Application Notes

Understanding the New Audit Logging Format

05 May 2026

Table of Contents

In HSM firmware version 13.5, nShield updated the audit logging mechanism from a logging mechanism based on Common Event Format (CEF) to one that better aligns with the nCore data structures.

If you used audit logging on older firmware versions and have since upgraded to 13.5 or later, read this document to get a better understanding of the changes and to understand how the newer version of audit logging works.

This document explains why the audit logging format changed, how the new model differs from CEF-based audit logging, and what operational and planning implications users should consider. It is intended to help users justify upgrades and plan changes to audit log handling with confidence.

1. Why the Audit Logging Format Changed

- **Reliability and Performance:** The legacy audit logging mechanism relied on CEF messages exported over UDP syslog. This approach could lose audit records without detection, because UDP does not guarantee delivery or ordering. Internal review identified this as a risk for audit completeness and reliability.
- **Performance Overhead:** CEF-based audit logging also imposed significant performance overhead. Internal observations showed that enabling full audit logging could reduce cryptographic throughput by up to an order of magnitude in some workloads. This impact made continuous audit logging impractical in performance-sensitive environments.
- **New Audit Logging Format:** The new audit logging format was designed to address these limitations by improving performance, ensuring detectable and bounded record loss, and providing a structured and extensible audit format aligned with nCore data structures.

2. High-Level Comparison: CEF Audit Logging vs New Audit Logging

The new audit logging model represents a significant evolution from the CEF-based approach. The following sections summarize the key differences and what has not changed.

2.1. Summary of Key Differences

- **CEF Audit Logging:** CEF audit logging exported text-formatted records over UDP syslog when events occurred. The new audit logging model stores audit records locally in a compressed hardserver database and exports them through the nShield Audit Log Service with confirmation and verification support.
- **New Audit Logging Format:** The new format uses a binary representation based on nCore data structures rather than free-form text. This change enables precise field definitions, richer metadata, and future extensibility without redesigning the logging system.

2.2. What has not Changed

- **Purpose:** The purpose of audit logging has not changed. Audit logs still record security-relevant operations performed by the HSM to support accountability, forensic investigation, and compliance activities.
- **Scope:** The scope of audited events and the overall compliance intent remain consistent. The change affects how records are stored, transported, and verified, not which operations are auditable.

3. Key Benefits of the New Audit Logging Format

The new audit logging format provides several important benefits compared to CEF-based logging:

3.1. Performance Improvements

The new binary audit logging format significantly reduces adverse performance impact com pared to CEF. Cryptographic throughput is now only modestly affected, even when full audit logging is enabled.

This improvement allows users to enable comprehensive auditing without sacrificing sys- tem throughput in production environments.

3.2. Security and Reliability Improvements

CEF logging relied on UDP syslog, which can silently drop messages during congestion, fail- ures, or shutdowns. The new audit logging model ensures that any loss of audit records is detectable and bounded.

Audit records remain stored locally until the nShield Audit Log Service confirms receipt. This design prevents silent loss and improves reliability across host and network transitions.

3.3. Improved Audit Record Integrity and Verification

The new system supports cryptographic verification of audit logs using the nshieldaudit tooling. Verification allows users to confirm that records are complete and unmodified since creation.

This capability strengthens the evidentiary value of audit logs during internal reviews and external audits.

3.4. Enhanced Tooling and Usability

The nshieldaudit utility provides a unified tool for querying, verifying, and exporting audit logs. Users can export logs in both human-readable text and structured JSON formats.

This tooling improves usability and integration with downstream analysis and log manage-

ment systems.

3.5. Extensibility and Future-Proofing

The new binary audit format aligns directly with nCore structures, which allows structured evolution of audit records over time. New fields can be added without breaking existing tooling.

This approach supports future audit and compliance requirements without requiring another fundamental redesign.

