. 重新生成客户端证书
  d. 备份还原
  e. 外部数据提供程序
  f. 性能轮询间隔配置
  g. 禁用 SAML 身份验证
  h. 查看/更改应用程序端口
  i. 调试日志配置
  j. 控制对 MySQL 端口 3306 的访问
  k. 退出

您可以从列表中选择数字来访问特定的菜单选项。例如，对于备份和还原，您可以选择 *4*。

Active IQ Unified Manager 中的网络配置菜单

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

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

提供以下菜单选项。

- 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

  使您能够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。您必须选择 提交更改 才能使更改生效。

- 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

  使您能够在解析主机名时更改要搜索的域名。您必须选择*提交更改*才能使更改生效。

- 显示静态路由

  显示当前静态网络路由。

- 更改静态路由

  使您可以添加或删除静态网络路由。必须选择*提交更改*才能使更改生效。

  - 添加路由

    使您可以添加静态路由。

  - 删除路由

    使您可以删除静态路由。

  - 返回

    带您返回*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，则无法禁用它。必须选择*提交更改*才能使更改生效。

- 启用网络接口

  启用可用的网络接口。您必须选择*提交更改*才能使更改生效。

- 提交更改

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

- **Ping** 主机

  Ping 目标主机以确认 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。必须选择*提交更改*才能使更改生效。

- 返回

  带您返回*主菜单*。

- 退出

  退出维护控制台。

使用 **Active IQ Unified Manager** 中的系统配置菜单

系统配置菜单通过提供各种选项，例如查看服务器状态以及重新启动和关闭虚拟机，使您能够管理虚拟设备。

在 Linux 或 Microsoft Windows 系统上安装 Unified Manager 时，此菜单中仅提供 “从 Unified Manager 备份还原” 选项。

提供以下菜单选项：

- 显示服务器状态

  显示当前服务器状态。状态选项包括运行和未运行。

  如果服务器未运行，您可能需要与技术支持联系。

- 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**<logged in user>**用户密码

  更改当前登录的用户的密码，此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 地址或完全限定的域名（FQDN）。

- 更改 **NTP** 服务

  在 `ntp`和 `systemd-timesyncd`服务之间切换。

- 从 **Unified Manager** 备份还原

  从以前备份的版本恢复 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。

- 更改主机名称

  更改安装虚拟设备的主机名称。

- 返回

  退出系统配置菜单并返回主菜单。

- 退出

  退出维护控制台菜单。

使用 **Active IQ Unified Manager** 中的支持和诊断菜单

通过“支持和诊断”菜单，您可以生成可发送给技术支持以获得故障排除帮助的支持包。

提供以下菜单选项：

- 生成轻量级支持捆绑包

  使您能够生成仅包含 30 天日志和配置数据库记录的轻量级支持包——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

  允许您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互联网，您也可以将支持包上传到 NetApp。

  该文件包括由 AutoSupport 消息生成的信息、Unified Manager 数据库的内容、有关 Unified Manager 服务器内部的详细信息以及通常不包含在 AutoSupport 消息或轻量级支持捆绑包中的详细级别日志。

了解有关 **Active IQ Unified Manager** 中其他维护控制台菜单选项的信息

以下菜单选项可用于在 Unified Manager 服务器上执行各种管理任务。

提供以下菜单选项：

- 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 GUI 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 GUI 的用户提供登录身份验证。当 IdP 服务器或 SAML 配置出现问题，导致用户无法访问 Unified Manager GUI 时，通常会使用此控制台选项。

- 外部数据提供商

  提供用于将 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--允许您为外部数据提供程序输入新的连接设置，或更改现有设置。
  - 修改服务器配置--允许您为外部数据提供程序输入新的配置设置，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。

