正在配置Unified Manager

OnCommand Unified Manager 9.5

NetApp
December 20, 2023

目录

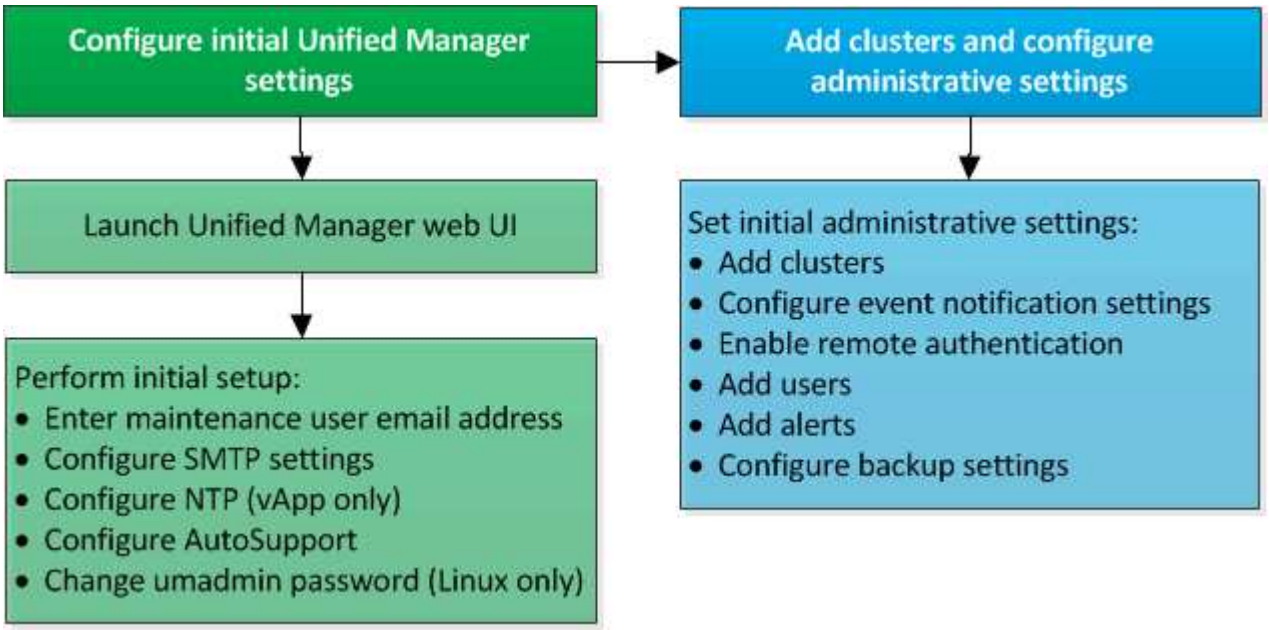
正在配置Unified Manager

安装Unified Manager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以及SMTP服务器主机名和选项。

