



# Establishing a Strong Chain of Custody for your Digital Assets with Leonovus

**AUTHOR: ALLAN MACPHEE, SALES ENGINEER**

**DATE: JUNE 14, 2019**

---

**CONTENTS:**

Contents:..... 2

Intended audience..... 3

Introduction..... 3

Logged compliance events ..... 4

Local compliance log files..... 5

SIEM/Syslog integration ..... 5

Blockchain for higher assurance audit trails..... 8

Blockchain overview - hyperledger..... 9

High level arcitecture..... 11

Summary..... 12

## INTENDED AUDIENCE

---

The intended audience for this document is IT professionals and business management interested in understanding the high-level technical description of the Leonovus chain of custody capabilities. It is assumed that the reader is familiar with the Leonovus Vault solution. For detailed information about Leonovus Vault, please visit <https://www.leonovus.com/multi-cloud-data-controller/>

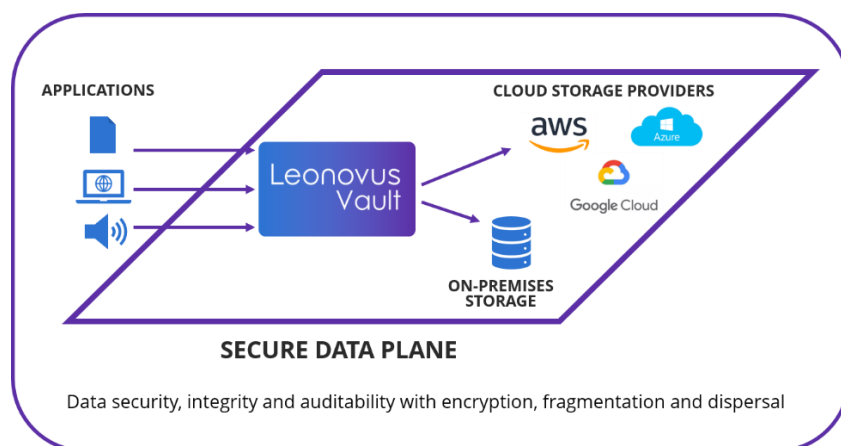
## INTRODUCTION

---

Leonovus Vault is a multi-cloud data controller that acts as a unified storage target for all applications and storage. You can now create a long-term security strategy that:

- Puts you in control of your data's security by decoupling data from the underlying infrastructure
- Mitigates data breaches and establishes true data sovereignty by storing discretely indecipherable data in public clouds
- Minimizes administrative error through a single pane of glass for applying consistent security policy
- Is tailored to each of your data sets with granular control of data placement, key management and long-term retention
- Provides an immutable chain of custody and mechanisms to ensure data integrity

The Leonovus Vault solution provides advanced data protection by encrypting your data, shredding it and distributing these data fragments across on-premises and public cloud storage nodes. The encryption keys and security policies used to do so remain completely under your control. With the multi-cloud data controller, if one of your nodes were to be breached, only a partial – and dispensable – fragment of your encrypted data files is exposed, which when viewed on its own, is entirely unintelligible to an unauthorized user. Data fragmentation is achieved using erasure coding, effectively establishing RAID 5/6 equivalent data resiliency across the storage nodes you've configured.



Securing your data is an important first step, the next challenge is to prove that the data security controls in place are working. Organizations must be able to track what data has been migrated to the cloud, when it was migrated, who migrated it (upload), and where it is located. They also require visibility into who has accessed this data, when the data was accessed and what operation was performed (download, copy, delete). A trusted audit trail of all compliance-related events must be maintained to provide the visibility necessary for data security audits and compliance requirements. Organizations must be able to immediately respond to requests such as “provide a list of all users who accessed file ‘x’ ”, or “provide records for all the files that user ‘y’ accessed over the last 30, 60, 90 days” in support of forensic investigations or compliance audits.

This paper will provide insight into the audit and compliance capabilities provided by the Leonovus Vault solution and the different options available for implementing Leonovus compliance logging.