    删除连接后，Unified Manager 将失去与外部服务器的连接。

- 备份还原

  有关信息，请参见 "管理备份和还原操作" 下的主题。

- 性能轮询间隔配置

  提供配置 Unified Manager 从群集收集性能统计数据的频率的选项。默认收集间隔为 5 分钟。

  如果发现来自大型集群的收集未按时完成，则可以将此时间间隔更改为 10 或 15 分钟。

- 查看/更改应用程序端口

  如果出于安全需要，提供更改 Unified Manager 用于 HTTP 和 HTTPS 协议的默认端口的选项。HTTP 的默认端口为 80，HTTPS 的默认端口为 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。此选项使您能够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此端口，您也可以将此端口提供给远程主机。或者，当对所有主机启用时，您可以将此端口的访问限制为仅本地主机。如果以前在远程主机上启用了访问，则在升级场景中保留配置。切换端口可见性后，应检查 Windows 系统上的防火墙设置，如果设置配置为限制对 MySQL 端口 3306 的访问，则应禁用防火墙设置。

- 退出

  退出维护控制台菜单。

在 **Windows** 中更改 **Active IQ Unified Manager** 的维护用户密码

您可以在需要时更改 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，提示输入要重置密码的用户名。

2. 输入用户名并单击*提交*。

   带有重置密码链接的电子邮件将发送到为该用户名定义的电子邮件地址。

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 **Active IQ Unified Manager 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，您可以稍后随时再次更改密码。

开始之前

- Unified Manager 必须安装在 Red Hat Enterprise Linux 系统上。
- 您必须具有安装了 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
   ```

   系统会提示您输入 umadmin 用户的新密码。

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

如果出于安全原因需要，可以在安装后更改 Unified Manager 用于 HTTP 和 HTTPS 协议的默认端口。HTTP 的默认端口为 80，HTTPS 的默认端口为 443。

开始之前

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

> 在使用 Mozilla Firefox 或 Google Chrome 浏览器时，有些端口被认为是不安全的。在为 HTTP 和 HTTPS 流量分配新的端口号之前，请检查您的浏览器。选择不安全的端口可能会导致系统无法访问，这需要您联系客户支持以获得解决方案。

更改端口后，Unified Manager 的实例会自动重新启动，因此请确保这是让系统在短时间内停止运行的好时机。

1. 使用 SSH 作为维护用户登录到 Unified Manager 主机。

   此时将显示 Unified Managermaintenance 控制台提示。

2. 键入标有 **View/Change Application Ports** 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。

   将端口号留空将为协议分配默认端口。

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

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

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、https://12.13.14.15:1122 或 https://[2001:db8:0:1]:2123。

向 **Active IQ Unified Manager** 添加网络接口

如果需要分离网络流量，可以添加新的网络接口。

开始之前

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 > 重启操作系统。

   重新启动后，维护控制台可以检测到新添加的网络接口。

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，然后按 **Enter**。

   选择 **eth1**，然后按 **Enter**。

5. 键入 **y** 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*网络配置*菜单。

7. 选择*提交更改*。

   必须提交更改才能添加网络接口。

在 **Active IQ Unified Manager** 中重新生成客户端证书

您可以使用维护控制台重新生成 Unified Manager 客户端证书。您的证书有效期延长为五年。

步骤

1. 以维护用户身份登录。
2. 选择*重新生成客户端证书*，然后按*Enter*。
3. 如果系统提示进行身份验证，请输入所需的凭据。
4. 选择 确认重新生成，然后按 **Enter**。
5. 重新生成证书后，重新启动 Unified Manager 服务以应用更改。
6. 要验证更新的证书，请登录到 ONTAP。查看客户端证书状态和有效性状态。

相关信息 "使用 System Manager 管理 ONTAP 证书"

添加磁盘空间

向 **Active IQ 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 从每个群集都有多个节点的大量群集收集数据，则数据库目录可能会变满。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。

目录满 95% 后，不会再从集群中收集其他数据。

向数据目录添加容量所需的步骤不同，具体取决于 Unified Manager 是在 VMware ESXi 服务器上运行、在 Red Hat 服务器上运行还是在 Microsoft Windows 服务器上运行。

在 **Active IQ Unified Manager** 的 **Linux** 主机上向数据目录添加空间

如果您在最初设置 Linux 主机并安装 Unified Manager 时为 `/opt/netapp/data`目录分配的磁盘空间不足以支持 Unified Manager，则可以在安装后通过增加 `/opt/netapp/data`目录上的磁盘空间来添加磁盘空间。

开始之前

您必须具有对安装了 Unified Manager 的 Red Hat Enterprise Linux 计算机的 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. 创建具有足够磁盘空间的临时备份文件夹（例如 `/backup-data`），以包含当前 `/opt/netapp/data` 目录中的数据。
4. 将现有 `/opt/netapp/data`目录的内容和权限配置复制到备份数据目录：

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

5. 如果启用了 SE Linux：

   a. 获取现有 `/opt/netapp/data`文件夹中文件夹的 SE Linux 类型：

      ```
      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 `/opt/netapp/data`目录的内容：

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. 通过 LVM 命令或添加额外磁盘，将 `/opt/netapp/data`目录的大小扩展到至少 150 GB。

   > 如果您从磁盘创建了 `/opt/netapp/data`，则不应尝试将 `/opt/netapp/data`作为 `NFS` 或 `CIFS` 共享进行挂载。因为在这种情况下，如果您尝试扩展磁盘空间，某些 `LVM` 命令（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）未更改：

   ```
   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 `/opt/netapp/data` 目录的上下文仍然设置为 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，以免这个多余的文件在将来引发数据库错误。
11. 将 backup-data 中的内容复制回扩展的 `/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. MySQL 服务启动后，按所示顺序启动 ocie 和 ocieau 服务：

```
systemctl start ocie ocieau
```

