

sayFUSE Backup & Restore Platform

Data Security Concept



Table of Contents

1. Preamble	3
2. Target Identification	4
3. Projected condition	4
4. The concept of Security	5
4.1. The sayFUSE Backup and Restore Platform	5
4.2. The 1st and 2nd Security Level / Secondary Application Conditions	5
5. Enclosures: sayFUSE Backup and Restore Platform	9
(The Platform of the Backup process and Restoring)	
5.1. The Security Concept on New Data (renewal, updating your existing sayFUSE system)	9
5.2. A four-stage Data Security	11
5.3. Data Transfer Capacity (Transfer Capacity)	12



1. Preamble

High data security always requires concepts prepared according to requirements. Technical failure, user error or data loss after a cyber intrusion, the breakdown of server systems and not being able to use the archives are problems that many companies have been encountering. It should be possible to re-establish the scheme securely by recalling the data via the backup infrastructure in such an occurrence. According to research done, as a result of a fault or an intrusion, companies are unable to reach 70% of their data. Unfortunately, plenty of security systems have been unsuccessful to date. This might be the outcome of the inadequacy of the existing Backup solutions and technologies or the result of the damaged data recording outline. sayTec has been analysing these problems for a long time and thus has developed the high security Backup and Restore Platform as a result. This solution not only covers all the expectations which might be needed for effective promoted data security but also all the technical and legal obligations.

The IT infrastructure determines the schema of the data security process and the factors that can affect all this structure and the system network. The contributing factors are generally the used server systems, the data volume, the data banks and the frequency of change. The sayFuse data security concepts takes all the problems above into consideration and gets the IT substructure ready while providing high data security. In order to realise the concept, it is essential to determine the hardware and software solutions and to check the functions regularly.

The conditions of a properly operating data security are to reach the data by the system when required, to officiate most systematic tasks and to document these actions clearly.

A unique high-speed backup with up to 12TB/hour for Live backup and up to 18 TB/hour for migration backup.



2. Target identification

The aim of the Data Security Concept is to maintain the security of the usage of the data and to protect both the data and the server in the event of a server collapse. In this regard, the aim is to meet the current and future expectations of the sector at the highest level. It is essential to keep the concept operational in case of necessity and sustenance of broad-based data handling by taking the physical and virtual frame into consideration.

In order to reach the ideal solution, it is necessary to transfer the periodically recorded data to an external environment in other words to an integrated module. For this reason, it is essential for the Backup and Restore Platform to be easily accessible in order not to experience any scaling problems during data backup. It is not to mention that the accessibility of the infrastructure and the scaling systematic is of great importance. One of the most critical part of the data security strategy is that the data backup can't be changed by third parties or ransomware.

At present, data security doesn't only mean securing the data. Data security also means that businesses must enable security by insuring themselves in some way to be able to be working in critical times. The demand of some operations that must be performed by Backup and Restore Platform such as archival storage, virtualization repository and migration is increasing day by day. However, the point that must be given great significance is that while performing such secondary functions, the primary applications should not be affected negatively by these procedures. In other words, real security is to be able to always start-up systems and infrastructure reliably and fast during a disturbance or after an intrusion.

3. Projected condition

The expectations towards ever-mounting throughput and information technologies have made uninterrupted data security and communication inevitable. In that it may lead to great loss for an operation not to be able to access data and to have its infrastructure collapse.

The sayFUSE Platform not only performs the primary and the secondary security operations of the Backup and Restore process but also deactivates the system and enables to reach the data in a very short time in the event of a disturbance or shut down of the infrastructure. Should the need arise, two sayFUSE gadgets may be clustered. sayFUSE is designed to put all the necessary factors within the system together without requiring any new software or hardware. In this manner the technological infrastructure has been made more secure and operational expenses have decreased measurably.