4. How the New Audit Logging Model Works (Conceptual Overview)

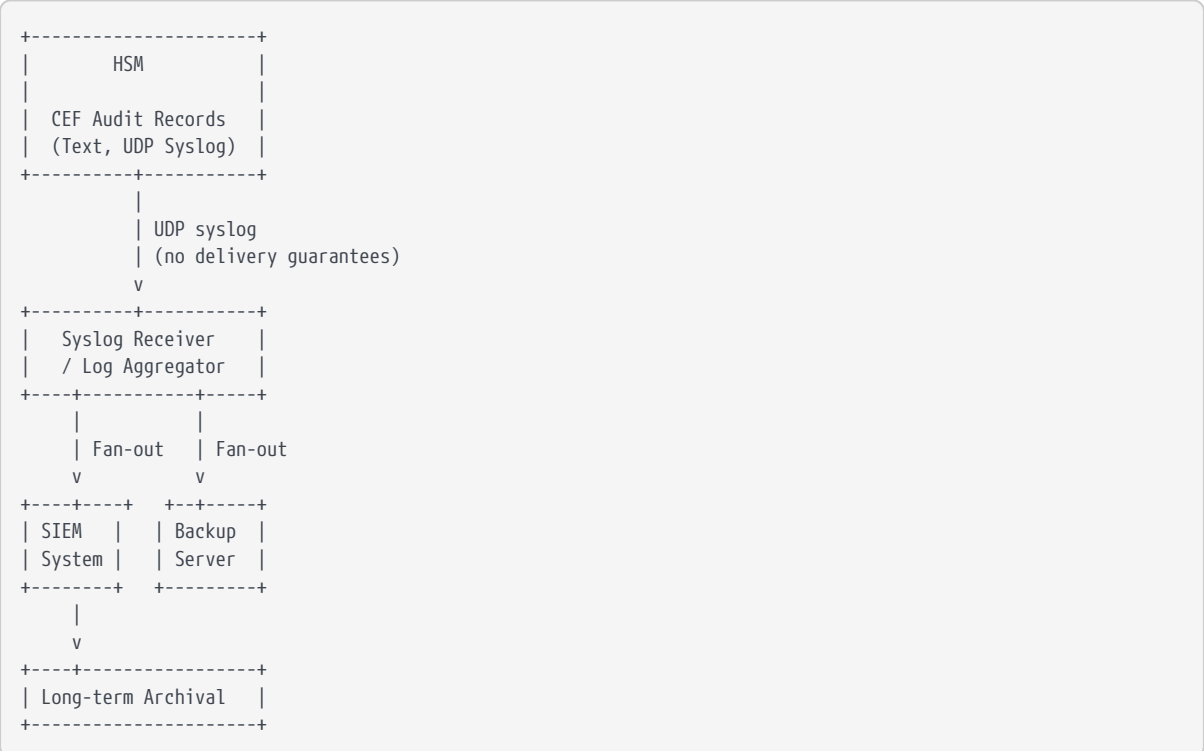
The HSM generates audit records and stores them locally in a compressed hardserver database. Records persist locally until the nShield Audit Log Service confirms successful receipt.

Startup and shutdown handshakes coordinate between the HSM, host, and audit services to prevent record loss during transitions. This design improves durability across restarts and failures.

4.1. Audit Logging Architecture Overview: CEF vs New Model

The following diagrams provide a high-level comparison of the legacy CEF audit logging architecture and the new audit logging architecture. They focus on how audit records flow through the system and where customers can integrate their own log management, backup, and distribution solutions.