## LOGGED COMPLIANCE EVENTS

---

Leonovus Vault supports three different categories of compliance audit events: file, authentication, and management.

### **File events**

All interactions with files/data under Leonovus management such as upload, download and delete operations are captured. The events logged include:

- filename
- cryptographic hash of the file
- operation type (upload, download, copy, delete)
- user performing the operation
- timestamp of the operation
- Leonovus internal file Id

### **Authentication events**

Authentication events logged include:

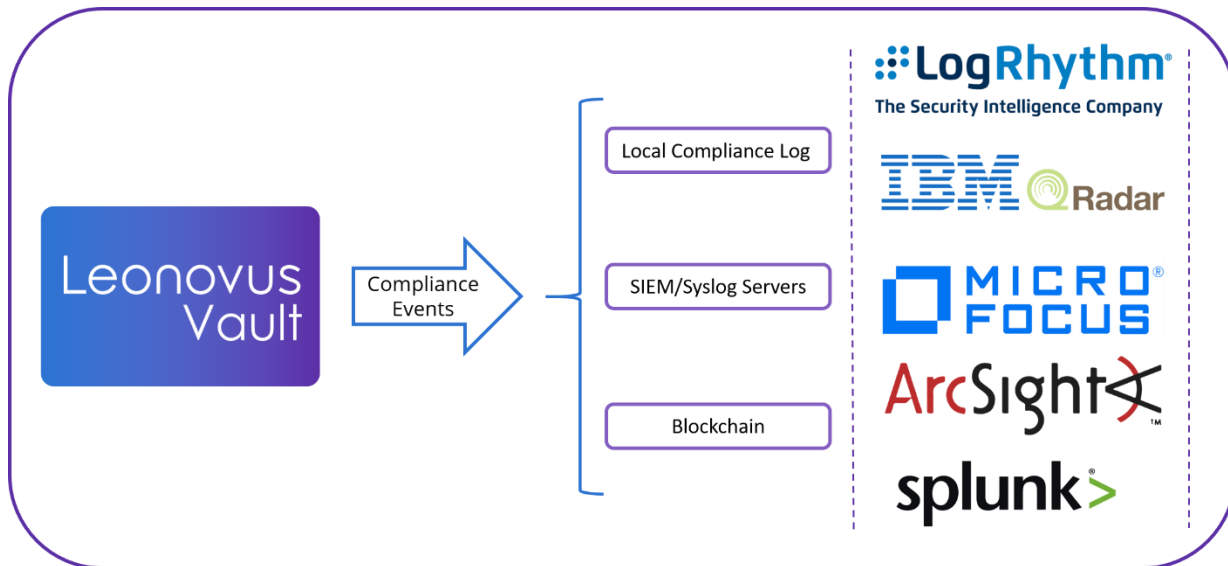
- administrative successful login
- administrative successful logout
- administrative login failures

### **Management events**

Management events that are logged from a compliance perspective include operations related to the following tasks:

- creation, modification, and deletion of cloud providers
- creation, modification, and deletion of storage nodes
- creation, modification, and deletion of storage zones
- creation, modification, and deletion of storage pools
- user administration
- tenant management

Leonovus compliance events can be made available via three complementary and non-exclusive approaches.



## Local compliance log files

Leonovus Vault maintains a local compliance log capturing all three categories of compliance events. The compliance logs are rotated daily with the location and name of the log files configurable. The screen capture below shows what a successful login event would look like in a local compliance log.

```
2019-06-06 20:54:47,436 INFO [com.leonovus.vault.audit.ComplianceLogger] (default task - 19)
CEF:0|Leonovus|Vault|4.0.0+1206-2019-05-23_13_05|101|Login|6|info=
{"category": "Authentication", "timestamp": "2019-06-06T20:54:47.431Z", "site": "us-east-1", "result": "Success", "originator": "admin", "originatorAddress": "172.16.99.1", "tenant": "root", "role": "SiteAdmin"}
```

## SIEM/Syslog integration

Leonovus Vault supports the ability to send compliance events via syslog to target SIEM/Syslog servers. All three categories of compliance events are supported for forwarding via syslog. Leonovus syslog compliance events use the CEF syslog format, which is an easily extendable format using a key-value pair for each additional field of information.