15. 所有服务启动后，删除备份文件夹 `/backup-data`：

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

在 **Active IQ Unified Manager** 中向 **VMware** 虚拟机上的数据磁盘添加空间

如果需要增加 Unified Manager 数据库的数据磁盘上的空间量，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。

开始之前

- 您必须能够访问 vSphere 客户端。
- 虚拟机必须没有本地存储的快照。
- 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 `disk 3`添加更多磁盘容量。有关详细信息，请参阅 VMware 文档。

   在某些罕见情况下，Unified Manager 部署使用 “Hard Disk 2” 作为数据磁盘，而不是 “Hard Disk 3”。如果在您的部署中发生此情况，请增加较大磁盘的空间。数据磁盘的空间将始终大于另一个磁盘。

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. 在控制台窗口中单击，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. 在系统配置菜单中，输入*增加数据磁盘大小*选项的数字。

在 **Active IQ Unified Manager** 中向 **Windows** 服务器上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。

开始之前

您必须具有 Windows 管理员权限。

我们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. 请按照要添加更多空间的方法对应的步骤操作：

选项	问题描述
在物理服务器上，向安装有 Unified Manager 服务器的逻辑驱动器添加容量。	按照 Microsoft 主题中的步骤操作： "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 主题中的步骤操作： "增加磁盘分区的大小"

管理用户访问

添加用户

在 **Active IQ Unified Manager** 中添加用户

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

开始之前

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

将这些用户定义为 “remote” 用户。

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

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

步骤

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

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

4. 单击 **Add**。

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

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

开始之前

您必须具有应用程序管理员角色。

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

步骤

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

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

6. 单击 **Add**。

在 **Active IQ Unified Manager** 中编辑用户设置

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

开始之前

您必须具有应用程序管理员角色。

当您修改分配给用户的角色时，会在发生以下任一操作时应用更改：

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

步骤

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

在 **Active IQ Unified Manager** 中查看用户

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

开始之前

您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击 常规 > 用户。

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

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

开始之前

- 删除远程组时，必须重新分配已分配给远程组用户的事件。

  如果要删除本地用户或远程用户，则分配给这些用户的事件将自动取消分配。

- 您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击 常规 > 用户。
2. 在“用户”页面中，选择要删除的用户或组，然后单击 删除。
3. 单击 是 确认删除。

