执行配置和管理任务

Active IQ Unified Manager 9.8

NetApp
August 02, 2024

目录

执行配置和管理任务

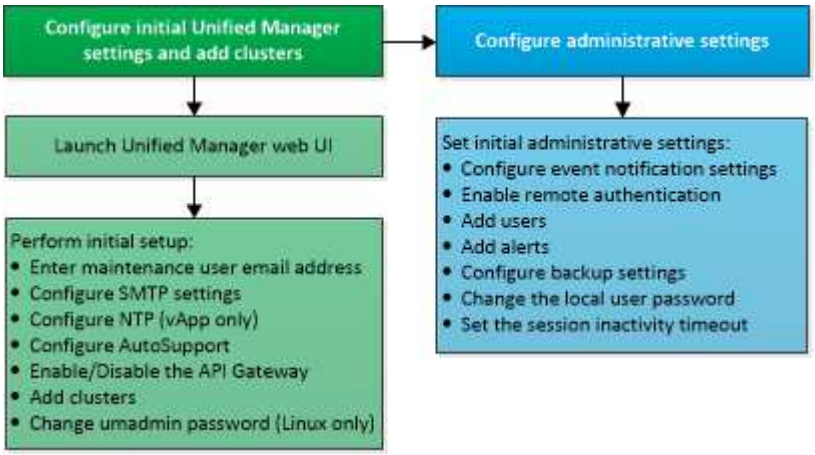
正在配置 **Active IQ Unified Manager**

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。

开始之前

- 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 。

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。

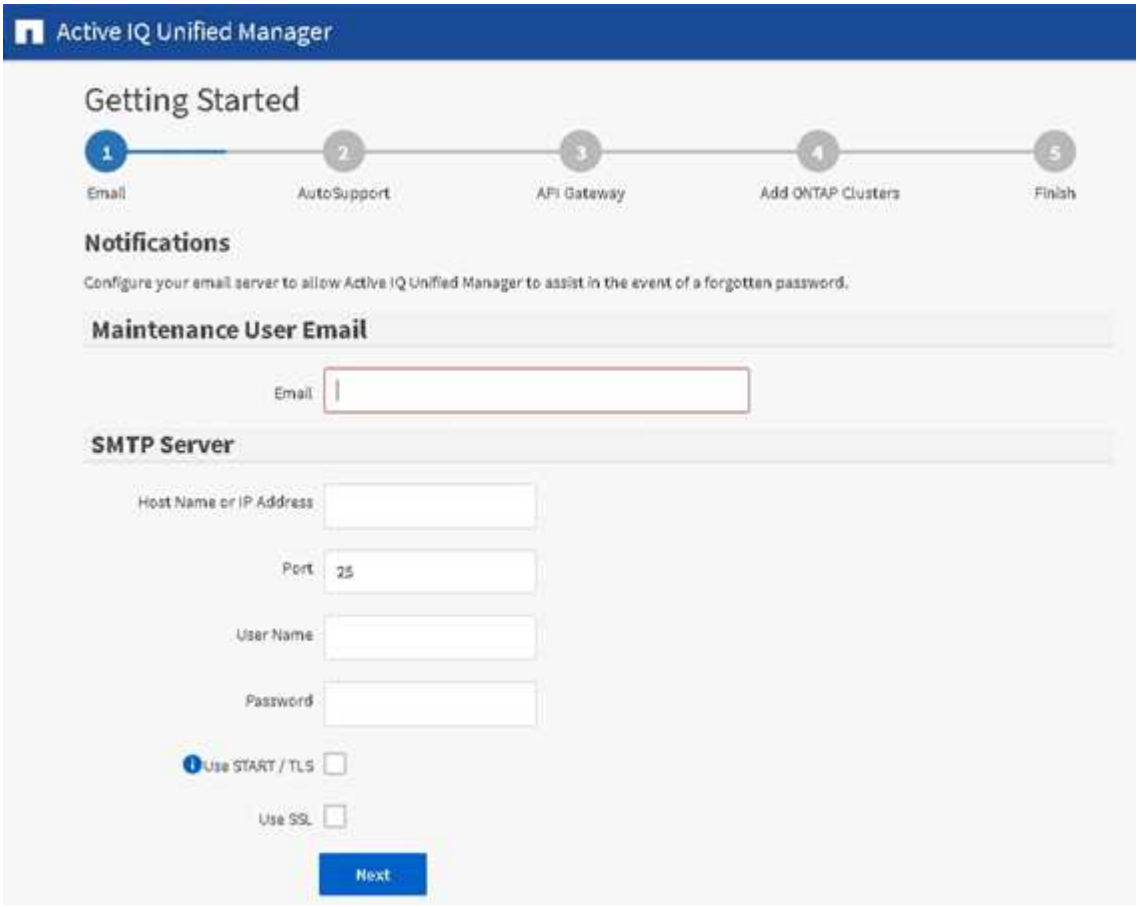
开始之前

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

关于此任务

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 * 。
2. 在* AutoSupport *页面中、单击*同意并继续*以启用从Unified Manager向AutoSupport IQ发送消息的功能。

   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、您可以将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、以使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*。

结果

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。

开始之前

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

    主机名是 Unified Manager 用于连接到集群的 FQDN 或简称。主机名必须解析为集群管理 IP 地址。

    集群管理 IP 地址必须是管理 Storage Virtual Machine （ SVM ）的集群管理 LIF 。如果使用节点管理 LIF ，则操作将失败。
  - 集群必须运行 ONTAP 9.1 或更高版本的软件。
  - ONTAP 管理员用户名和密码

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

◦ 使用 HTTPS 协议连接到集群的端口号（通常为端口 443 ）

您可以使用 Unified Manager NAT IP 地址添加位于 NAT/ 防火墙后面的集群。任何已连接的 Workflow Automation 或 SnapProtect 系统也必须位于 NAT/ 防火墙后面， SnapProtect API 调用必须使用 NAT IP 地址来标识集群。

- 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。

关于此任务

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。

您可以通过两个 Unified Manager 实例监控一个集群，但前提是您已在集群上配置了另一个集群管理 LIF ，以便 Unified Manager 的每个实例都通过不同的 LIF 进行连接。

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 * 。

   只有在首次添加集群时， Unified Manager 才会检查证书。Unified Manager 不会检查对 ONTAP 的每次 API 调用的证书。

   如果证书已过期、则无法添加新集群。您必须先续订SSL证书、然后再添加集群。

结果

发现新集群的所有对象(大约15分钟)后、Unified Manager将开始收集前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。

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。

开始之前

您必须具有应用程序管理员角色。

关于此任务

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。

开始之前

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、配置相应的设置并单击*保存*。
   - 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。

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。

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）。

关于此任务

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. 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。

开始之前

- 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。

关于此任务

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 * 。

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 。

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
- 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。

关于此任务

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。

如果您要 ...	然后执行此操作 ...
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。

开始之前

- 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。

关于此任务

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。

添加用户

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

开始之前

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

  启用 SAML 身份验证后，类型为 "`local` " 或 " m维护 " 的用户不允许访问此 UI 。

关于此任务

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

步骤

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

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

4. 单击 * 添加 * 。

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。

开始之前

- 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。

关于此任务

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 * 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 * ，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、一个"`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：

1. 单击*名称*、然后输入 `HealthTest` 在*警报名称*字段中。
2. 单击 * 资源 * ，然后在包括选项卡中，从下拉列表中选择 * 卷 * 。
   a. 输入 … `abc` 在*名称包含*字段中、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*、然后输入 `xyz` 在*名称包含*字段中、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 * 。

自动添加到 **Unified Manager** 的 **EMS** 事件

以下 ONTAP EMS 事件将自动添加到 Unified Manager 中。如果在 Unified Manager 监控的任何集群上触发这些事件，则会生成这些事件。

