管理系统日志
SANtricity 11.8

NetApp
December 16, 2024

目录

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： • 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	确定达到最大容量时用于覆盖旧事件的策略： • 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。 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。 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。
要记录的操作级别	确定要记录的事件类型： • 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-从下拉列表中选择一个协议(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-从下拉列表中选择一个协议(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。