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

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

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

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

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

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

Unified Manager 用户类型如下：

- 维护用户

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

- 本地用户

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

- 远程组

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

- 远程用户

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

- 数据库用户

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

了解 **Active IQ Unified Manager** 中的用户角色

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

Unified Manager 包括以下预定义的用户角色：

- 操作员

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

- 存储管理员

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

- 应用程序管理员

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

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

- 集成架构

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

- 报告架构

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

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

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

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

下表显示了每个用户角色可以执行的功能：

功能	运算符	存储管理员	应用程序管理员	集成架构	报告架构
查看存储系统信息	•	•	•	•	•

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
查看其他数据，例如历史记录和容量趋势	•	•	•	•	•
查看、分配和解决事件	•	•	•		
查看存储服务对象，例如 SVM 关联和资源池	•	•	•		
查看阈值策略	•	•	•		
管理存储服务对象，例如 SVM 关联和资源池		•	•		
定义警报		•	•		
管理存储管理选项		•	•		
管理存储管理策略		•	•		
管理用户			•		
管理管理选项			•		
定义阈值策略			•		
管理数据库访问			•		
管理与 WFA 的集成并提供对数据库视图的访问				•	
安排并保存报告		•	•		
从管理操作执行 “Fix It” 操作		•	•		
提供对数据库视图的只读访问权限					•

管理 SAML 身份验证设置

在 Active IQ Unified Manager 中启用 SAML 身份验证

配置远程身份验证设置后，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 之前由安全身份提供程序（IdP）进行身份验证。

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

在 **Active IQ Unified Manager** 中使用身份提供程序

在将 Unified Manager 配置为使用身份提供程序（IdP）为所有远程用户执行 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。

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 被视为服务提供程序（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（SHA）：SHA-1 和 SHA-256

已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

- 必须按以下顺序定义三个声明规则，这些规则是 Unified Manager 解析此依赖方信任项的 ADFS SAML 响应所必需的。

声明规则	值
SAM-account-name	名称 ID
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
令牌组 — 未限定名称	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“表单身份验证”，否则用户在注销 Unified Manager 时可能会收到错误。按照以下步骤操作：
  a. 打开 ADFS 管理控制台。
  b. 单击左侧树视图上的身份验证策略文件夹。
  c. 在右侧的“操作”下，单击“编辑全局主要身份验证策略”。
  d. 将 Intranet 身份验证方法设置为“`Forms Authentication`”，而不是默认的“`Windows Authentication`”。
- 在某些情况下，当 Unified Manager 安全证书经过 CA 签名时，通过 IdP 登录会被拒绝。有两种解决方法可以解决此问题：
  - 按照链接中标识的说明，在 ADFS 服务器上禁用链式 CA 证书关联依赖方的吊销检查：

    "禁用每个依赖方信任的吊销检查"
  - 请让 CA 服务器驻留在 ADFS 服务器内，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。

在 **Active IQ Unified Manager** 中启用 **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 之前由安全身份提供程序（IdP）进行身份验证。

开始之前

- 您必须已配置远程身份验证并验证其成功。
- 您必须至少创建了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。
- 您必须能够访问 IdP 服务器。

从 Unified Manager 启用 SAML 身份验证后，在使用 Unified Manager 服务器主机信息配置 IdP 之前，用户无法访问图形用户界面。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 UI。此配置不会影响访问维护控制台、Unified Manager 命令或 ZAPI 的用户。

完成此页面上的 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。

   将显示配置 IdP 连接所需的字段。

3. 请输入将 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，您可以在输入 IdP URI 后单击 获取 **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，或将主机元数据保存到 XML 文本文件。