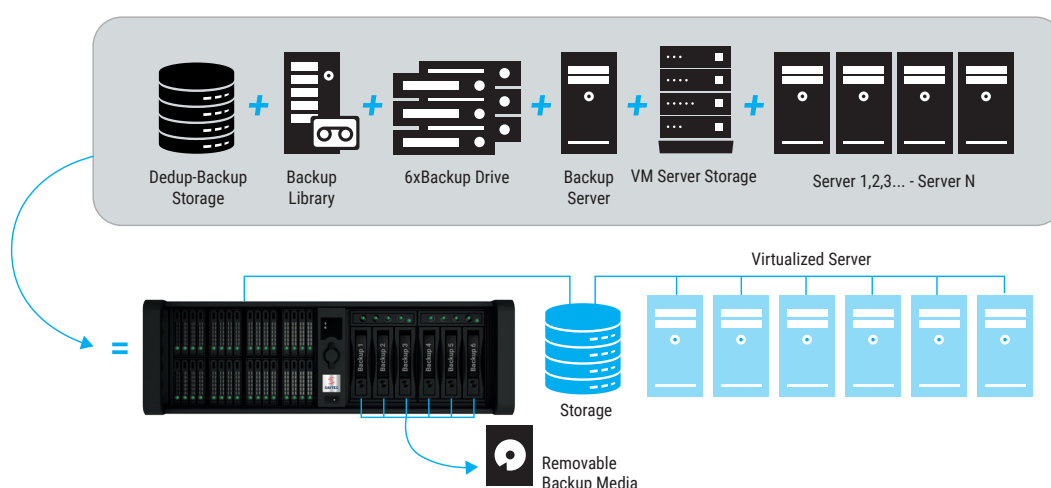
The sayFUSE Backup Platform provides the fundamental four operation stages which are a must in a secure strategy, within one application.



4. The Concept

4.1. The sayFUSE Backup and Restore Platform

Data security in companies by setting up the Backup and Restore Platform in every stage. The Backup and Restore Platform regards both the primary and the secondary stages of the application stages. Thus, sayFUSE meets all the needs in such cases as data recovery, migrating data to an external source, data security, the availability or the shutdown of the system. Your existing IT infrastructure is optimized via the Backup and Restore Platform and so not only the security of your data is enabled but also the possibility of a shutdown is eradicated.



4.2. The Primary and secondary security level

The concept covers primary and secondary security operations and the secondary application operations. Thus, systems defined as critical are operationalised in a very short time as a secondary application system by sayFUSE in case these systems are disabled.

The first security stage cluster1/ data processing centre 1; from the operation network to the Backup or Dedup Storage of sayFUSE. This data security steps in everyday as the first security stage. The daily backup records are kept here at least for one week and it steps in when required during the stage of reloading of the data to the system. Apart from this, if each server is disabled the data in each of them can be reloaded.

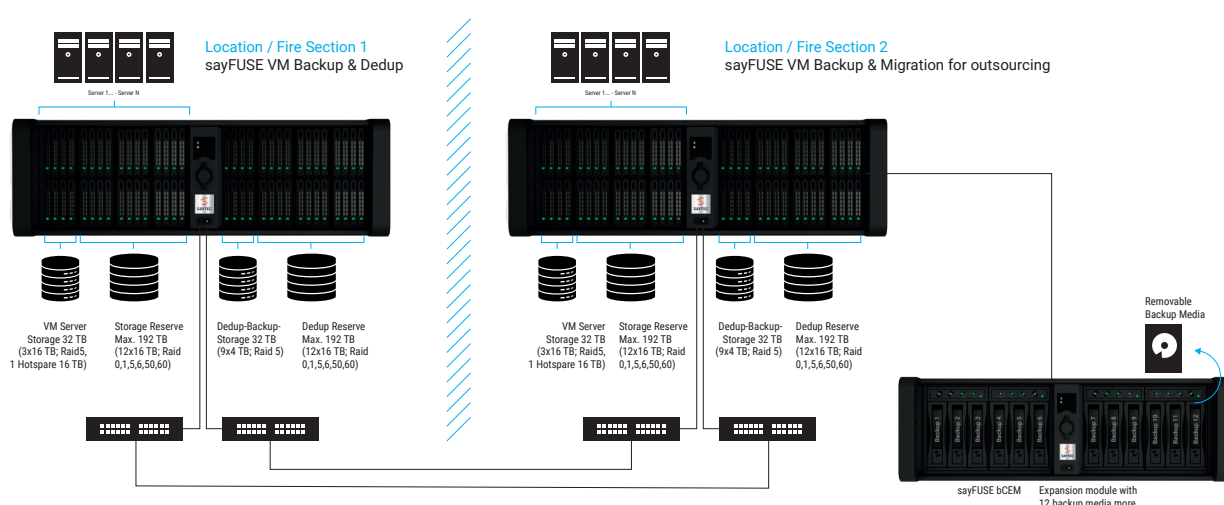
The secondary security stage is always made up through migration without blocking the network volume (and so without intervening the systems with critical



