



审核日志记录 ONTAP 9

NetApp
April 24, 2024

目录

- 审核日志记录 1
 - ONTAP 如何实施审核日志记录 1
 - 对 ONTAP 9 中的审核日志记录进行的更改 1
 - 显示审核日志内容 2
 - 管理审核获取请求设置 3
 - 管理审核日志目标 3

审核日志记录

ONTAP 如何实施审核日志记录

审核日志中记录的管理活动包括在标准 AutoSupport 报告中，某些日志记录活动包括在 EMS 消息中。此外，您还可以将审核日志转发到指定的目标，并可使用命令行界面或 Web 浏览器显示审核日志文件。

从ONTAP 9.11.1开始、您可以使用System Manager显示审核日志内容。

从ONTAP 9.12.1开始、ONTAP可为审核日志提供篡改警报。ONTAP会运行每日后台作业来检查audit.log文件是否被篡改、如果发现任何已更改或篡改的日志文件、则会发送EMS警报。

ONTAP 会记录在集群上执行的管理活动，例如发出了什么请求，触发了该请求的用户，用户的访问方法以及发出请求的时间。

管理活动可以是以下类型之一：

- 设置请求、通常适用于非显示命令或操作
 - 运行时会发出这些请求 `create`，`modify``或 ``delete` 命令、例如。
 - 默认情况下，系统会记录设置请求。
- 获取请求、用于检索信息并将其显示在管理界面中
 - 运行时会发出这些请求 `show` 命令、例如。
 - 默认情况下、不会记录获取请求、但您可以控制是否从ONTAP命令行界面发送获取请求 (`-cliget`ONTAP`) (`-ontapiget``)或REST API (`-httpget`)将记录在文件中。

ONTAP会在中记录管理活动 `/mroot/etc/log/mlog/audit.log` 节点的文件。此处会记录三个 shell 中用于 CLI 命令的命令— `clustershell`，`nodeshell` 和非交互式 `systemshell`（交互式 `systemshell` 命令不会记录）—以及 API 命令。审核日志包含时间戳，用于显示集群中的所有节点是否都进行了时间同步。

◦ `audit.log` AutoSupport工具会将文件发送给指定的收件人。您还可以将内容安全地转发到指定的外部目标，例如 Splunk 或系统日志服务器。

◦ `audit.log` 文件每天轮换。当大小达到 100 MB 时，也会进行轮换，并保留前 48 个副本（最多总共 49 个文件）。当审核文件执行每日轮换时，不会生成 EMS 消息。如果审核文件因超过其文件大小限制而发生轮换，则会生成一条 EMS 消息。

对 ONTAP 9 中的审核日志记录进行的更改

从ONTAP 9开始、`command-history.log` 文件将替换为 `audit.log``和 ``mgwd.log` 文件不再包含审核信息。如果要升级到 ONTAP 9，则应查看引用旧文件及其内容的任何脚本或工具。

升级到ONTAP 9后、现有 `command-history.log` 文件将保留。它们将作为新的旋转(删除) `audit.log` 文件将进行轮换(创建)。

用于检查的工具和脚本 `command-history.log` 文件可能会继续工作、因为中有一个软链接 `command-history.log` to `audit.log` 在升级时创建。但是、用于检查的工具和脚本 `mgwd.log` 文件将失败、因为该文件不再包含审核信息。

此外，ONTAP 9 及更高版本中的审核日志不再包含以下条目，因为它们不会被视为有用，并且发生原因不必要的日志记录活动：

- ONTAP 运行的内部命令（即 `username=root`）
- 命令别名（与其所指向的命令不同）

从 ONTAP 9 开始，您可以使用 TCP 和 TLS 协议将审核日志安全地传输到外部目标。

显示审核日志内容

您可以显示集群的内容 `/mroot/etc/log/mlog/audit.log` 使用ONTAP命令行界面、系统管理器或Web浏览器访问文件。

集群的日志文件条目包括以下内容：

时间

日志条目时间戳。

应用程序

用于连接到集群的应用程序。可能值的示例包括 `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, 和 `service-processor`。

用户

远程用户的用户名。

State

审核请求的当前状态、可能为 `success`, `pending`, 或 `error`。

message

一个可选字段、其中可能包含有关命令状态的错误或追加信息。

会话ID

接收请求时使用的会话ID。每个SSH `_session_` 都分配有一个会话ID、而每个HTTP、ONTAPI或SNMP `_request_` 都分配有一个唯一的会话ID。