   您此时可以使用此信息配置 IdP 服务器。

5. 单击 **Save**。

   此时将显示一个消息框，以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。

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

页面中输入其凭据。

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

> 将 ADFS 用作身份提供程序时，Unified Manager GUI 不会遵守 ADFS 超时，并且将继续工作，直到达到 Unified Manager 会话超时。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。

在 **Active IQ Unified Manager** 中更改 **SAML** 身份验证标识提供程序

您可以更改 Unified Manager 用来验证远程用户的身份提供程序（IdP）。

开始之前

- 您必须具有 IdP URL 和元数据。
- 您必须能够访问 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. 请输入将 Unified Manager 服务器连接到 IdP 所需的新 IdP URI 和 IdP 元数据。

   如果可以直接从 Unified Manager 服务器访问 IdP，您可以在输入 IdP URL 后单击 获取 **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，以确认您要更改配置。

5. 单击 **OK**。

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

下次授权远程用户尝试访问 Unified Manager 图形界面时，他们将在新的 IdP 登录页面而不是旧的 IdP 登录页面中输入其凭据。

在 **Active IQ Unified Manager** 安全证书更改后更新 **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，则会更新证书。

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

步骤

1. 登录维护控制台。
2. 在*主菜单*中，输入*禁用 SAML 身份验证*选项的数字。

   系统将显示一条消息，以确认您要禁用 SAML 身份验证并重新启动 Unified Manager。
3. 使用更新的 FQDN 或 IP 地址启动 Unified Manager 用户界面，在浏览器中接受更新的服务器证书，然后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，或将主机元数据保存到 XML 文本文件。
6. 单击 **Save**。

   此时将显示一个消息框，以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. 请访问您的 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. 删除 ADFS 管理 GUI 中的现有依赖方信任条目。 b. 使用更新后的 Unified Manager 服务器中的 `saml_sp_metadata.xml`添加新的依赖方信任项。 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 `attribute-filter.xml`和 `relying-party.xml`文件中。 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，并通过 IdP 验证 SAML 身份验证是否按预期工作。

在 **Active IQ Unified Manager** 中禁用 **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）对其进行身份验证，则可以禁用 SAML 身份验证。禁用 SAML 身份验证时，已配置的目录服务提供程序（如 Active Directory 或 LDAP）将执行登录身份验证。

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

如果您无权访问图形用户界面，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，将自动重新启动 Unified Manager。

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 **Save**。

   此时将显示一个消息框，以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 登录页面中输入其凭据。

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

从 **Active IQ Unified Manager** 维护控制台禁用 **SAML** 身份验证

当无法访问 Unified Manager GUI 时，您可能需要从维护控制台禁用 SAML 身份验证。这可能发生在配置错误或 IdP 不可访问的情况下。

开始之前

您必须能够以维护用户的身份访问维护控制台。

禁用 SAML 身份验证时，已配置的目录服务提供程序（如 Active Directory 或 LDAP）将执行登录身份验证。除了已配置的远程用户外，本地用户和维护用户也将能够访问图形用户界面。

您还可以从 UI 中的“设置/身份验证”页面禁用 SAML 身份验证。

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

步骤

1. 登录维护控制台。
2. 在*主菜单*中，输入*禁用 SAML 身份验证*选项的数字。

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

3. 键入 **y**，然后按 Enter，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 登录页面中输入其凭据。

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

使用 **Active IQ Unified Manager** 中的 **SAML** 身份验证页面

您可以使用 SAML 身份验证页面将 Unified Manager 配置为使用 SAML 通过安全身份提供程序（IdP）对远程用户进行身份验证，然后他们才能登录到 Unified Manager web UI。

- 您必须具有应用程序管理员角色才能创建或修改 SAML 配置。

- 您必须事先配置远程身份验证。
- 您必须事先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，以启用使用安全身份提供程序的身份验证。

- **IdP URI**

  从 Unified Manager 服务器访问 IdP 的 URI。以下列出了示例 URI。

  ADFS 的示例 URI：

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

  Shibboleth 的示例 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 获取 **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

