



是否可以CEF格式发送ONTAP事件通知？

https://kb-cn.netapp.com/on-prem/ontap/Ontap_OS/OS-KBs/Is_it_possible_to_sent_ONTAP_event_not...

Updated: 周六, 12 7月 2025 16:52:44 GMT

适用场景

- ONTAP 9
- 事件管理系统(EMS)
- 系统日志
- 通用事件格式(CEF)
- 安全信息和事件管理(SIEM)
- 日志事件扩展格式(leef)

问题解答

- Syslog 是为计算机消息日志记录定义的标准
- 该标准由[RFC 3164](#) 和中的IETF 定义[RFC 5424](#)
- EMS 是基于syslog 标准构建的ONTAP消息传送工具
- CEF 是 ArcSight开发的一种系统日志替代方案
- SIEM syslog 以外的替代方案(CEF 、LEEF 等) 不能用于ONTAP

追加信息

另请参见：

- [登录到集群模式Data ONTAP](#)
- [RFC 3164：《BSD系统日志协议》](#)
- [RFC 5424：系统日志协议](#)
- [系统日志服务器不采用ONTAP格式](#)
- [RFC 5424格式支持系统日志事件消息](#)