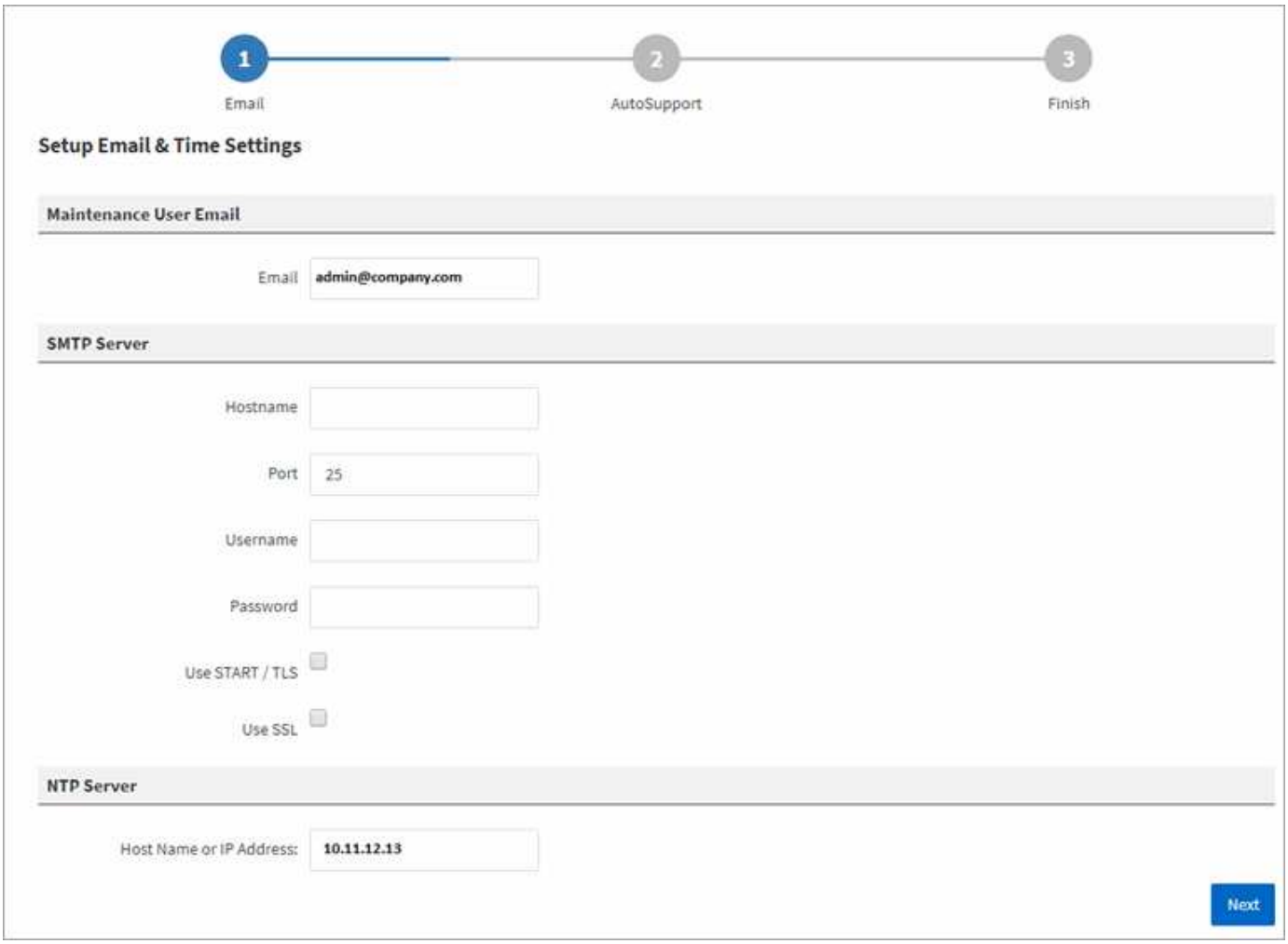
开始之前

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OnCommand 统一管理器Web UI时、才会显示"Unified Manager初始设置"页面。以下页面来自VMware 上的安装。



如果稍后要更改其中任何选项、您可以使用管理选项、单击*即可访问这些选项*。

步骤

1. 在* OnCommand Unified Manager初始设置*窗口中、输入维护用户电子邮件地址、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 * 下一步 * 。
2. 在*同意并继续*页面中、单击*同意并继续*以启用AutoSupport AutoSupport。

   如果您需要指定一个代理来提供Internet访问、以便向支持部门发送AutoSupport 内容、或者要禁用AutoSupport 、请使用管理选项。

3. 在Red Hat和CentOS系统上、您可以选择将umadmin用户密码从默认的"`admin`"字符串更改为个性化字符串。

结果

此时将关闭初始设置窗口、并显示Unified Manager Web UI。此时将显示配置/集群数据源页面、以便您可以向系统添加集群。

添加集群

您可以将集群添加到OnCommand 统一管理器中、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OnCommand 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。

  - Data 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* 。

  - 可以在集群上配置的协议类型(HTTP或HTTPS)以及用于连接到集群的端口号

    > 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 FQDN必须能够对ONTAP 系统执行ping操作。