在 **Active IQ Unified Manager** 中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。

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* > 远程身份验证。
2. 选中 **Disable Nested Group Lookup**（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 **Save**。

删除 **Active IQ Unified Manager** 中的身份验证服务器

如果要阻止 Unified Manager 服务器与身份验证服务器通信，则可以删除身份验证服务器。例如，如果要更改与管理服务器通信的身份验证服务器，则可以删除身份验证服务器并添加新的身份验证服务器。

开始之前

您必须具有应用程序管理员角色。

删除身份验证服务器时，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。

在 **Active IQ Unified Manager** 中使用 **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您的身份验证服务器进行通信，以便身份验证服务器内的用户可以访问 Unified Manager。

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 Lightweight Directory Services。

- OpenLDAP

您可以选择所需的身份验证服务并添加适当的身份验证服务器，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（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，管理服务器维护其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

了解 **Active IQ Unified Manager** 中的审核日志

您可以使用审核日志来检测审核日志是否已受损。用户执行的所有活动都将受到监控并记

录在审核日志中。审核针对 Active IQ Unified Manager 的所有用户界面和公开的 API 功能执行。

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目前为止在系统中捕获的所有审核日志的信息。每当您在 Unified Manager 中执行操作时，信息都会更新并在日志中可用。每个日志文件的状态是使用“File Integrity Status” 属性捕获的，该属性受到主动监控，以检测日志文件是否被篡改或删除。当审核日志在系统中可用时，审核日志可以具有以下状态之一：

州/省	问题描述
处于活动状态	当前正在记录日志的文件。
正常	非活动、压缩并存储在系统中的文件。
已篡改	已被手动编辑该文件的用户破坏的文件。
MANUAL_DELETE	已被授权用户删除的文件。
ROLLOVER_DELETE	由于根据滚动配置策略滚动而被删除的文件。
UNEXPECTED_DELETE	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

DELETE 按钮使您能够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，并可选择提供删除文件的原因，这有助于将来确定有效的删除。REASON 列列出原因以及执行删除操作的用户的名称。

删除日志文件将导致从系统中删除文件，但不会删除 DB 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 “TAMPERED” 的文件将以压缩 `.gzip`格式下载。

审核日志文件定期存档并保存到数据库中以供参考。在存档之前，审核日志经过数字签名，以维护安全性和完整性。

生成完整的 AutoSupport 捆绑包时，支持捆绑包将包含已归档和活动的审核日志文件。但是，当生成轻型支持捆绑包时，它仅包含活动的审核日志。不包含已归档的审核日志。

配置 **Active IQ Unified Manager** 审核日志

您可以使用审核日志部分中的*配置*按钮来配置审核日志文件的滚动策略，并启用审核日志的远程日志记录。

您可以根据要在系统中存储的数据量和频率，设置 **MAX FILE SIZE** 和 **AUDIT LOG RETENTION DAYS** 的值。**TOTAL AUDIT LOG SIZE** 字段中的值是系统中存在的审核日志数据的总大小。滚动策略由 **AUDIT LOG RETENTION DAYS**、**MAX FILE SIZE** 和 **TOTAL AUDIT LOG SIZE** 字段中的值决定。当审核日志备份的大小达到 **TOTAL AUDIT LOG SIZE** 中配置的值时，将删除最先归档的文件。这意味着最旧的文件将被删除。但该文件条目在数据库中仍然可用，并被标记为“`Rollover Delete`”。**AUDIT LOG RETENTION DAYS** 值用于指定

保留审核日志文件的天数。任何早于此字段中设置值的文件都将被滚动。

步骤

1. 单击*审核日志* > > 配置。
2. 在*最大文件大小*、*总审计日志大小*和*审计日志保留天数*中输入值。

   要启用远程日志记录，请选择*启用远程日志记录*。

在 **Active IQ Unified Manager** 中启用审计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 Syslog 服务器。这使您能够在受到空间限制时管理审核日志。