The CEF syslog format consists of:

Timestamp Hostname CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

Note the use single spaces to separate Timestamp, Hostname, and the Message part of the log.

The Message is the rest of the CEF log, in which fields are separated using the vertical bar character "|", until the Extension field.

The Extension field is made of a series of "key=value " expressions, each of which is separated by a single space character " ".

The following is a sample syslog message:

```
Oct 29 13:13:17 lab02 CEF:0|Leonovus|Vault|3.4.0+482-2018-11-01_09_11|2001|UploadFile
|4|info={"category":"File","timestamp":"2018-10-29T17:13:17.255Z",
"node":"MY-VAULT-NODE-1","site":"us-east-1","result":"Success",
"originator":"sys-test-43105admin","tenant":"sys-test-43105",
"bucket":"testbucket-d34ad15a-b4ce-41c9-a9e6-dc84a2789675",
"fileId":"EzuzzJe2RVqWAYjpLLggQQ","filename":"file1",
"sha256hash":"fe55e1fef265a011a118fcd87f825c9ba60387b5bf869083000cb309fd73d24a",
"treeshash":"fe55e1fef265a011a118fcd87f825c9ba60387b5bf869083000cb309fd73d24a"}
```

**Syslog field descriptions:**

Field Name	Description	Example
Timestamp	Time of log. Format is normally controlled by syslog.	Oct 29 13:13:17
Hostname	Hostname of the system generating the log.	lab02
CEF:Version	The text "CEF:", followed by the version number of the CEF format.	CEF:0
Device Vendor	"Leonovus"	Leonovus
Device Product	The name of the Leonovus product generating this log.	Vault
Device Version	The version of the product.	3.4.0+482-2018-11-01_09_11
Signature ID	This is the Action Code, which is a numerical code uniquely identifying the action being logged.	2001
Name	This is the human-readable unique name of the Action.	UploadFile
Severity	An integer from 0 to 10 that indicates the importance of the event, with 10 meaning the most important, and 0 meaning the least important.	4

**Extension Fields**

There is only one CEF extension field, with the key name of "info". The field value is a JSON structure containing the complete set of information about an Action being logged, included information already captured in the standard CEF fields.

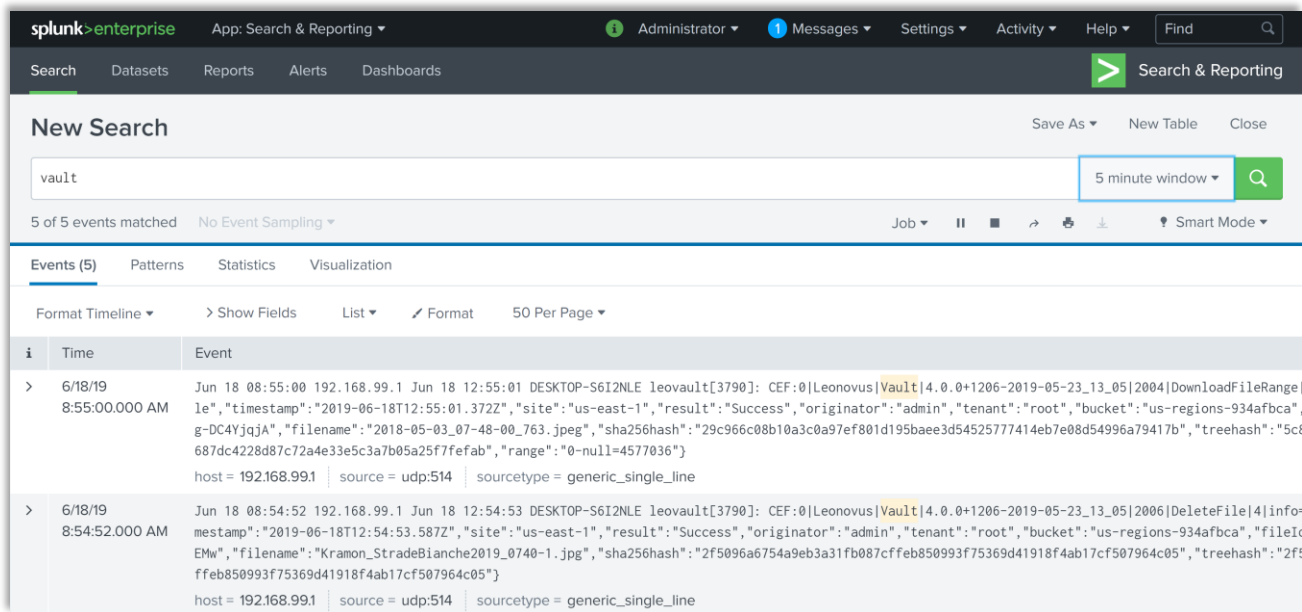
The JSON structure contains a set of common fields and an "additionalInfo" field containing a JSON object that is specific to the Category of the Action. Example categories are Bucket, File, Authentication, User, Vault-Administration, etc.