  您可以使用以下ONTAP 命令验证此问题： `ping -node node_name -destination Unified_Manager_FQDN`。

- 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*配置*>*集群数据源*。
2. 在*配置/集群数据源*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、通信协议和端口号。

   默认情况下、HTTPS协议和端口443处于选中状态。

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. 如果选择 HTTPS ，请执行以下步骤：
   a. 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。
   b. 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，请检查是否存在以下问题：

- 如果两个系统上的时钟未同步，并且 Unified Manager HTTPS 证书开始日期晚于集群上的日期。您必须确保时钟使用 NTP 或类似服务进行同步。
- 如果集群已达到 EMS 通知目标的最大数量，则无法添加 Unified Manager 地址。默认情况下，只能在集群上定义 20 个 EMS 通知目标。

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OnCommand 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
- SNMP版本、陷阱目标主机IP地址、出站陷阱端口以及用于配置SNMP陷阱的社区

您必须具有OnCommand 管理员或存储管理员角色。

步骤

1. 在工具栏中、单击*⚙、然后单击左侧设置菜单中的*通知。
2. 在*设置/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"`OnCommand@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OnCommand 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. 在工具栏中、单击*⚙、然后单击左侧设置菜单中的*身份验证。
2. 在*设置/身份验证*页面中、选择*启用远程身份验证*。
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）

身份验证类型 ...	输入以下信息 ...
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 * 保存并关闭 * 。

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OnCommand 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. 在工具栏中、单击*、然后单击左侧设置菜单中的*身份验证。
2. 在*设置/身份验证*页面中、选中*禁用嵌套组查找*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OnCommand 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. 在工具栏中、单击*、然后单击左侧设置菜单中的*身份验证。
2. 在*设置/身份验证*页面中、单击*管理服务器*>*身份验证*。
3. 启用或禁用*使用安全连接身份验证*选项：

如果您要 ...	然后执行此操作 ...
启用它	a. 在启用远程身份验证复选框中、选择*使用安全连接*选项。 b. 在身份验证服务器区域中，单击 * 添加 * 。 c. 在添加身份验证服务器对话框中，输入服务器的身份验证名称或 IP 地址（ IPv4 或 IPv6 ）。 d. 在授权主机对话框中，单击查看证书。 e. 在查看证书对话框中，验证证书信息，然后单击 * 关闭 * 。 f. 在 Authorize Host 对话框中，单击 * 是 * 。 启用 * 使用安全连接身份验证 * 选项后， Unified Manager 将与身份验证服务器通信并显示证书。Unified Manager 使用 636 作为安全通信的默认端口，使用端口号 389 进行非安全通信。
请将其禁用	a. 在启用远程身份验证复选框中、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。

4. 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OnCommand 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. 在工具栏中、单击*⚙、然后单击左侧设置菜单中的*身份验证。
2. 在*设置/身份验证*页面中、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

您可以使用管理/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OnCommand 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. 在工具栏中、单击*、然后单击左侧管理菜单中的*用户。
2. 在*管理/Users*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、以便Unified Manager服务器能够使用这些设置在生成事件时向用户发送通知。
- 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、则必须已使用管理/脚本页面将脚本添加到Unified Manager中。
- 您必须具有OnCommand 管理员或存储管理员角色。

关于此任务

除了从配置/警报页面创建警报之外、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、如下所述。

步骤

1. 在左侧导航窗格中、单击*配置*>*警报*。
2. 在*配置/警报*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"管理/用户"页面修改了选定用户的电子邮件地址、则修改后的电子邮件地址不会针对选定用户进行更新。

   您也可以选择通过 SNMP 陷阱通知用户。

7. 单击 * 保存 * 。

添加警报的示例

此示例显示了如何创建满足以下要求的警报：

- 警报名称： HealthTest
- 资源：包括名称包含 "`abc` " 的所有卷，并排除名称包含 "`xyz` " 的所有卷
- 事件：包括所有严重运行状况事件
- 操作：包括"`sample@domain.com`"、"`Test`"脚本、必须每15分钟通知一次用户

