ONTAP日志概述

https://kb-cn-stage.netapp.com/on-prem/ontap/Ontap_OS/OS-KBs/Overview_of_ONTAP_Logs
Updated: Wed, 22 Apr 2026 05:29:49 GMT

适用场景

- ONTAP 9
- 日志路径 和日志文件

问题解答

正在登录ONTAP

- 日志是由ONTAP操作系统生成并记录在集群上的平面文本文件中的事件触发的消息、其严重性不等。
- 日志是管理员、NetApp支持和AutoSupport系统确定和隔离各种问题根源的主要资源™。
- 可以使用多种不同的方法收集、查看和转发日志。
- 所有日志都存储在`/mroot/etc/log` 和`/mroot/etc/log/mlog` 中，包括EMS、审核日志和用户空间应用程序日志。 无法更改这些路径。
- 日志 `/mroot/etc/log` 每周轮换一次、最多 轮换5到10次、然后删除最早的日志。
- `/mroot/etc/log/mlog` 中的日志每天轮换一次、最多轮换35次、然后删除最早的日志。

- 使用Web浏览器访问节点的日志、核心转储和MIB文件
  - 如何通过SPI手动下载EMS日志文件？

Event Management System（事件管理系统）(EMS)

- 事件管理系统(EMS)是基于系统日志标准构建的ONTAP消息传送工具。
- EMS可简化集群范围事件的管理以及管理员选择接收通知的方式。
- EMS提供了一个编目日志记录机制、每个事件都有一个正式定义。
- 这样、EMS就可以提供自动垃圾邮件管理(如邮件禁止)、可配置的通知、帮助将低级别的数据转换为可理解的文本、NVRAM支持邮件以及自动标记邮件等服务。
- EMS包含数千条预定义消息、这些消息会在相应事件上触发。
- 消息的以点分隔的树状命名方案可提供与消息的来源和含义相关的显著准确性。
- 正式事件定义描述了事件在集群环境中的含义。
- 每个事件都包含一个更正操作问题描述、它可以帮助管理员更快地做出响应事件所需的决策。
- 这种标准化和准确性还会转移到NetApp的管理工具中、这些工具利用EMS数据。
  - **注意**：EMS不包含命令历史记录或管理审核。
- EMS事件可通过以下命令行进行查看：

```
cluster::> event log show
Time                Node             Severity       Event
------------------- ---------------- -------------- ---------------------------
3/18/2014 13:00:04  cluster-01       INFORMATIONAL kern.uptime.filer: 1:00pm up
20:17
```

审核日志

- 审核日志记录对于ONTAP系统的管理安全性至关重要。
- 审核日志会记录发送到集群的命令、发送命令的用户以及命令的成功或失败情况。
- 此适用场景命令行界面(Command-Line Interface, CLI)、Data ONTAP API (ONTAPI®)调用(例如NetApp易管理性工具中的命令)和HTTP请求。
- 在Data ONTAP 8™3及更早版本中，审核日志存储在`/mroot/etc/log/mlog/command-history.log` 中。
- 也可以在`/mroot/etc/log/mlog/mgwd.log` 中的M木质 日志中查看命令历史记录。
- 从ONTAP 9开始， `command-history.log` 文件将被 `audit.log` 替换，并且 `mgwd.log` 文件不再包含审核信息。

ONTAP如何实施审核日志记录

- 审核日志中记录的管理活动包含在标准AutoSupport报告中、某些日志记录活动包含在EMS消息中。

- 您还可以将审核日志转发到指定的目标、并使用命令行界面或Web浏览器显示审核日志文件。
- ONTAP会记录在集群上执行的管理活动、例如发出的请求、触发此请求的用户、用户的访问方法以及发出请求的时间。
- 管理活动的类型可以为以下几种之一：
  - 设置请求、通常适用于非显示命令或操作
    - 例如、在运行create、修改或delete命令时会发出这些请求。
    - 默认情况下、系统会记录设置请求。
  - 获取请求，即检索信息并将其显示在管理接口中
    - 例如、在运行show命令时会发出这些请求。
    - 默认情况下不会记录获取请求，但您可以使用 `security audit modify` 命令控制是将从ONTAP命令行界面(`-cliget`)还是从ONTAP API (`-ontapiget`)发送的获取请求记录在文件中。
- ONTAP会将管理活动记录在 节点的`/mroot/etc/log/mlog/audit.log` 文件中。
- 此处会记录三个命令行界面命令Shell (即、clistershell、nandeshell和非交互式systemshell)中的命令以及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同步了时间。
- `audit.log` 文件由AutoSupport工具发送给指定的收件人。您还可以将内容安全地转发到您指定的外部目标、例如Splunk或系统日志服务器。
- `audit.log` 文件每天进行轮换。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。
- 如果审核文件因超出其文件大小限制而发生轮换、则会生成EMS消息。
- 您可以使用 `security audit log show` 命令显示集群中单个节点或多个节点的合并审核条目。
- 您还可以 使用Web浏览器在单个节点上显示 `/mroot/etc/log/mlog` 目录的内容。

其他日志

- EMS事件符合系统日志标准、因为它们能够转发到系统日志服务器进行实时监控、并且EMS事件是与管理员最相关的事件。
- ONTAP操作系统生成的其余日志是由不断记录其活动的用户空间应用程序生成的。
- 这些日志级别较低、不面向管理员、但主要供NetApp支持、开发和QA人员使用。

