配置 Unified Manager 以发送警报通知

Active IQ Unified Manager 9.10

NetApp
December 18, 2023

目录

配置 Unified Manager 以发送警报通知

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

- 您需要的内容 *

您必须具有应用程序管理员角色。

在部署 Unified Manager 并完成初始配置后，您应考虑将环境配置为触发警报，并根据收到的事件生成通知电子邮件或 SNMP 陷阱。

步骤

1. "配置事件通知设置"

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

2. "启用远程身份验证"

   如果您希望远程 LDAP 或 Active Directory 用户访问 Unified Manager 实例并接收警报通知，则必须启用远程身份验证。

3. "添加身份验证服务器"

   您可以添加身份验证服务器，以便身份验证服务器中的远程用户可以访问 Unified Manager 。

4. "添加用户"

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

5. "添加警报"

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

配置事件通知设置

您可以将 Unified Manager 配置为在生成事件或将事件分配给用户时发送警报通知。您可以配置用于发送警报的 SMTP 服务器，也可以设置各种通知机制，例如，警报通知可以通过电子邮件或 SNMP 陷阱发送。

- 您需要的内容 *

您必须具有以下信息：

- 发送警报通知的电子邮件地址

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

- 用于访问服务器的 SMTP 服务器主机名以及用户名和密码
- 要接收 SNMP 陷阱的陷阱目标主机的主机名或 IP 地址，以及 SNMP 版本，出站陷阱端口，社区和其他所需的 SNMP 配置值

  要指定多个陷阱目标，请使用逗号分隔每个主机。在这种情况下，列表中所有主机的所有其他 SNMP 设置（例如版本和出站陷阱端口）都必须相同。

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 通知 * 。
2. 在通知页面中，配置相应的设置并单击 * 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。

- 您需要的内容 *

您必须具有应用程序管理员角色。

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

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

支持通过 LDAP 和 LDAPS （安全 LDAP ）进行远程身份验证。Unified Manager 使用 389 作为非安全通信的默认端口，使用 636 作为安全通信的默认端口。

> 用于对用户进行身份验证的证书必须符合 X.509 格式。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 远程身份验证 * 。
2. 选中 * 启用远程身份验证 …* 复选框。
3. 在身份验证服务字段中，选择服务类型并配置身份验证服务。

身份验证类型 ...	输入以下信息 ...
Active Directory	• 身份验证服务器管理员名称采用以下格式之一： ◦ `domainname\username` ◦ 用户名@域名 ◦ 绑定可分辨名称 （使用适当的 LDAP 表示法） • 管理员密码 • 基本可分辨名称（使用适当的 LDAP 表示法）
打开 LDAP	• 绑定可分辨名称（采用适当的 LDAP 表示法） • 绑定密码 • 基本可分辨名称

如果 Active Directory 用户的身份验证需要很长时间或超时，则身份验证服务器可能需要很长时间才能响应。在 Unified Manager 中禁用对嵌套组的支持可能会缩短身份验证时间。

如果为身份验证服务器选择使用安全连接选项，则 Unified Manager 将使用安全套接字层（ SSL ）协议与身份验证服务器进行通信。

4. * 可选： * 添加身份验证服务器并测试身份验证。
5. 单击 * 保存 * 。

禁用远程身份验证中的嵌套组

如果启用了远程身份验证，则可以禁用嵌套组身份验证，以便只有单个用户（而不是组成员）可以远程向 Unified Manager 进行身份验证。如果要缩短 Active Directory 身份验证响应时间，可以禁用嵌套组。

- 您需要的内容 *
- 您必须具有应用程序管理员角色。
- 只有在使用 Active Directory 时，禁用嵌套组才适用。

在 Unified Manager 中禁用对嵌套组的支持可能会缩短身份验证时间。如果禁用嵌套组支持，并且将远程组添加到 Unified Manager 中，则各个用户必须是远程组的成员才能向 Unified Manager 进行身份验证。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 远程身份验证 * 。
2. 选中 * 禁用嵌套组查找 * 复选框。
3. 单击 * 保存 * 。

设置身份验证服务

通过身份验证服务，可以先对身份验证服务器中的远程用户或远程组进行身份验证，然后再为其提供对 Unified Manager 的访问权限。您可以使用预定义的身份验证服务（例如 Active Directory 或 OpenLDAP ）或配置自己的身份验证机制来对用户进行身份验证。

- 您需要的内容 *
- 您必须已启用远程身份验证。
- 您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 远程身份验证 * 。
2. 选择以下身份验证服务之一：

如果选择	然后执行此操作 ...
Active Directory	a. 输入管理员名称和密码。 b. 指定身份验证服务器的基本可分辨名称。 例如，如果身份验证服务器的域名为 +ou@domain.com + ，则基本可分辨名称为 * CN=ou ， dc=domain ， dc=com* 。
OpenLDAP	a. 输入绑定可分辨名称和绑定密码。 b. 指定身份验证服务器的基本可分辨名称。 例如，如果身份验证服务器的域名为 +ou@domain.com + ，则基本可分辨名称为 * CN=ou ， dc=domain ， dc=com* 。
其他	a. 输入绑定可分辨名称和绑定密码。 b. 指定身份验证服务器的基本可分辨名称。 例如，如果身份验证服务器的域名为 +ou@domain.com + ，则基本可分辨名称为 * CN=ou ， dc=domain ， dc=com* 。 c. 指定身份验证服务器支持的 LDAP 协议版本。 d. 输入用户名，组成员资格，用户组和成员属性。

