



审核日志记录

Active IQ Unified Manager 9.14

NetApp
November 12, 2024

目录

审核日志记录	1
配置审核日志	2
启用审核日志的远程日志记录	2

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：

状态	说明
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 " 正常 " 或 " 被篡改 " 的文件将以压缩格式下载 .gzip。

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。

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

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

后您应将客户端身份验证证书象征性地链接到以<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。

版权信息

版权所有 © 2024 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。