在添加警报对话框中执行以下步骤：

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. 从"Available Resources"区域中选择*\<Resources>*<All Volumes whose name contains 'abc'> 、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*、然后输入 `sample@domain.com` 在向这些用户发送警报字段中。
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. 在选择要执行的脚本菜单中、选择*测试*脚本。
8. 单击 * 保存 * 。

自动添加到 Unified Manager 的 EMS 事件

使用Unified Manager 9.4或更高版本的软件时、以下ONTAP EMS事件会自动添加到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	**ONTAP** 严重性
用于聚合重新定位的对象存储访问被拒绝	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对象存储访问被拒绝	gb.netra.ca.check.failed	聚合	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
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

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**ONTAP** 严重性
Cloud AWS IAMRoleNotFound	cloud 。 aws.iamRoleNotFound	Node	error
Objstore主机无法解析	objstore.host.unresolvable	Node	error
对象存储集群间生命周期	objstore.interclusterlifDown	Node	error
请求与对象存储签名不匹配	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
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

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**ONTAP** 严重性
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
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.近 全	Volume	警告
卷逻辑空间已满	monitor.vol.full	Volume	error

Unified Manager 事件名称	EMS 事件名称	受影响的资源	ONTAP 严重性
卷逻辑空间正常	monitor.vol.one.ok	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

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*配置*>*管理事件*。
2. 在*配置/管理事件*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`"、否则用户在使用Internet Explorer时从Unified Manager注销时可能会收到错误。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：

    http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/

  - 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。
- 当用户尝试使用Internet Explorer访问Unified Manager时、他们可能会看到消息*网站无法显示页面*。如果发生这种情况、请确保这些用户取消选中*工具*>* Internet选项*>*高级*中的`SHTTP错误消息友好程度`选项。

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。
- 您必须已创建至少一个具有OnCommand 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. 在工具栏中、单击*⚙、然后单击左侧设置菜单中的*身份验证。
2. 在*设置/身份验证*页面中、选择* SAML身份验证*选项卡。
3. 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。

4. 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。

5. 复制 Unified Manager 主机元数据 URI ，或者将主机元数据保存到 XML 文本文件中。

   此时，您可以使用此信息配置 IdP 服务器。

6. 单击 * 保存 * 。

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

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

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。在Windows、Red Hat或CentOS上部署Unified Manager时、您可以使用以下Unified Manager命令行界面命令更改GUI会话超时： `um option set absolute.session.timeout=00:15:00`此命令会将Unified Manager GUI会话超时设置为15分钟。

配置数据库备份设置

您可以配置Unified Manager数据库备份设置、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。

开始之前

- 您必须具有操作员、OnCommand 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。

步骤

1. 在工具栏中、单击*⚙、然后单击*管理>*数据库备份*。
2. 在*管理/数据库备份*页面中、单击*操作*>*数据库备份设置*。
3. 为备份路径和保留数量配置适当的值。

   保留数量的默认值为 10 ；您可以使用 0 创建无限备份。

4. 在*计划频率*部分中、选中*启用*复选框、然后指定每日或每周计划。
   - * 每日 *

     如果选择此选项、则必须以24小时格式输入时间以创建备份。例如、如果指定18：30、则每天下午6：30创建一个备份。

   - * 每周 *

     如果选择此选项、则必须指定创建备份的时间和日期。例如、如果将日期指定为星期一、时间指定为16：30、则每周一下午4：30将创建每周备份。

5. 单击 * 保存并关闭 * 。

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 "使用维护控制台"。

步骤

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

   如果您是远程用户，则不会显示 * 更改密码 * 选项。

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

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。

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OnCommand 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。如果未正确配置DHCP或OnCommand 、则会自动分配主机名"`DHCP`"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OnCommand 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. 在工具栏中、单击*⚙、然后单击*设置*菜单中的 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	`Click the *Update the Current Certificate Attributes* option.` 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

此外、您还可以使用"**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. 按所示顺序输入以下命令、以停止Unified Manager软件和关联的MySQL软件：
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、按所示顺序输入以下命令以重新启动Unified Manager：