在监控运行 ONTAP 9.5 或更高版本软件的集群时，可以使用以下 EMS 事件：

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**Unified Manager** 严重性
聚合重新定位时，云层访问被拒绝	arl.netra.ca.check.failed	聚合	error
在存储故障转移期间，用于聚合重新定位的云层访问被拒绝	gb.netra.ca.check.failed	聚合	error
FabricPool 镜像复制重新同步已完成	wafl.ca.resync.complete	集群	error
FabricPool 空间接近全满	fabricpool.nNearly.full	集群	error
NVMe-oF 宽限期已开始	nvmf.graceperiod.start	集群	警告
NVMe-oF 宽限期处于活动状态	nvmf.graceperiod.active	集群	警告
NVMe-oF 宽限期已过期	nvmf.graceperiod.expired	集群	警告
LUN 已销毁	lun.destroy	LUN	信息
Cloud AWS MetaDataConnFail	cloud 。aws.metadataConnFail	Node	error
Cloud AWS IAMCredsExpired	cloud 。aws.iamCredsExpire	Node	error
Cloud AWS IAMCredsInvalid	cloud 。aws.iamCredsInvalid	Node	error

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**Unified Manager** 严重性
Cloud AWS IAMCredsNotFound	cloud 。 aws.iamCredsNotFound	Node	error
Cloud AWS IAMCredsNotInitialized	cloud 。 aws.iamNotInitialized	Node	信息
Cloud AWS IAMRoleInvalid	cloud 。 aws.iamRoleInvalid	Node	error
Cloud AWS IAMRoleNotFound	cloud 。 aws.iamRoleNotFound	Node	error
无法解析云层主机	objstore.host.unresolvable	Node	error
云层集群间 LIF 已关闭	objstore.interclusterlifDown	Node	error
请求不匹配云层签名	OSC.signatureMismatch	Node	error
其中一个 NFSv4 池已用尽	nblade.nfsV4PoolExhaust	Node	严重
QoS 监控内存已达到上限	qos.monitor.memory.maxed	Node	error
QoS 监控器内存已减少	qos.monitor.memory.abated	Node	信息
NVMeNS 销毁	NVMeNS.destroy	命名空间	信息
NVMeNS Online	NVmeNS.offline	命名空间	信息
NVMeNS 脱机	NVmeNS.online	命名空间	信息
NVMeNS 空间不足	nvmens.out 。 space	命名空间	警告
同步复制不同步	sms.status.out	SnapMirror 关系	警告
同步复制已还原	sms.status.in.sync	SnapMirror 关系	信息
同步复制自动重新同步失败	sms.resync.Attempt.failed	SnapMirror 关系	error

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**Unified Manager** 严重性
多个 CIFS 连接	nblade.cifsManyAss	SVM	error
已超过最大 CIFS 连接数	nblade.cifsMaxOpenSameFile	SVM	error
已超过每个用户的最大 CIFS 连接数	nblade.cifsMaxSessPerUsrConn	SVM	error
CIFS NetBIOS 名称冲突	nblade.cifsNbNameConflict	SVM	error
尝试连接不存在的 CIFS 共享	nblade.cifsNoPrivShare	SVM	严重
CIFS 卷影复制操作失败	CIFS.ShadowCopy.Failure	SVM	error
AV 服务器发现病毒	已检测 Nblade.vscanVirusDetened.	SVM	error
没有用于病毒扫描的 AV 服务器连接	nblade.vscanNoScannerConn	SVM	严重
未注册 AV 服务器	nblade.vscanNoRegd扫描程序	SVM	error
AV 服务器连接无响应	nblade.vscanConnInactive.	SVM	信息
AV 服务器太忙，无法接受新扫描请求	nblade.vscanConnBackPressure	SVM	error
未经授权的用户尝试访问 AV 服务器	nblade.vscanBadUserPrivAccess	SVM	error
FlexGroup 成分卷存在空间问题	flexgroup.constitutions.have .space.issues	Volume	error
FlexGroup 成分卷空间状态一切正常	flexgroup.constitutions.space.status.all.ok	Volume	信息
FlexGroup 成分卷存在索引节点问题	flexgroup.constituents.have.inodes.issues	Volume	error

