



管理系统日志

SANtricity 11.8

NetApp
December 16, 2024

目录

管理系统日志	1
查看审核日志活动	1
定义审核日志策略	2
从审核日志中删除事件	4
为审核日志配置系统日志服务器	4
编辑审核日志记录的系统日志服务器设置	5

管理系统日志

查看审核日志活动

通过查看审核日志、具有安全管理员权限的用户可以监控用户操作、身份验证失败、无效登录尝试以及用户会话生命周期。

开始之前

您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择"Audit Log"选项卡。

审核日志活动以表格形式显示、其中包括以下信息列：

- 日期/时间-存储阵列检测到事件的时间戳(GMT)。
 - 用户名-与事件关联的用户名。对于存储阵列上的任何未经身份验证的操作、"N/A"将显示为用户名。未经过身份验证的操作可能由内部代理或其他机制触发。
 - 状态代码—操作的HTTP状态代码(200、400等)以及与事件关联的描述性文本。
 - "已访问URL"-完整URL (包括主机)和查询字符串。
 - 客户端IP地址-与事件关联的客户端的IP地址。
 - 源—与事件关联的日志记录源、可以是System Manager、CLI、Web服务或支持Shell。
 - *问题描述 *-有关事件的追加信息、如果适用。
3. 使用审核日志页面上的选项可查看和管理事件。

选择详细信息

选择	说明
显示事件	按日期范围(过去24小时、过去7天、过去30天或自定义日期范围)显示的限制事件。
筛选器	限制按字段中输入的字符显示的事件。使用引号("")表示完全匹配的单词, 输入 `OR` 以返回一个或多个单词, 或者输入短划线(--)以省略单词。
刷新	选择*刷新*可将页面更新为最新事件。
查看/编辑设置	选择*查看/编辑设置*以打开一个对话框、在此可以指定完整的日志策略以及要记录的操作级别。
删除事件	选择*删除*以打开一个对话框、在此可以从页面中删除旧事件。
显示/隐藏列	单击*显示/隐藏*列图标  以选择要在表中显示的其他列。其他列包括: <ul style="list-style-type: none">• 方法- HTTP方法(例如POST、GET、DELETE等)。• 已执行命令行界面命令—为安全命令行界面请求执行的命令行界面命令(语法)。• 命令行界面返回状态—命令行界面状态代码或客户端请求输入文件。• *符号操作步骤 *—符号操作步骤 已执行。• * SSH事件类型*-安全Shell (SSH)事件类型、例如login、logout和login_fail。• * SSH会话PID*—SSH会话的进程ID号。• * SSH会话持续时间*-用户登录的秒数。• 身份验证类型-类型可以包括本地用户、LDAP、SAML和访问令牌。• 身份验证ID-已身份验证会话的ID。
切换列筛选器	单击*切换*图标  打开每列的过滤字段。在列字段中输入字符、以限制这些字符显示的事件。再次单击图标以关闭筛选字段。
撤消更改	单击*Undo*图标  可将表恢复为默认配置。
导出	单击*导出*将表数据保存到逗号分隔值(CSV)文件。

定义审核日志策略

您可以更改覆盖策略以及审核日志中记录的事件类型。

开始之前

您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

关于此任务

此任务介绍如何更改审核日志设置、其中包括用于覆盖旧事件的策略以及用于记录事件类型的策略。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择*审核日志*选项卡。
3. 选择*查看/编辑设置*。

此时将打开审核日志设置对话框。

4. 更改覆盖策略或记录的事件类型。

字段详细信息

设置	说明
覆盖策略	<p>确定达到最大容量时用于覆盖旧事件的策略：</p> <ul style="list-style-type: none">• 允许在审核日志已满时覆盖审核日志中最早的事件-当审核日志达到50、000条记录时覆盖旧事件。• 需要手动删除审核日志事件-指定不会自动删除事件；而是以设置的百分比显示阈值警告。必须手动删除事件。 <p> 如果禁用了覆盖策略、并且审核日志条目达到最大限制、则没有安全管理员权限的用户将无法访问System Manager。要还原没有安全管理员权限的用户的系统访问权限、分配有安全管理员角色的用户必须删除旧事件记录。</p> <p> 如果为归档审核日志配置了系统日志服务器、则覆盖策略不适用。</p>
要记录的操作级别	<p>确定要记录的事件类型：</p> <ul style="list-style-type: none">• 仅记录修改事件-仅显示用户操作涉及在系统中进行更改的事件。• 记录所有修改和只读事件-显示所有事件、包括涉及读取或下载信息的用户操作。