priority). The backup of the whole is made up within the daily and monthly backups in sayFUSE through Migration. These backups, on demand can be transferred to a more secure external source with a mere command. A reasonable distribution in terms of security (with virtualisation, according to data and with controlling server systems) enables flexible and fast intervention possibilities. Thus, data can be recovered by reactivating the systems in the primary security. The systems disabled can be renewed or repaired.

sayFUSE Backup

Concept: Dedup & Migration + Failure & Availability



The migration of the secondary security stage can be transferred to another 2nd cluster in a 2nd data processing centre within sayFUSE via Backup/Dedup Storage found in the primary security stage.

A reasonable distribution in terms of security (with virtualisation, according to data and with controlling server systems) enables flexible and fast intervention possibilities. Thus, data can be recovered by reactivating the systems in the primary security. The systems disabled can be renewed or repaired.

The secondary application conditions/rapid intervention ability

The infrastructure and systems with priority can be enabled directly through the application of sayFUSE. For example, in the event of a complete collapse of the server system (software and hardware). The infrastructure or server systems set with priority are backed up daily through the sayFUSE Platform by being installed off and online. When a system with a priority of being critical collapses, it is deactivated within sayFUSE within minutes. Thus, a maximum availability and recovery for critical infrastructures will be reached.



The monthly backup of data should be sufficient to maintain the whole security of the network, the data and the server. It is necessary that the monthly backup is archived and saved for 6 even for 12 months. At the end of the archiving period, the capacities can be used again. It is possible to connect a second Backup and Restore Platform to the sayFUSE capacity extension module (bCEM). 18 Backup drives each of which has a 14 TB capacity (uncompressed), are transferred through the first migration data centre of sayFUSE Backup Dedup to the second data centre. Up to date a capacity of uncompressed 252 TB can be externalised with such a configuration.

Upgrading the sayFUSE system via a new Backup and Restore Platform is beneficial as the existing backup media can be used even after further upgrades. The sayFUSE technology is both up and down compatible which enables the usage of existing media respectively the restoration of the located fuse.

The concept supports both the physical and virtual frame. That's why it can operate with broad-based data processing and can be kept ready to use according to requirements. In addition, the Backup and Restore Platform is always fast and easy to scale and is perfectly equipped to meet all the future expectations.

The sayFUSE Backup and Restore Platform is also available for additional fields of usage without affecting the secondary field of usage of the primary objective. These fields might be listed as follows: archiving, virtualising storage and migration, the virtual server and other means of storage.

Munich, 2024

sayTEC AG



5. Enclosures:

The sayFUSE Backup and Restore Platform (The Backup and Recovery Platform)

5.1. The improvement of your new data security concept (renewal, upgrading your existing sayFUSE system)

By upgrading your sayFUSE Backup system, your existing security concept will be extended by adding the new functions offered by the Backup and Restore Platform.