> 如果要修改身份验证服务，必须删除任何现有的身份验证服务器，然后添加新的身份验证服务器。

3. 单击 * 保存 * 。

正在添加身份验证服务器

您可以在管理服务器上添加身份验证服务器并启用远程身份验证，以便身份验证服务器中的远程用户可以访问 Unified Manager 。

- 您需要的内容 *
- 必须提供以下信息：
  - 身份验证服务器的主机名或 IP 地址
  - 身份验证服务器的端口号
- 您必须已启用远程身份验证并配置身份验证服务，以便管理服务器能够对身份验证服务器中的远程用户或组进行身份验证。
- 您必须具有应用程序管理员角色。

如果要添加的身份验证服务器属于高可用性（ HA ）对（使用同一数据库），则还可以添加配对身份验证服务器。这样，当其中一个身份验证服务器无法访问时，管理服务器便可与配对服务器进行通信。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 远程身份验证 * 。
2. 启用或禁用 * 使用安全连接 * 选项：

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

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。

- 您需要的内容 *
- 您必须已启用远程身份验证并配置身份验证服务，以便 Unified Manager 服务器能够对远程用户或远程组进行身份验证。
- 您必须已添加身份验证服务器，以便管理服务器可以从这些服务器中搜索远程用户或远程组并对其进行身份验证。
- 您必须具有应用程序管理员角色。

如果身份验证服务设置为 Active Directory ，并且您要验证属于身份验证服务器主组的远程用户的身份验证，则身份验证结果中不会显示有关主组的信息。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 远程身份验证 * 。
2. 单击 * 测试身份验证 * 。
3. 在测试用户对话框中，指定远程用户的用户名和密码或远程组的用户名，然后单击 * 测试 * 。

   如果要对远程组进行身份验证，则不能输入密码。

正在添加警报

您可以配置警报，以便在生成特定事件时向您发出通知。您可以为单个资源，一组资源或特定严重性类型的事件配置警报。您可以指定通知频率，并将脚本与警报关联。

- 您需要的内容 *
- 您必须已配置通知设置，例如用户电子邮件地址， SMTP 服务器和 SNMP 陷阱主机，以使 Active IQ Unified Manager 服务器能够在生成事件时使用这些设置向用户发送通知。

- 您必须了解要触发警报的资源和事件，以及要通知的用户的用户名或电子邮件地址。
- 如果要根据事件执行脚本，则必须已使用脚本页面将脚本添加到 Unified Manager 中。
- 您必须具有应用程序管理员或存储管理员角色。

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

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 警报设置 * 。
2. 在 "Alert Setup" 页面中，单击 * 添加 * 。
3. 在添加警报对话框中，单击 * 名称 * ，然后输入警报的名称和问题描述。
4. 单击 * 资源 * ，然后选择要包含在警报中或从警报中排除的资源。

   您可以通过在 * 名称包含 * 字段中指定文本字符串来设置筛选器，以选择一组资源。根据您指定的文本字符串，可用资源列表仅显示与筛选器规则匹配的资源。指定的文本字符串区分大小写。

   如果某个资源同时符合您指定的包含和排除规则，则排除规则优先于包含规则，并且不会为与排除的资源相关的事件生成警报。

5. 单击 * 事件 * ，然后根据要触发警报的事件名称或事件严重性类型选择事件。

   要选择多个事件，请在选择时按 Ctrl 键。

6. 单击 * 操作 * ，然后选择要通知的用户，选择通知频率，选择是否将 SNMP 陷阱发送到陷阱接收方，并分配生成警报时要执行的脚本。

   如果修改为用户指定的电子邮件地址并重新打开警报进行编辑，则 " 名称 " 字段将显示为空，因为修改后的电子邮件地址不再映射到先前选择的用户。此外，如果您从用户页面修改了选定用户的电子邮件地址，则不会为选定用户更新修改后的电子邮件地址。

   您也可以选择通过 SNMP 陷阱通知用户。

7. 单击 * 保存 * 。

添加警报的示例

此示例显示了如何创建满足以下要求的警报：

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

在添加警报对话框中执行以下步骤：

步骤

1. 单击 * 名称 * ，然后在 * 警报名称 * 字段中输入 * 运行状况测试 * 。
2. 单击 * 资源 * ，然后在包括选项卡中，从下拉列表中选择 * 卷 * 。
   a. 在 * 名称包含 * 字段中输入 * abc* 以显示名称包含 "`abc` " 的卷。
   b. 选择 * +[All Volumes whose name contains 'abc']从 "Available Resources" 区域中选择 +* ，然后将其移动到 "Selected Resources" 区域。
   c. 单击 * 排除 * ，在 * 名称包含 * 字段中输入 * xyz* ，然后单击 * 添加 * 。
3. 单击 * 事件 * ，然后从事件严重性字段中选择 * 严重 * 。
4. 从匹配事件区域中选择 * 所有严重事件 * ，然后将其移动到选定事件区域。
5. 单击 * 操作 * ，然后在警报这些用户字段中输入 * sample@domain.com * 。
6. 选择 * 每 15 分钟提醒一次 * 以每 15 分钟通知一次用户。

   您可以将警报配置为在指定时间内向收件人重复发送通知。您应确定警报的事件通知处于活动状态的时间。

7. 在 Select Script to Execute 菜单中，选择 * 测试 * 脚本。
8. 单击 * 保存 * 。