5. 单击 * 保存 *。

从审核日志中删除事件

您可以清除旧事件的审核日志、从而使搜索事件更易于管理。删除后、您可以选择将旧事件保存到CSV (逗号分隔值)文件中。

开始之前

您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择*审核日志*选项卡。
3. 选择 * 删除 *。

此时将打开删除审核日志对话框。

4. 选择或输入要删除的最旧事件的数量。
5. 如果要将已删除的事件导出到CSV文件(建议)、请保持选中状态。在下一步中单击*删除*时、系统将提示您输入文件名和位置。否则、如果您不想将事件保存到CSV文件、请单击复选框以取消选中它。
6. 单击 * 删除 *。

此时将打开确认对话框。

7. 键入 `delete` 字段，然后单击*Delete*。

最早的事件将从审核日志页面中删除。

为审核日志配置系统日志服务器

如果要将审核日志归档到外部系统日志服务器、则可以配置该服务器与存储阵列之间的通信。建立连接后、审核日志会自动保存到系统日志服务器。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- 系统日志服务器地址、协议和端口号必须可用。服务器地址可以是完全限定域名、IPv4地址或IPv6地址。
- 如果您的服务器使用安全协议(例如TLS)、则本地系统上必须具有证书颁发机构(CA)证书。CA证书用于标识服务器和客户端之间安全连接的网站所有者。

步骤

1. 选择菜单：设置[访问管理]。
2. 从审核日志选项卡中、选择*配置系统日志服务器*。

此时将打开配置系统日志服务器对话框。

3. 单击 * 添加 *。

此时将打开添加系统日志服务器对话框。

4. 输入服务器的信息、然后单击*添加*。

- 服务器地址-输入完全限定域名、IPv4地址或IPv6地址。
- 协议-从下拉列表选择一个协议(例如TLS、UDP或TCP)。
- 上传证书(可选)—如果您选择了TLS协议但尚未上传签名的CA证书、请单击*浏览*上传证书文件。如果没有可信证书、则不会将审核日志归档到系统日志服务器。



如果证书稍后变得无效、TLS握手将失败。因此、将向审核日志发布错误消息、并且不再向系统日志服务器发送消息。要解决此问题描述、您必须修复系统日志服务器上的证书、然后转到菜单：设置(审核日志>配置系统日志服务器>测试全部)。

- 端口-输入系统日志接收器的端口号。单击*添加*后、配置系统日志服务器对话框将打开、并在页面上显示已配置的系统日志服务器。

5. 要测试服务器与存储阵列的连接、请选择*全部测试*。

结果

配置后、所有新审核日志都会发送到系统日志服务器。不会传输先前的日志。要进一步配置警报的系统日志设置、请参见 ["为系统日志服务器配置警报"](#)。

```
NOTE: If multiple syslog servers are configured, all configured syslog servers will receive an audit log.
```

编辑审核日志记录的系统日志服务器设置

您可以更改用于归档审核日志的系统日志服务器的设置、也可以为该服务器上传新的证书颁发机构(CA)证书。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- 系统日志服务器地址、协议和端口号必须可用。服务器地址可以是完全限定域名、IPv4地址或IPv6地址。
- 如果要上传新的CA证书、则此证书必须在本地系统上可用。

步骤

1. 选择菜单：设置[访问管理]。
2. 从审核日志选项卡中、选择*配置系统日志服务器*。

已配置的系统日志服务器将显示在页面上。

3. 要编辑服务器信息、请选择服务器名称右侧的*编辑*(铅笔)图标、然后在以下字段中进行所需的更改：
 - 服务器地址-输入完全限定域名、IPv4地址或IPv6地址。
 - 协议-从下拉列表选择一个协议(例如TLS、UDP或TCP)。
 - 端口-输入系统日志接收器的端口号。

4. 如果将协议更改为安全TLS协议(从UDP或TCP)、请单击*导入可信证书*以上传CA证书。
5. 要测试与存储阵列的新连接、请选择*全部测试*。

结果

配置后、所有新审核日志都会发送到系统日志服务器。不会传输先前的日志。

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。