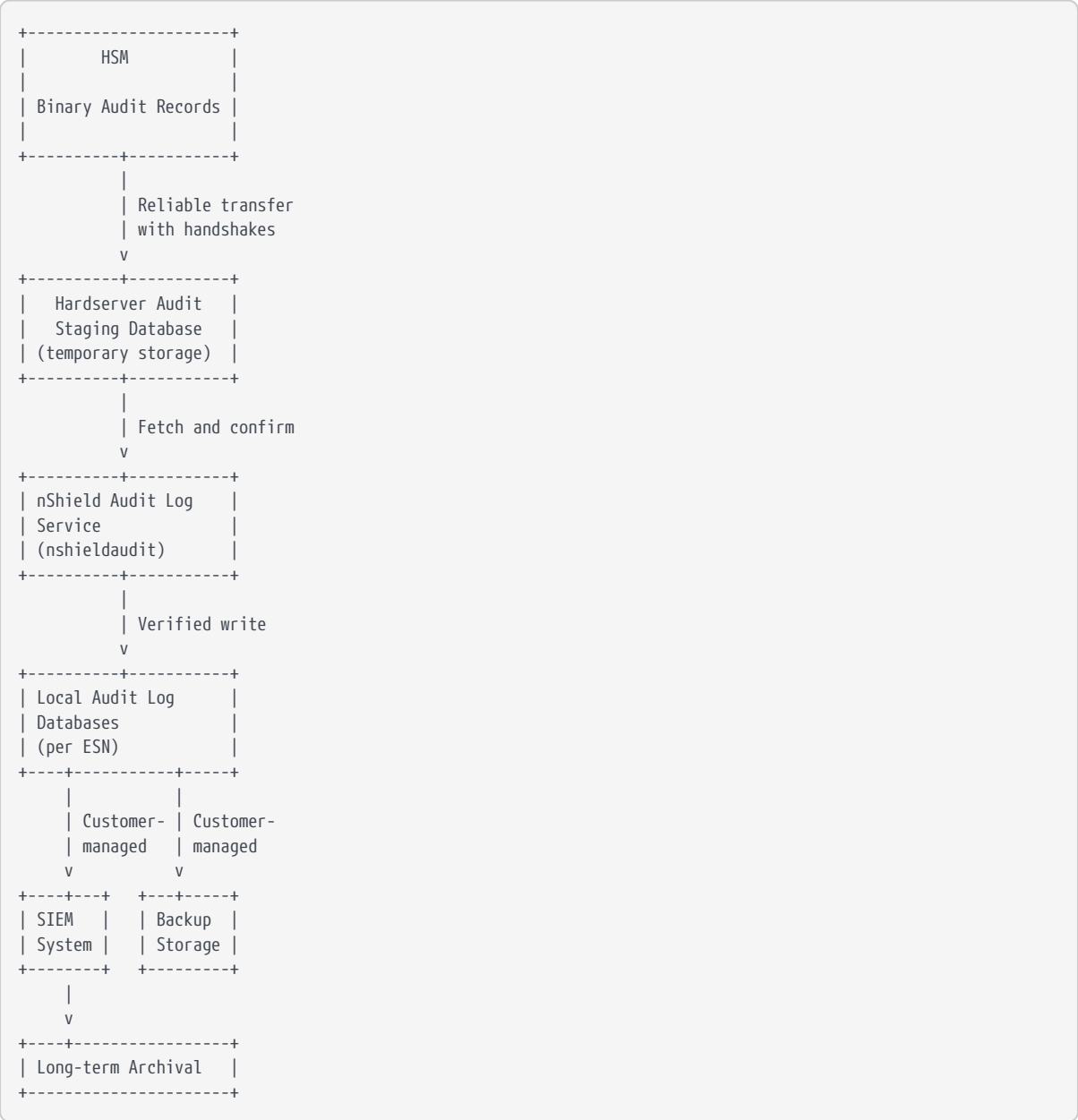
Legacy CEF Audit Logging Architecture



The Legacy CEF Audit Logging Architecture diagram shows the legacy model where audit records were emitted directly from the HSM as syslog messages over UDP. Log duplication

and sharing relied on external syslog infrastructure, and message loss could go undetected.

New Audit Logging Architecture Using the nShield Audit Log Service



The New Audit Logging Architecture Using the nShield Audit Log Service diagram shows how audit records are staged, retrieved, and stored using the nShield Audit Log Service. Once records are written to local audit log databases, customers can back up, replicate, and distribute them using standard enterprise tools.

In the new model, duplication and backup do not occur at the HSM boundary. Instead, the nShield Audit Log Service provides a reliable, verifiable mechanism for delivering audit records to a local filesystem. From that point onward, customers can apply existing IT practices such as file replication, backups, centralized log ingestion, or offline archival. This approach avoids undetectable data loss while preserving flexibility in how audit data is

shared and retained.

5. Operational Considerations for Users

Users should be aware of the following operational considerations when using the new audit logging format:

5.1. Detectable Audit Record Loss

If audit records are lost due to hardware failure or similar events, the system records how many records were lost, provided the HSM remains accessible. Loss does not occur silently.

5.2. Exporting and Retaining Audit Logs

Users export audit logs using the nshieldaudit utility. Exported records can be retained exter nally in accordance with local retention policies.

5.3. Verifying Audit Logs

Users can verify audit logs using nshieldaudit to confirm integrity and completeness. Verifi- cation provides evidence that logs have not been altered.

5.4. Deleting or Rotating Audit Logs

Audit records are deleted locally only after confirmation by the nShield Audit Log Service. Users control external retention after export, per organizational policy.

5.5. Using Transaction IDs for Correlation

Customer applications can attach Transaction IDs to nCore commands. These IDs appear in audit records and support correlation between application activity and audit events.

6. Impact on Existing Environments and Upgrade Planning

Environments may temporarily contain both CEF-based and new-format audit logs during upgrades. Users should plan for parallel log handling during transition periods.

No migration of historical CEF logs is required, because the new format applies only to newly generated audit records.

7. Frequently Asked Questions (FAQs)

1. Did the audit logging change affect compliance or certification requirements?
    - The audit logging objectives remain the same. The change improves reliability and verifiability without reducing compliance coverage.
2. Can audit records still be lost, and how would I know?
    - Loss is detectable and quantified if it occurs and the HSM remains accessible.
3. Why was UDP-based CEF logging considered a problem?
    - UDP syslog can lose messages without detection, which risks silent audit gaps.
4. Do I need to migrate old CEF logs to the new format?
    - No. Existing CEF logs remain valid historical records.
5. Can I still export logs in a human-readable format?
    - Yes. Logs can be exported in text and JSON formats using nshieldaudit.
6. How do I prove audit log completeness to an external auditor?
    - Use verification tooling to demonstrate the integrity and detectability of loss.
7. What happens if the host or HSM shuts down unexpectedly?
    - Startup and shutdown handshakes limit and detect any audit record loss.
8. Can I correlate application activity with audit records?
    - Yes. Transaction IDs allow correlation across application and audit data.
9. Does this change increase storage or management overhead?
    - Local compression and confirmation-based deletion help control storage growth.
10. Where can I find detailed command-level instructions?
    - Refer to the Audit Logging, nShield Audit Log Service, and nshieldaudit sections in the HSM User Guide.