Here is the info field for the UploadFile log from the example above, reformatted for readability.

**Formatted info block**

```
info={
  "category":"File",
  "timestamp":"2018-10-29T17:13:17.255Z",
  "node":"MY-VAULT-NODE-1",
  "site":"us-east-1",
  "result":"Success",
  "originator":"sys-test-43105admin",
  "tenant":"sys-test-43105",
  "bucket":"testbucket-d34ad15a-b4ce-41c9-a9e6-dc84a2789675",
  "fileId":"EzuzzJe2RVqWAyjpLLggQQ",
  "filename":"file1",
  "sha256hash":"fe55e1fef265a011a118fcd87f825c9ba60387b5bf869083000cb309fd73d24a",
  "treehash":"fe55e1fef265a011a118fcd87f825c9ba60387b5bf869083000cb309fd73d24a"}
```

## Sample of syslog events sent to Splunk:



The screenshot shows the Splunk Enterprise Search & Reporting interface. The search bar contains the query 'vault' and a '5 minute window' filter. Below the search bar, there are 5 events matched. The interface displays two events in a table format:

i	Time	Event
>	6/18/19 8:55:00.000 AM	Jun 18 08:55:00 192.168.99.1 Jun 18 12:55:01 DESKTOP-S6I2NLE leovault[3790]: CEF:0 Leonovus Vault 4.0.0+1206-2019-05-23_13_05 2004 DownloadFileRange le", "timestamp": "2019-06-18T12:55:01.372Z", "site": "us-east-1", "result": "Success", "originator": "admin", "tenant": "root", "bucket": "us-regions-934afbca", "g-DC4YjqjA", "filename": "2018-05-03_07-48-00_763.jpeg", "sha256hash": "29c966c08b10a3c0a97ef801d195baee3d54525777414eb7e08d54996a79417b", "treehash": "5c8687dc4228d87c72a4e33e5c3a7b05a25f7fefab", "range": "0-null=4577036"} host = 192.168.99.1   source = udp:514   sourcetype = generic_single_line
>	6/18/19 8:54:52.000 AM	Jun 18 08:54:52 192.168.99.1 Jun 18 12:54:53 DESKTOP-S6I2NLE leovault[3790]: CEF:0 Leonovus Vault 4.0.0+1206-2019-05-23_13_05 2006 DeleteFile 4 informestamp": "2019-06-18T12:54:53.587Z", "site": "us-east-1", "result": "Success", "originator": "admin", "tenant": "root", "bucket": "us-regions-934afbca", "fileIdEMw", "filename": "Kramon_StradeBianche2019_0740-1.jpg", "sha256hash": "2f5096a6754a9eb3a31fb087cffe850993f75369d41918f4ab17cf507964c05"} host = 192.168.99.1   source = udp:514   sourcetype = generic_single_line

## Blockchain for higher assurance audit trails

For organizations who require a higher assurance trust level for their compliance audit logs, Leonovus is working on delivering a blockchain-based compliance audit logging capability that is currently available in beta form.