Storage VM

用户连接到的SVM。

范围

显示 `svm` 请求位于数据Storage VM上时；否则显示 `cluster`。

命令ID

在CLI会话上收到的每个命令的ID。这样、您就可以关联请求和响应。ZAPI、HTTP和SNMP请求没有命令ID。

您可以从ONTAP 命令行界面、Web浏览器以及从ONTAP 9.11.1开始的System Manager中显示集群的日志条目。

System Manager

- 要显示清单、请选择*事件和作业>审核日志*。+ 每列都有用于筛选、排序、搜索、显示和清单类别的控件。清单详细信息可作为Excel工作簿下载。
- 要设置过滤器，请单击右上角的*Filter*按钮，然后选择所需的字段。+ 您还可以通过单击会话ID链接来查看在发生故障的会话中执行的所有命令。

命令行界面

要显示从集群中的多个节点合并的审核条目、请输入：`+ security audit log show [parameters]`

您可以使用 `security audit log show` 命令以显示集群中单个节点或多个节点合并的节点的审核条目。您还可以显示的内容 `/mroot/etc/log/mlog` 目录。有关详细信息，请参见手册页。

Web 浏览器


您可以显示的内容 `/mroot/etc/log/mlog` 目录。 ["了解如何使用Web浏览器访问节点的日志、核心转储和MIB文件"](#)。

管理审核获取请求设置

虽然默认情况下会记录设置请求、但不会记录获取请求。但是、您可以控制是否从ONTAP HTML发送GET请求 (`-httpget`)、ONTAP命令行界面 (`-cliget`)或ONTAP API (`-ontapiget`)将记录在文件中。

您可以从ONTAP 命令行界面修改审核日志记录设置、并从ONTAP 9.11.1开始从System Manager修改。

System Manager

1. 选择*事件和作业>审核日志*。
2. 单击  然后、在右上角选择要添加或删除的请求。

命令行界面

- 要指定应将来自ONTAP命令行界面或API的获取请求记录在审核日志(audit.log文件)中、除了默认设置请求之外、还应输入：`+ security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- 要显示当前设置、请输入：`+ security audit show`

有关详细信息、请参见手册页。

管理审核日志目标

您最多可以将审核日志转发到10个目标。例如，您可以将日志转发到 Splunk 或系统日志服务器，以便进行监控，分析或备份。

关于此任务

要配置转发、您必须提供系统日志或Splunk主机的IP地址、其端口号、传输协议以及用于转发日志的系统日志工具。 ["了解系统日志工具"](#)。

您可以选择以下传输值之一：

UDP未加密

无安全性的用户数据报协议(默认)

TCP未加密

传输控制协议无安全性

TCP已加密

传输控制协议与传输层安全(Transport Layer Security、TLS)+ 选择TCP加密协议后，可使用*Verify server*选项。

您可以从ONTAP 命令行界面转发审核日志、并从ONTAP 9.11.1开始从System Manager转发审核日志。

System Manager

- 要显示审核日志目标、请选择*集群>设置*。+ 日志目标计数显示在*Notification Management磁贴*中。单击 ⓘ 以显示详细信息。
- 要添加、修改或删除审核日志目标、请选择*事件和作业>审核日志*、然后单击屏幕右上角的*管理审核目标*。+ 单击 + Add、或单击 ⓘ 在*主机地址*列中编辑或删除条目。

命令行界面

1. 对于要将审核日志转发到的每个目标，请指定目标 IP 地址或主机名以及任何安全选项。

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

- 如果 cluster log-forwarding create 命令无法对目标主机执行ping操作以验证连接、命令失败并显示错误。尽管不建议使用 -force 参数并使用命令可绕过连接验证。
 - 设置时 -verify-server 参数设置为 true、日志转发目标的标识通过验证其证书进行验证。您可以将此值设置为 true 仅当您选择时 tcp-encrypted 中的值 -protocol 字段。
2. 使用验证目标记录是否正确 cluster log-forwarding show 命令：

```
cluster1::> cluster log-forwarding show
```

Destination Host	Port	Protocol	Verify Server	Syslog Facility
192.168.123.96	514	udp-unencrypted	false	user
192.168.123.98	514	tcp-encrypted	true	user

2 entries were displayed.

有关详细信息、请参见手册页。

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。