表1)登录 `/mroot/etc/log/`

日志或目录	问题描述
`acp/`	• 发送到ASUP • 磁盘架备用控制路径管理(ACP)日志

日志或目录	问题描述
auditlog.log	• 记录节点Shell命令(即、node run命令) • 在8.3及更早版本中、相当于command-history.log。 • 从集群模式Data ONTAP 8 2.2开始、在AutoSupport中发送
autosupport/	• 此目录包含此节点最近生成的50条AutoSupport消息
backup.log	• 记录SMTape等NDMP备份过程
bcomka/	• SAN内核模块的调试级别日志
clone.log	• 记录LUN克隆
ems, ems.log	• EMS 事件 • 在AutoSupport中发送
ems_persist	• 二进制格式的文件、由NetApp支持部门在某些情况下使用
leak_data, leak_data_filtered	• 内存信息、主要用于调试目的
messages, messages.log	• 节点级日志 • 日志是/mroot/etc/log/mllog/messages.log的链接
mlog/	• 此目录的内容将发送到ASUP • 包含管理组件应用程序日志

日志或目录	问题描述
named.log	• 名称服务日志
nbu_snapvault.log	• SnapVault®日志
playlist_diag	• 从WAFL播放列表中记录缺失的文件ID®
plxcoeff/	• 包含PLX PCI-E交换机日志 • 从集群模式ASUP 2.1开始发送到Data ONTAP 8
rastrace/	• 调试SAN跟踪日志
servprocd/	• 服务处理器日志
shelflog/	• 磁盘架日志
sis, sis.log	• 重复数据删除日志
ssram/	• 系统暂存器RAM日志
stats/	• 与性能相关的日志
snapmirror.log, snapmirror_audit.log, snapmirror_error.log	• SnapMirror®日志

日志或目录	问题描述
treecompare.log	• 树管理进程的日志、用于比较 使用Snapshot副本的卷和/或qtrees中的数据完整性®
volread.log	• SnapMirror使用的卷读取引擎的日志

表2)登录 /mroot/etc/log/mlog/

日志或目录	问题描述
last_rotate.log	• 记录日志轮换的历史记录
apache_access.log	• 记录对Apache服务器的访问历史记录 • 包含通过HTTP (S)获取日志文件请求的历史记录
apache_error.log	• 记录Apache错误
audit.log	• ONTAP 9 0及更高版本的审核日志 • 记录命令行界面、ONTAP、HTTP中的命令 • 始终记录设置的请求，但可以切换获取请求的记录
bcomd.log	• 用于处理管理组件与SCSI刀片式服务器之间的SAN交互的BCOM守护进程的日志
command-history.log	• 集群模式Data ONTAP 8 3及更早版本的审核日志 • 记录命令行界面、ONTAP、HTTP中的命令 • 始终记录设置的请求，但可以切换获取请求的记录

日志或目录	问题描述
debug.log	• 调试严重性级别的日志
fpolicy.log	• FPolicy的日志®
hashd.log	• 有关anchCache哈希守护进程的日志
jm-restart.log	• 包含作业管理器已重新启动的作业的列表
memsnap-*.log (星号是通配符、因为memSnap日志有多种类型)	• 包含内存信息
messages.log	• 这些消息会记录在ONTAP中 • 包含整个集群中的重要日志 • 有些与EMS重叠、但没有诸如抑制等EMS功能
mgwd.log	• 包含管理组件的日志 • 默认情况下，记录设置请求，但可以进行开关
ndmpd.log	• 包含NDMP守护进程的日志
notifyd.log	• 包含用于处理AutoSupport (ASUP)的通知守护进程的日志
php.log	• 包含PHP进程的日志 • 包含集群中各个节点之间同步日志的历史记录

日志或目录	问题描述
secd.log	• 包含安全 守护进程的日志、该守护进程负责处理各种身份验证任务、例如NAS身份验证 ◦ 最多保留10个副本
servprocd.log	• 包含有关服务处理器守护进程的日志
sktlog/	• 主内核的调试级别日志
sktlogd.log	• 主内核的调试级别日志
spdebug.log	• 包含与来自服务处理器的异常事件相关的日志
spmd.log	• 包含有关服务进程管理器守护进程的日志、该守护进程可监控用户空间应用程序以确保其运行状况良好
vifmgr.log	• 包含与接口和网络连接相关的日志
vldb.log	• 包含卷位置数据库应用程序上的日志

追加信息

- 管理管理活动的审核日志记录
  - 对ONTAP 9中的审核日志记录进行的更改
  - ONTAP如何实施审核日志记录
  - 将审核日志转发到目标
  - 用于管理为管理活动配置的审核设置的命令
- EMS.log 将根据以下配置进行轮换。

::> set d ::*> event config show Mail From: admin@localhost Mail Server: localhost Proxy URL: - Proxy User: -

> Suppression: on Console: on Max Target Log Size: 36700160 Max Filter Count: 50 Max Filter Rule Count: 128 Max Destination Count: 20 Max Notification Count: 20 Filter Exempt from Suppression: no-info-debug-events Duplicate Suppression Duration (secs): 120 Log Rotation Size (bytes): 40MB <---- Default value REST API Delivery Timeout (secs): 60

- 如有必要、可以修改默认值。最大大小为**100MB**：

```
::*> set diag; event config modify -log-rotation-size 80MB
```

- 无法延长`event log show`命令显示的日志的存储期限。

AutoSupport

- AutoSupport (ASUP™)系统是Data ONTAP的自动运行状况监控工具，可用于报告错误，在某些情况下，还可以生成NetApp支持案例。
- 报告可能由使用EMS事件或计划的错误情况触发。
- ASUP警报可以通过电子邮件发送到管理员的内部IT组织和/或发送到NetApp支持部门进行自动分析。
- ASUP消息包含EMS和其他用户空间应用程序的重要日志数据。
- 下一节将确切讨论ASUP收集的日志。