The Leonovus blockchain-based logging capability has been designed to provide an immutable audit trail for Leonovus Vault compliance log events. An immutable audit trail is critical for situations which require long term retention of audit events to support data forensics activities or for legislative compliance reasons (i.e. file access logs which must be maintained for 5, 7, 15 years or longer). Sample use cases include financial records which must be maintained for 7 years, health records which must be maintained and protected for the life of the patient, engineering and design documents which must be maintained until the end of service (airplanes, trains, nuclear generators, etc.), police records, pharmaceutical trial data, and intellectual property documents to name a few examples.

The compliance events displayed in the blockchain-based implementation differs from the other logging methods supported by Leonovus. All File events are logged to the blockchain, but Authentication events are not logged and only Management events that change storage assets such as create bucket, delete bucket are recorded.

In the Leonovus blockchain implementation, administrators can sort events based upon the different columns to facilitate displaying information such as all operations associated with a file name or by a specific user for example.

The screen shot below shows an example of the types of file compliance log events that are logged onto the Blockchain ledger.



Transaction Details					File Details >	
ID	Log time	Action	User	File Name	Bucket	
> 15bab6aa-00ea-...	2019-06-07T18:18:01.996Z	DeleteBucket	admin		new-bucket-38ce901d	
> 041fa1eb-2c8b-...	2019-06-07T18:17:41.413Z	CreateBucket	admin		new-bucket-38ce901d	
> d065c35c-cfc8-4...	2019-06-07T18:17:07.501Z	DeleteFile	admin	Leonovus - brochure - Corp Overview_20...	allan-demo	
> e75005d1-450d-...	2019-06-07T18:17:00.039Z	DownloadFil...	admin	Leonovus Corp Overview_Final.pdf	allan-demo	
> c5220fa7-7be6-...	2019-06-07T18:16:26.116Z	UploadFile	admin	2018-06-23_03-00-10_777.jpeg	allan-demo	
> 90978ddf-90c7-...	2019-06-04T18:48:53.713Z	CreateBucket	peter		dojtest	
> 709cab93-e8f1-...	2019-05-22T13:21:09.601Z	CopyFile	peter	Docs/Docs/Leonovus - brochure - Corp ...	image-bucket	
> a31ed600-e519-...	2019-05-22T13:21:09.17Z	CopyFile	peter	Docs/Docs/Leonovus - Whitepaper - GD...	image-bucket	
> b3eb3f01-0f5c-4...	2019-05-22T13:21:09.162Z	CopyFile	peter	Docs/Docs/Leonovus - Use case - Optimi...	image-bucket	
> e3ea7450-f56b-...	2019-05-22T13:21:08.52Z	CopyFile	peter	Docs/Docs/Leonovus - Use Case - Secur...	image-bucket	

To drill down on a specific event, administrators can select a specific event and select 'File Details' at the top of the page to view the cryptographic hash value (SHA256) of the file related operation.

Transaction Details				File Details <			
ID	Log time	Action	User	File Name	File Id	File Hash	Bucket
> 15bab6aa-00ea-...	2019-06-07T18:18:01.996Z	DeleteBucket	admin				new-bucket-38ce901d
> 041fa1eb-2c8b-...	2019-06-07T18:17:41.413Z	CreateBucket	admin				new-bucket-38ce901d
> d065c35c-cfc8-4...	2019-06-07T18:17:07.501Z	DeleteFile	admin	Leonovus - brochure - Corp Overview_20...	jlUjKO3CQnKBVVzhEaVg	364970785b834c1069f0e15862a3a5f8806342329b933c6426df3c4b6f6117	allan-demo
> e75005d1-450d-...	2019-06-07T18:17:00.039Z	DownloadFil...	admin	Leonovus Corp Overview_Final.pdf	XWw67yAJtQ2BvWwAjO7yLig	24aaa25f232ac890697ceeb052984bb2e0c514d829a0cac8a0c7c98f3546722a	allan-demo
> c5220fa7-7be6-...	2019-06-07T18:16:26.116Z	UploadFile	admin	2018-06-23_03-00-10_777.jpeg	XX6v0MgJQWCKX6nt0GR0G...	5a7e774dee1b2f207967422288076fdcc1af42d3b4530516c7d30a0c3ad87e67	allan-demo