审核日志的远程日志记录提供了防篡改备份，以防 Active IQ Unified Manager 服务器上的审核日志文件被篡改。

步骤

1. 在*配置审计日志*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*主机名*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共证书。

   证书应以 `.pem`格式上传。此证书应从目标 `Syslog` 服务器获取且不应过期。证书应包含选定的“`hostname`” 作为 `SubjectAltName` （SAN）属性的一部分。

4. 输入以下字段的值：**CHARSET**、**CONNECTION TIMEOUT**、**RECONNECTION DELAY**。

   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 Syslog 格式和 TLS 协议版本。
6. 如果目标 Syslog 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 Syslog 服务器，否则连接将失败。根据 Syslog 服务器的类型，可能需要创建客户端身份验证证书的哈希。

   示例：syslog-ng 需要使用命令 `openssl x509 -noout -hash -in cert.pem` 创建证书的 <hash>，然后您应将客户端身份验证证书符号链接到以 <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。

   您将被重定向至“审核日志”页面。

*连接超时*值可能会影响配置。如果配置的响应时间长于定义的值，则可能由于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。

使用 **Active IQ Unified Manager** 中的远程身份验证页面

您可以使用“远程身份验证”页面配置 Unified Manager 与您的身份验证服务器进行通信，以对尝试登录到 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，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

  使您能够配置管理服务器，以便在目录服务提供程序（如 Active Directory、OpenLDAP）中对用户进行身份验证，或者指定您自己的身份验证机制。仅当启用了远程身份验证时，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。

    - 密码

      指定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是 ou@domain.com，则基本可分辨名称是 **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

      指定与基本可分辨名称一起使用的绑定可分辨名称，以在身份验证服务器中查找远程用户。

    - 绑定密码

      指定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是 ou@domain.com，则基本可分辨名称是 **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 bind 可分辨名称，以在已配置的身份验证服务器中查找远程用户。

- 绑定密码

  指定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是 ou@domain.com，则基本可分辨名称是 **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的名称。

- 组成员资格属性

  指定一个值，该值基于用户身份验证服务器中指定的属性和值将管理服务器组成员身份分配给远程用户。

- UGID

  如果远程用户作为 GroupOfUniqueNames 对象的成员包含在身份验证服务器中，则此选项使您能够根据该 GroupOfUniqueNames 对象中的指定属性将管理服务器组成员身份分配给远程用户。

- 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个别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 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，请确保删除所有现有的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和对远程用户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

  允许您添加、编辑或删除身份验证服务器。

  - 添加

    允许您添加身份验证服务器。

  如果要添加的身份验证服务器是高可用性对的一部分（使用相同的数据库），则还可以添加伙伴身份验证服务器。这使管理服务器能够在其中一个身份验证服务器无法访问时与伙伴通信。

  - 编辑

    允许您编辑所选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

  显示用于对管理服务器上的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。

  在测试期间，如果仅指定用户名，则管理服务器会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。

  如果禁用远程身份验证，则无法测试身份验证。

管理安全证书

在 **Active IQ Unified Manager** 中查看 **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。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

查看证书使您能够验证重新生成的证书的内容，或查看可以从中访问 Unified Manager 的使用者备用名称（SAN）。

步骤

1. 在左侧导航窗格中，单击 常规 > **HTTPS** 证书。

   此时 HTTPS 证书将显示在页面顶部。

如果您需要查看比 HTTPS 证书页面上显示的更详细的安全证书信息，则可以在浏览器中查看连接证书。

在 **Active IQ Unified Manager** 中下载 **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，以便将该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。

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 > **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以签名，然后安装签名证书。

在 **Active IQ Unified Manager** 中安装 **CA** 签名的 **HTTPS** 证书

您可以在证书颁发机构签名并返回安全证书之后上传并安装它。您上传和安装的文件必须是签名版本的现有自签名证书。CA 签名证书有助于避免受到中间人攻击，且可提供比自签名证书更好的安全保护。