The new sayFUSE Platform provides you with significant characteristic features. Very fast data backup and the data availability of critical businesses take care of data security and recovery. It is a necessity to clarify some points for the optimal implementation of the system:

Detection and Setting Priority

- Application data, System data, Software, Protocol data
- Business Continuity, Critical Systems
- Full Backup, Incremental Backup, Migration and transferring to an external environment
- The Cluster System of the sayFUSE Platform to maintain availability at all times and Disablement

Threat Scenario

- Dependence; the sustainability of usual workflow in a company (data base and IT systems)
- Typical cases of danger, uneducated users, shared data bases, computer viruses, external threats and intrusion, power cut off, failure of backup devices and environment.
- Possible damages inflicted in a business
- Inflicted damages in buildings

Influencing factors for each IT system

- Specification of the data to be secured according to the attribute
- To make IT applications suitable for the usage of data
- Reconstruction of data without data backup
- Data Volume
- Data Volume that is to be changed
- Timing of Data Change
- Given Duration
- Confidential Data Situations
- Data Integrity
- Experience of IT users and qualifications respecting IT



Backup plan IT system

- Making a reasonable job plan by grouping security
- Setting priority without affecting the daily workflow of a business

Specifying Data according to their types

- The form of Data Security
- Frequency and timing of Data Backup
- The number of Data Generation
- Data Backup Environment
- Individuals responsible for Data Backup
- The Location of Backup Units
- Obligations owed for the Backup Archive
- Transfer Rules for Data posted to External Sources
- Restructuring Process of Data Backup

Planning the steps in case of Restoring

- Determining the Terms of Use of the Archive where Data is Backed up securely
- Making up a Contract (for Archives of which the Infrastructure is in an External Environment)
- The Frequency of Data Security Update
- Inventory Catalogue
- Deleting Data secured previously
- Demolishing Data Environments that are no longer usable
- Maintaining the use of Readers that are viable

Minimal Data Security Concept

It is necessary to create a data security concept which meets the minimum requirements of Data Security. This includes descriptions of how to achieve Data Security, how to be able to restore Data, which parameter to choose and which hard and software to use.

Regular Exercises with application on Restoration for Employees responsible for Data Security

Every business backs up its important data regularly, particularly the data about its customers. However, if these aren't tested periodically on whether the data is im- portable, in case of a real fault, it is probable that this stored data is not usable any more or it is also possible that this data might not be recalled. It may lead to a total loss or even to a wind up of a business if customer data is harmed.

Test Questions

- Are the Restore Tests being carried out regularly?
- Are the relevant IT systems listed in the Data Security Concept?
- Is the responsible employee informed about the details of the concept respecti- vely about some parts of it?
- Is the implementation of the Data Security Concept regularly checked?
- Are the necessary requirements met for the system, the IT infrastructure to be externally backed- up?



5.2. The 4-step generation backup concept

Through Multi- Back up- Drives, Multi- Steam and Migration, the speed of Restoration and Security with sayFUSE has risen over average. A lot of Terabytes of Data can be secured and stored in an external environment within a couple of hours.

Step 1

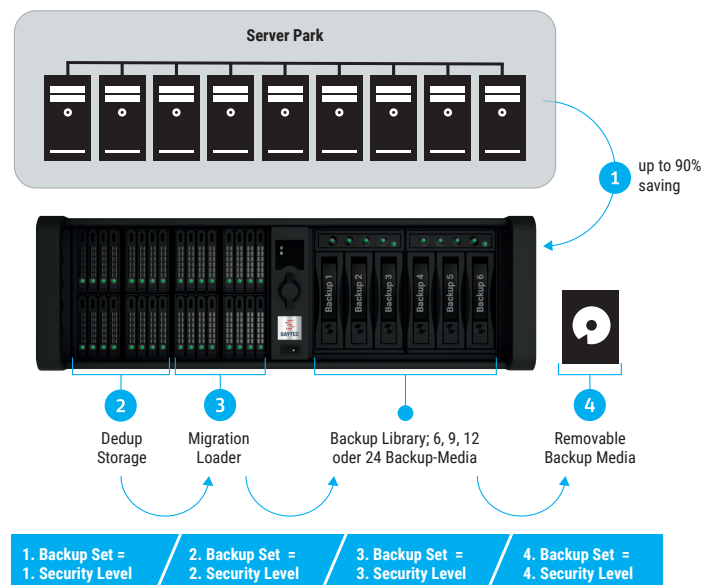
The first stage begins with a real complete Backup in the part called Backup-Dedup-Storage located in sayFUSE. This process not only saves time but also creates the first secure database by reducing 90% of the burden on the network.