To view additional blockchain metadata details, administrators can select an event and expand the view to see blockchain specific details:

▼ c5220fa7-7be6-...	2019-06-07T18:16:26.116Z	UploadFile	admin	2018-06-23_03-00-10_777.jpeg	allan-demo
<b>Blockchain metadata:</b>					
<b>Block Number:</b>	103				
<b>Log Id:</b>	c5220fa7-7be6-45cb-9ea6-470a664de2f9				
<b>Transaction ID:</b>	cb2081764cb0727c32963840c7376b07e8f4dc11b0a1ca6237352ee84fe029d7				
<b>Block Hash:</b>	983df2fdd4478d299dbd14d8c3b0a89ba07bebf2ad3c4f3f079cad6b08f0fbaa				
<b>Previous Block Hash:</b>	b8a02a13d856b050438178e47fb6bbe95a02ff7da2cc7ce009b53c8a25199d11				

## BLOCKCHAIN OVERVIEW - HYPERLEDGER

Leonovus has selected Hyperledger to be the platform for developing its blockchain-based compliance audit capability. Hyperledger is the leading enterprise private blockchain infrastructure solution focused on enterprise business to business collaboration and is not restricted to any one industry or market segment. The Hyperledger project comprises over 250 companies with more than 3.6 million lines of code written to date.

Originally created by the Linux Foundation, project members now include companies such as IBM, Cisco, Intel, Red Hat, VMware, Accenture, Wipro, DTCC, SAP, AMEX, JP Morgan, SWIFT, CLS Group, and many others.

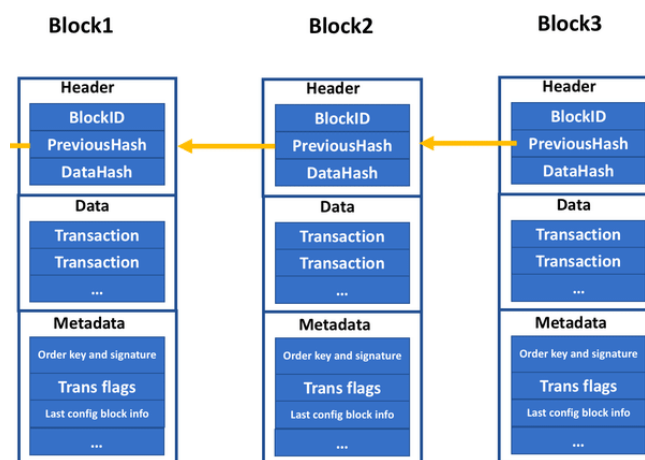
The Hyperledger project is a framework for multiple blockchain initiatives that promote the development and creation of projects targeting specific use cases. Leonovus is leveraging the work from the Hyperledger Fabric project and as such, an overview of Hyperledger Fabric is provided below. Additional details related to the Hyperledger project can be found at <https://www.hyperledger.org/>

Hyperledger Fabric is a permissioned blockchain infrastructure originally contributed by IBM, who continues to be the most active contributor of the Fabric project. At the heart of a blockchain network is a distributed ledger that records all the transactions that take place on the network. A ledger is just a specialized distributed database implementation.

A blockchain ledger is said to be decentralized because it is replicated across multiple network nodes, where each node contains a copy of the ledger. The blockchain ledger is deemed immutable, because each entry on the ledger is cryptographically linked to previous ledger entries, such that ledger entries cannot be modified or changed after the fact.

A permissioned blockchain means that all participants interacting with the ledger must be registered and authenticated. In this sense, the blockchain ledger is closed and controlled based upon the role/privileges granted upon participant authentication.