*什么 .开始之前

您必须已完成以下操作：

- 下载证书签名请求文件并由证书颁发机构签名
- 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。

如果为其创建 CSR 的证书的有效期超过 397 天，则 CA 将在签署并返回证书之前将其有效期缩短至 397 天

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……*以查找要上传的文件。
4. 选择文件，然后单击*安装*以安装文件。

   有关信息，请参见 "安装使用外部工具生成的 HTTPS 证书"。

示例证书链

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-----
```

了解在 **Active IQ Unified Manager Unified Manager** 中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 、LetsEncrypt 等外部工具生成的。

您应该将私钥与证书链一起加载，因为这些证书是外部生成的公钥-私钥对。允许的密钥对算法是“RSA”和“EC”。安装 **HTTPS** 证书 选项在常规部分下的 HTTPS 证书页面中提供。您上传的文件应采用以下输入格式。

1. Active IQ Unified Manager 主机所属服务器的私钥
2. 与私钥匹配的服务器证书
3. 反向直至根证书的 CA 证书，用于签署上述证书

使用 **EC** 密钥对加载证书的格式

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 密钥对的允许密钥大小为 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的检查

系统在上传使用外部工具生成的证书时会执行检查。如果任何检查失败，则证书将被拒绝。此外，还包括对从产品内的 CSR 生成的证书以及使用外部工具生成的证书的验证。

- 输入中的私钥将根据输入中的主机证书进行验证。
- 根据主机的 FQDN 检查主机证书中的通用名称（CN）。
- 主机证书的公用名称（CN）不应为空或空白，也不应设置为 localhost。
- 有效期开始日期不应为将来日期，证书的有效期到期日期不应为过去日期。
- 如果存在中间 CA 或 CA，则证书的有效期开始日期不应在未来，有效期到期日期不应在过去。

输入中的私钥不应加密。如果存在任何已加密的私钥，则会被系统拒绝。

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-----
```

如果证书安装失败，请参阅知识库 (KB) 文章：https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager 无法安装外部生成的证书"^]

证书管理的页面描述

了解 **Active IQ Unified Manager** 中的 **HTTPS** 证书页面

可使用 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就是在安装过程中生成的证书。

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 证书的证书请求。您的浏览器会提示您保存 <hostname>.csr 文件，以便您可以将该文件提供给证书颁发机构进行签名。

- 安装 **HTTPS** 证书

  使您能够在证书颁发机构签名并返回后上传和安装安全证书。重新启动管理服务器后，新证书即生效。

- 重新生成 **HTTPS** 证书

  使您能够生成新的自签名 HTTPS 证书，以替换当前的安全证书。重新启动 Unified Manager 后，新证书即生效。

在 **Active IQ Unified Manager** 中重新生成 **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。

此页面上将显示当前证书信息。

“使用当前证书属性重新生成”和“更新当前证书属性”选项使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。

- 通用名称

  必需。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。通常是公司的法定名称。

- 部门

  可选。公司部门名称。

- 城市

  可选。公司所在的城市位置。

- **State**

  可选。公司所在的州或省/自治区/直辖市位置（非缩写）。

- 国家/地区

  可选。公司所在的国家/地区位置。这通常是指国家/地区的两个字母的 ISO 代码。

- 备用名称

  必需。除了现有本地主机或其他网络地址以外，还可以使用其他非主域名来访问此服务器。每个替换名称均使用英文逗号进行分隔。

  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.g. localhost)” 复选框。选中此复选框时，仅在“备用名称”字段中使用您在该字段中输入的内容。留空时，生成的证书将完全没有“备用名称”字段。

- 密钥大小（密钥算法：**RSA**）

  密钥算法设置为 RSA。您可以选择一种密钥大小：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。如果您已从早期版本升级，您可能会看到以前的证书有效期保持不变。

有关详细信息，请参见"生成 HTTPS 证书"。

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。