Unified Manager 事件名称	EMS 事件名称	受影响的资源	Unified Manager 严重性
FlexGroup 成分卷索引节点状态一切正常	flexgroup.constituents.inodes.status.all.ok	Volume	信息
卷逻辑空间接近全满	monitor.vol.nearFull.inc.sav	Volume	警告
卷逻辑空间已满	monitor.vol.full.inc.sav	Volume	error
卷逻辑空间正常	monitor.vol.one.ok.inc.sav	Volume	信息
WAFL 卷自动调整大小失败	wafl.vol.autoSize.fail	Volume	error
WAFL 卷自动调整大小已完成	wafl.vol.autoSize.done	Volume	信息
WAFL READDIR 文件操作超时	wafl.readdir.expired.	Volume	error

订阅 ONTAP EMS 事件

您可以订阅接收由安装了 ONTAP 软件的系统生成的事件管理系统（ EMS ）事件。系统会自动向 Unified Manager 报告一部分 EMS 事件，但只有在订阅这些事件后，才会报告其他 EMS 事件。

开始之前

请勿订阅已自动添加到 Unified Manager 的 EMS 事件，因为这可能会在收到同一问题描述的两个事件时造成发生原因混淆。

关于此任务

您可以订阅任意数量的 EMS 事件。您订阅的所有事件都会经过验证，并且只有经过验证的事件才会应用于您在 Unified Manager 中监控的集群。_EMS ONTAP 9 事件目录 _ 提供指定版本 ONTAP 9 软件的所有 EMS 消息的详细信息。有关适用事件的列表，请从 ONTAP 9 产品文档页面找到 _EMS 事件目录 _ 的相应版本。

"ONTAP 9 产品库"

您可以为订阅的 ONTAP EMS 事件配置警报，也可以为这些事件创建要执行的自定义脚本。

如果您未收到订阅的 ONTAP EMS 事件，则可能存在具有集群 DNS 配置的问题描述，从而阻止集群访问 Unified Manager 服务器。要解决此问题描述，集群管理员必须更正集群的 DNS 配置，然后重新启动 Unified Manager 。这样做会将待定 EMS 事件刷新到 Unified Manager 服务器。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 事件设置 * 。
2. 在*事件设置*页面中、单击*订阅EMS事件*按钮。
3. 在*订阅EMS事件*对话框中、输入要订阅的ONTAP EMS事件的名称。

   要查看可订阅的EMS事件的名称、可以从ONTAP 集群Shell使用 `event route show` 命令(ONTAP 9之前的版本)或 `event catalog show` 命令(ONTAP 9或更高版本)。

   "如何在OnCommand Unified Manager-/ Active IQ Unified Manager 中配置ONTAP EMS事件订阅"

4. 单击 * 添加 * 。

   EMS 事件将添加到 " 已订阅 EMS 事件 " 列表中，但 " 适用于集群 " 列会将您添加的 EMS 事件的状态显示为 "`未知` " 。

5. 单击 * 保存并关闭 * 向集群注册 EMS 事件订阅。
6. 再次单击 * 订阅 EMS 事件 * 。

   对于您添加的 EMS 事件，状态 "`是` " 将显示在 " 适用于集群 " 列中。

   如果状态不是 "`是` " ，请检查 ONTAP EMS 事件名称的拼写。如果输入的名称不正确，则必须删除不正确的事件，然后重新添加此事件。

完成后

发生 ONTAP EMS 事件时，事件将显示在事件页面上。您可以选择事件以在事件详细信息页面中查看有关 EMS 事件的详细信息。您还可以管理事件的处理方式或为事件创建警报。

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。

开始之前

- 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。

关于此任务

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。

结果

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。

完成后

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。

配置数据库转储备份的目标和计划

您可以配置 Unified Manager 数据库转储备份设置，以设置数据库备份路径，保留数量和备份计划。您可以启用每日或每周计划备份。默认情况下，计划的备份处于禁用状态，但您应设置备份计划。

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。
- 在定义为备份路径的位置中，必须至少有 150 GB 的可用空间。

  建议使用 Unified Manager 主机系统外部的远程位置。

- 如果Unified Manager安装在Linux系统上、请验证"`jboss`"用户是否具有对备份目录的写入权限。
- 在Unified Manager收集15天的历史性能数据时、您不应计划在添加新集群后立即执行备份操作。

