管理身份验证

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/task_edit_authentication_servers.html on November 13, 2026. Always check docs.netapp.com for the latest.

目录

管理身份验证 . . . 1
在 Active IQ Unified Manager 中编辑身份验证服务器 . . . 1
删除 Active IQ Unified Manager 中的身份验证服务器 . . . 1
在 Active IQ Unified Manager 中使用 Active Directory 或 OpenLDAP 进行身份验证 . . . 1
审核日志记录 . . . 2
了解 Active IQ Unified Manager 中的审核日志 . . . 2
配置 Active IQ Unified Manager 审核日志 . . . 3
在 Active IQ Unified Manager 中启用审计日志的远程日志记录 . . . 3
使用 Active IQ Unified Manager 中的远程身份验证页面 . . . 4
身份验证服务器区域 . . . 6

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。

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。