Step 2

In the second stage, the backup drive configured for this purpose is switched on by job control, and the daily backups are migrated from the Backup / Dedup-Pool to the corresponding media within the sayFUSE appliance. After finishing the Backup, the security drive is switched off. While all of these processes are done without any external interference, time and Network resources are saved.

sayFUSE Backup Dedup und Migration

- 1 First backup level**
The data backup is based on SayFuse DedUp unit with up to 90% reduction
The backup dataset (first backup set).
- 2 Second backup level**
From the DEDUP backup record the daily security on the corresponding Drives written.
Time and space saving.
The second backup set runs within the Sayfuse without network resources.
- 3 Third backup level**
The backup phrases can be fully Weekly / monthly fuses are migrated.
Time saving. This process is running automatically in the background of the Sayfuse.
- 4 Fourth backup level**
Outsourcing into a secure environment.



Step 3

In the third stage, the Backup Clusters migrate the daily changes of the weekly or monthly stored Data automatically in the background (within the Appliance). At the same time, the configured backup drives are switched on with the backup job and the backup Data is checked for consistency. After the process of storing, the Backup Drive is switched off first and then the preparation for outsourcing begins. This saves the security from attacks, saves energy and increases the lifespan of the stored Data.

Step 4

The fourth stage is the process of transferring Data to an external source. With one touch of a button, the stored Data can be removed from the Backup unit and then it can be transferred into a saved environment.

The Data Security is reasonable according to the generation principle (Grandfather, Father, Son). Generally, the loss of Data is not noticeable until sometime. Through database-driven backups after the Generations principle, data or entire systems of a past time can be restored.

According to this method, the Backup environments are specified as follows:

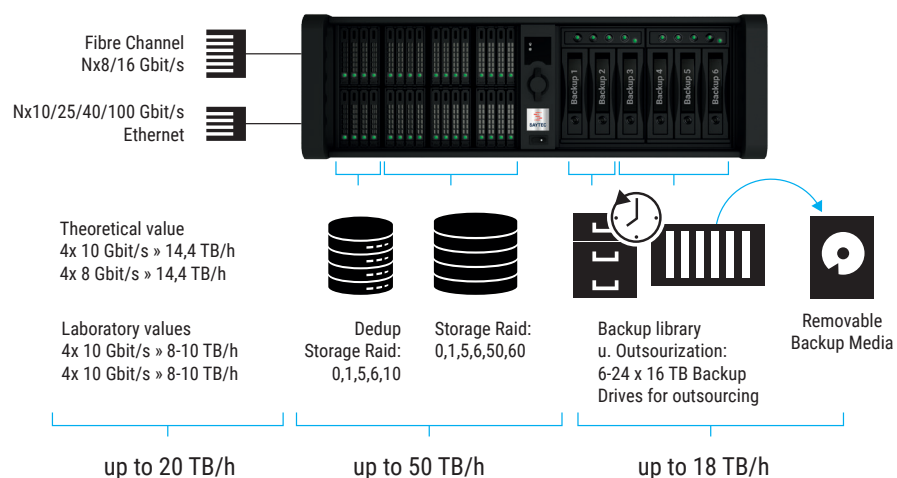
1. Daily Backups on the day of the following week
2. Weekly Backups in the same week of the following month
3. Monthly Backups in the same month of the following year

Therefore the back pursuit is guaranteed for a whole year (with 21 media).

5.3. Data Transfer Capacity

The Data Transfer Capacity depends on many factors such as the volume of the digital Data which are transferred in a transmission channel within a period. For a continuous Backup concept, all the factors must be taken into consideration. In order to save a great amount of Data, to replicate them and to store them, all interfaces, topology and storage drives for outsourcing must be considered.

In our present era, when large volume Data is used, it is possible for us to secure Data with a capacity of 100 TB or more within a day or at the weekend by backing it up to an external environment and to make the data ready for restoration.



high-speed backup with up to 12TB/hour for Live backup and up to 18 TB/hour for migration backup.