审核日志记录

Active IQ Unified Manager 9.12

NetApp
December 18, 2023

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：

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中 `.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。