



管理身份验证

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

目录

管理身份验证	1
编辑身份验证服务器	1
删除身份验证服务器	1
使用 Active Directory 或 OpenLDAP 进行身份验证	2
审核日志记录	2
远程身份验证页面	4

管理身份验证

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

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

编辑身份验证服务器

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

- 您需要的内容 *

您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 远程身份验证 *。
2. 选中 * 禁用嵌套组查找 * 框。
3. 在 * 身份验证服务器 * 区域中，选择要编辑的身份验证服务器，然后单击 * 编辑 *。
4. 在 * 编辑身份验证服务器 * 对话框中，编辑端口详细信息。
5. 单击 * 保存 *。

删除身份验证服务器

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

- 您需要的内容 *

您必须具有应用程序管理员角色。

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

步骤

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

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

使用 Active Directory 或 OpenLDAP 进行身份验证

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

您可以使用以下预定义的身份验证服务之一，也可以指定自己的身份验证服务：

- Microsoft Active Directory



您不能使用 Microsoft 轻型目录服务。

- OpenLDAP

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

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

审核日志记录

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

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

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

审核日志页面包含以下命令按钮：

- 配置
- 删除
- 下载

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



删除日志文件将从发生原因中删除系统中的文件，但不会删除数据库表中的条目。

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

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

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

配置审核日志

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

您可以根据要存储在系统中的所需数据量和频率设置 * 最大文件大小 * 和 * 审核日志保留天数 * 中的值。字段 * 审核日志总大小 * 中的值是系统中存在的审核日志总数据的大小。回滚策略由 * 审核日志保留天数 *，* 最大文件大小 * 和 * 审核日志总大小 * 字段中的值决定。当审核日志备份的大小达到在 * 审核日志总大小 * 中配置的值时，首先归档的文件将被删除。这意味着删除最旧的文件。但是，此文件条目在数据库中仍然可用，并标记为 "Rollover Delete"。审核日志保留天数 * 值用于保留审核日志文件的天数。超过此字段中设置的值的任何文件都会进行回滚。

步骤

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

如果要启用远程日志记录，则应选择 * 启用远程日志记录 *。

启用审核日志的远程日志记录

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

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

步骤

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

此时将显示用于配置远程日志记录的其他字段。

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

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

4. 输入以下字段的值： * 连接超时 * ， * 重新连接延迟 * 。

这些字段的值应以毫秒为单位。

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

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

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

7. 单击 * 保存 * 以配置与服务器的连接并启用远程日志记录。

您将重定向到 " 审核日志 " 页面。



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

远程身份验证页面

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

您必须具有应用程序管理员或存储管理员角色。

选中启用远程身份验证复选框后，您可以使用身份验证服务器启用远程身份验证。

- * 身份验证服务 *

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

- * Active Directory*

- 管理员名称

指定身份验证服务器的管理员名称。

- Password

指定用于访问身份验证服务器的密码。

- 基本可分辨名称

指定远程用户在身份验证服务器中的位置。例如，如果身份验证服务器的域名为 `+ou@domain.com` +，则基本可分辨名称为 `* CN=ou, dc=domain, dc=com*`。

- 禁用嵌套组查找

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

- 使用安全连接

指定用于与身份验证服务器通信的身份验证服务。

- * OpenLDAP*

- 绑定可分辨名称

指定用于在身份验证服务器中查找远程用户的绑定可分辨名称以及基本可分辨名称。

- 绑定密码

指定用于访问身份验证服务器的密码。

- 基本可分辨名称

指定远程用户在身份验证服务器中的位置。例如，如果身份验证服务器的域名为 `+ou@domain.com` +，则基本可分辨名称为 `* CN=ou, dc=domain, dc=com*`。

- 使用安全连接

指定使用安全LDAP与LDAP身份验证服务器进行通信。

- * 其他 *

- 绑定可分辨名称

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

- 绑定密码

指定用于访问身份验证服务器的密码。

- 基本可分辨名称

指定远程用户在身份验证服务器中的位置。例如，如果身份验证服务器的域名为 `+ou@domain.com` +，则基本可分辨名称为 `* CN=ou, dc=domain, dc=com*`。

- 协议版本

指定身份验证服务器支持的轻型目录访问协议（LDAP）版本。您可以指定是否必须自动检测协议

版本，或者将版本设置为 2 或 3。

- 用户名属性

指定身份验证服务器中包含要由管理服务器进行身份验证的用户登录名的属性名称。

- 组成员资格属性

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

- UGID

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

- 禁用嵌套组查找

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

- 成员

指定身份验证服务器用于存储有关组中各个成员的信息的属性名称。

- 用户对象类

指定远程身份验证服务器中用户的对象类。

- 组对象类

指定远程身份验证服务器中所有组的对象类。



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

- 使用安全连接

指定用于与身份验证服务器通信的身份验证服务。



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

身份验证服务器区域

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

- * 命令按钮 *

用于添加，编辑或删除身份验证服务器。

- 添加

用于添加身份验证服务器。

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

- 编辑

用于编辑选定身份验证服务器的设置。

- 删除

删除选定的身份验证服务器。

- * 名称或 IP 地址 *

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

- * 端口 *

显示身份验证服务器的端口号。

- * 测试身份验证 *

此按钮可通过对远程用户或组进行身份验证来验证身份验证服务器的配置。

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

如果禁用了远程身份验证，则无法测试身份验证。

版权信息

版权所有 © 2023 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。