The Leonovus blockchain implementation has been designed with security as a foundational component and leverages public key technology to provide security services. Digital certificates are used to authenticate participants on the blockchain and to ensure that all transactions on the ledger are from authorized parties. In addition, all transaction data is permanently recorded in data structures called blocks. Blocks are organized into a linear sequence over time, with each block including a cryptographic reference (hash) to the block that came immediately before it, along with a hash of all the transaction data specific to the block itself. In this sense, any tampering with a block of transactions will be immediately detected as the cryptographic validation checks are performed against a chain of blocks as shown below.



The block header section is comprised of three fields:

1. **Block number:** an integer starting at 0 and increasing by 1 for every new block appended to the blockchain
2. **Current block hash:** hash of all the transactions contained in the current block
3. **Previous block hash:** a copy of the hash from the previous block in the blockchain

It is the automated validation of the block header which provides the immutability of the ledger. If an attacker were to attempt to modify or delete individual transactions, not only would the block in question no longer validate cryptographically, but all newer blocks would also fail validation checks.

Each transaction is digitally signed and automatically validated as part of the process of adding the transaction to the block, ensuring authenticity and integrity.

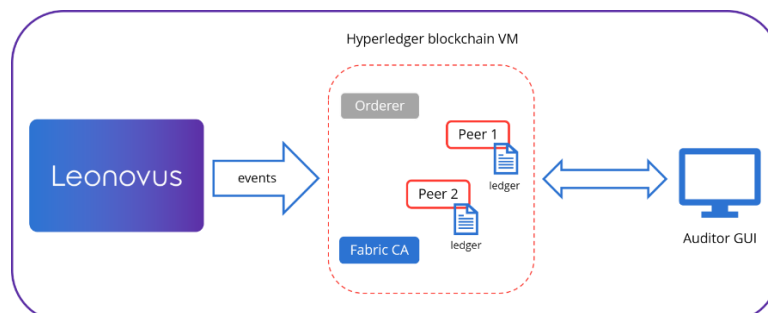
In terms of creating a trusted and immutable audit trail, blockchain technology is a perfect fit for recording Leonovus Vault file events as it provides the assurance organizations require in terms of the files that have been migrated to the cloud, who performed the operations, who has accessed the migrated files, the file operations performed and the timestamps of the operations. The fact that all transactions and blocks are cryptographically linked means that it is impossible to tamper with recorded events ensuring the immutability of the Leonovus audit trail. It also means that a permanent recording/history of Leonovus events is maintained all the way back to the first block in the blockchain with cryptographic integrity.

## HIGH LEVEL ARCITECTURE

---

The Leonovus blockchain implementation is based upon a private, permissioned model such that Leonovus Vault is the only 'author or entity' that has ability to write events to the ledger. All other roles are assigned auditor level privileges only. Auditor privileges enable the viewing of all Leonovus Vault events recorded on the ledger in a read-only mode. In this sense, the Leonovus blockchain implementation has been further locked down such that there is only a single source/initiator of events written to the ledger: the Leonovus Vault instance.

From an implementation perspective, the Leonovus blockchain implementation is comprised of a set of docker containers that can reside within a single virtual machine or across multiple virtual machines depending upon availability requirements. If, for some reason, the blockchain-based logger is unavailable, Leonovus Vault holds the events until the blockchain services becomes available, such that there is no loss in the audit trail.



## SUMMARY

---

From a compliance and audit perspective, Leonovus allows organizations to select the level of audit trail that best meets their internal and external compliance requirements. For the majority of customers, the ease of syslog integration to their SIEM/Syslog servers and the richness of SIEM analytic and reporting tools will make syslog-based audit trails the logical choice.

For organizations with higher audit assurance requirements and desire for an immutable audit trail of all file access operations, the Leonovus Blockchain compliance auditing solution can be used to address these needs. Leveraging the Hyperledger Fabric project provides both a stable and future-proofed platform for creating and accessing long lived immutable audit trails.

With these flexible auditing capabilities, organizations can not only have confidence in the security of data that has been archived and tiered to the cloud, they also have complete visibility into who has accessed their data, under what conditions and when. Having this level of insight and control, independent of the cloud service providers, is critical to retaining and proving sole control over sensitive data residing in the cloud.