

InfiniVault Audit Trail and Chain of Custody

Most of the regulations that pertain to storing of information have a requirement about maintaining an audit trail of access for the information. The actual mechanics of what is to be done is not prescribed but the implicit requirement is that a chain of custody report on the information when it is under the control of the storage environment must be able to be produced.

In the case of an archiving system, the audit trail begins when the information is ingested by the archiving system. Every action regarding that information must be tracked since the archiving system, which would be the same for any storage system where the compliance to regulations applies, is the custodian of that information. To prove the stewardship of the information and provenance of that information requires both the capabilities to ensure immutability – typically implemented as a WORM type of storage – and the production of a chain of custody report using the audit trail information.

Audit Trail Captures Information

InfiniVault has an extensive audit trail for the information that is archived. InfiniVault can produce a chain of custody report for each file on demand that will provide the needed information to verify the provenance of the data. The chain of custody reports become a narrative of what happens to the information from the point of ingestion to the time of reporting.

The information captured in the audit trail is the key component for the chain of custody report. The integrity of the information preserved through the WORM implementation in InfiniVault is fundamental to meeting regulations and is implicit with the audit trail. The information the InfiniVault captures includes:

At the time of ingestion when archiving software stores the information on InfiniVault in the form of files or containers of files:

- Date / time ingested
- File details – file name and size
- User identity that archived the file
- Name of the archive where the file was stored
- Number of copies made of the file
- Retention settings for the file
- Settings of encryption, retention, and single instancing



InfiniVault™ Product Family

On any subsequent access to the file:

- Date/time of access
- User identity that accessed the file
- Type of access: read or attempted write/delete (which would be prohibited)

File disposition when retention period expires:

- Deletion or secure deletion time/date from active archive
- Deletion time/date from file catalog (file metadata database)
- Secure deletion time/date from a cartridge

Legal hold actions:

- Legal hold applied time/date
- Identity of the InfiniVault administrator who applied the legal hold
- Legal hold released time/date
- Identity of the InfiniVault administrator who released the legal hold

RDX Cartridges:

- Completion of write to RDX cartridge time and date which includes the unique cartridge serial number and the cartridge label
- RDX cartridge removal and insertions that occurred where that file resided time and date

The chain of custody report can be run by an authorized administrator on InfiniVault. The InfiniVault administrator can select a file or set of files through the web GUI administration interface and a chain of custody report will be generated. The chain of custody report will be displayed for each file in chronological order. In addition to selection of a file or set of files, all files within a date range may be selected for a chain of custody report. The chain of custody report can be saved as a PDF file on the server of the client computer.