关于此任务

与后续备份相比，首次执行备份所需的时间要多，因为第一次备份是完整备份。完整备份可能超过 1 GB ，并且可能需要三到四个小时。后续备份是增量备份，所需时间更短。

如果您发现增量备份文件的数量过大，无法容纳为备份分配的空间，则可以定期创建新的完整备份，以替换旧的完整备份及其所有子增量文件。另外，如果 Unified Manager 安装在 Linux 系统上，则您可能需要开始使用 NetApp Snapshot 备份方法。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 数据库备份 * 。
2. 在 * 数据库备份 * 页面中，单击 * 备份设置 * 。
3. 为备份路径，保留数量和计划配置适当的值。

   保留数量的默认值为 10 ；您可以使用 0 创建无限备份。

4. 选择 * 计划每日 * 或 * 计划每周 * 按钮，然后指定计划详细信息。
5. 单击 * 应用 * 。

结果

数据库转储备份文件会根据计划创建。您可以在数据库备份页面中查看可用的备份文件。

- 相关信息 *

"如何在Active IQ Unified Manager 中启动新的增量备份链"

更改本地用户密码

您可以更改本地用户登录密码，以防止潜在的安全风险。

开始之前

您必须以本地用户身份登录。

关于此任务

维护用户和远程用户的密码不能使用以下步骤进行更改。要更改远程用户密码，请与密码管理员联系。要更改维护用户密码、请参见《Active IQ Unified Manager 系统配置指南》中有关"`使用维护控制台`"的章节。

步骤

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

   如果您是远程用户，则不会显示 * 更改密码 * 选项。

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

完成后

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

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）。

开始之前

您必须具有应用程序管理员角色。

关于此任务

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。

开始之前

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。

关于此任务

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

您可能会出于多种原因生成新的HTTPS安全证书、包括您希望使用其他证书颁发机构进行签名还是当前安全证书已过期。新证书将替换现有证书。

开始之前

您必须具有应用程序管理员角色。

关于此任务

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。

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。其他字段不需要值、但您可以为"城市"、"省/自治区/直辖市"和"国家/地区"输入值、以便在证书中填充这些值。 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"`exclude local Identifying information (e.g.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。

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。

完成后

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。

开始之前

虚拟设备已启动。

您以维护用户身份登录到维护控制台。

关于此任务

您也可以使用"*重新启动子系统"*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。

开始之前

您必须对安装了 Unified Manager 的 Linux 系统具有 root 用户访问权限。

关于此任务

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。

开始之前

您必须具有应用程序管理员角色。

关于此任务

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。

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。

开始之前

您必须已安装并配置 Unified Manager 。

关于此任务

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。

开始之前

- 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 ）
- 支持 / 诊断
- 重置服务器证书
- 外部数据提供程序
- 性能轮询间隔配置

网络配置菜单

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 ）。

- * 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。

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。

- * 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 。

- * 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。

开始之前

- 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 。

开始之前

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。

关于此任务

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。

步骤

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。

结果

完成此更改后，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 。

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。

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。

关于此任务

> 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。

开始之前

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。

关于此任务

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` 用于设置备份目录的SE Linux类型的命令： `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命令或添加额外磁盘将目录设置为至少750 GB。

   挂载 `/opt/netapp/data` 不支持NFS或CIFS共享上的目录。

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
```

1. 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
   ```

2. 删除文件 `abc` 这样、此无关文件将来不发生原因 会出现数据库错误。

3. 从复制内容 `backup-data` 返回到展开的 `/opt/netapp/data` 目录： `cp -arp /backup-data/* /opt/netapp/data/`

4. 如果启用了 SE Linux ，请运行以下命令： `chcon -R --type=mysqld_db_t /opt/netapp/data`

5. 启动 MySQL 服务： `systemctl start mysqld`
6. 启动 MySQL 服务后，按所示顺序启动 ocie 和 ocieau 服务： `systemctl start ocie ocieau`
7. 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。

开始之前

- 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。

关于此任务

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，为 * 系统配置 * 选项输入数字。
5. 在 * 系统配置菜单 * 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。

开始之前

您必须具有 Windows 管理员权限。

关于此任务

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"