

RazorSafe 7-Series

Remote Backup and NAS Support



TABLE OF CONTENTS

Background	3
Email Lifecycle	3
Tape Backup Solution	4
Raw Email Backup.....	4
The Challenges.....	5
NAS Backup SoluTion – RazorSafe AOS 5.x.....	6
Filesystem Backup	6
NAS Backup Configuration	6
Enhanced Search Retrieval	7
Full Restore without index rebuilding	7
Tertiary storage - Off site Backup	7
Data Lifecycle.....	8
Required components	9
Conclusion	9

REMOTE BACKUP AND NAS FUNCTIONALITY

BACKGROUND

RazorSafe is a purpose built compliance archiving appliance. It offers a set of features to allow the customers to discover the items based on certain criteria such as relevant keywords. Essentially, it serves the purpose of corporate governance and selective email recovery.

RazorSafe fetches the emails from a journal account of the email server(s). It then disassembles and indexes the messages, and so makes them available for searches. RazorSafe consists of a number of subsystems: administration, end user search facility, indexer and data management. The following sections focus on the data management and discuss the options in data protection and data lifecycle management.

EMAIL LIFECYCLE

When an email gets in the RazorSafe, it undergoes different phases in the system, before they get to the state that they become searchable. The following diagram shows how the emails go through the five stages, namely “fetcher” -> “shredder” -> “indexer” -> and “archiver”. The primary difference of the email throughout the lifecycle is that before the “shredder” process, the emails are in complete raw form, and the emails are split into different mime document after the shredder. The mime documents can then be further processed for the purpose of de-duplication and compression. This paper will focus on the subject on how the raw form and the shredded form are being handled differently in the tape backup and NAS backup.

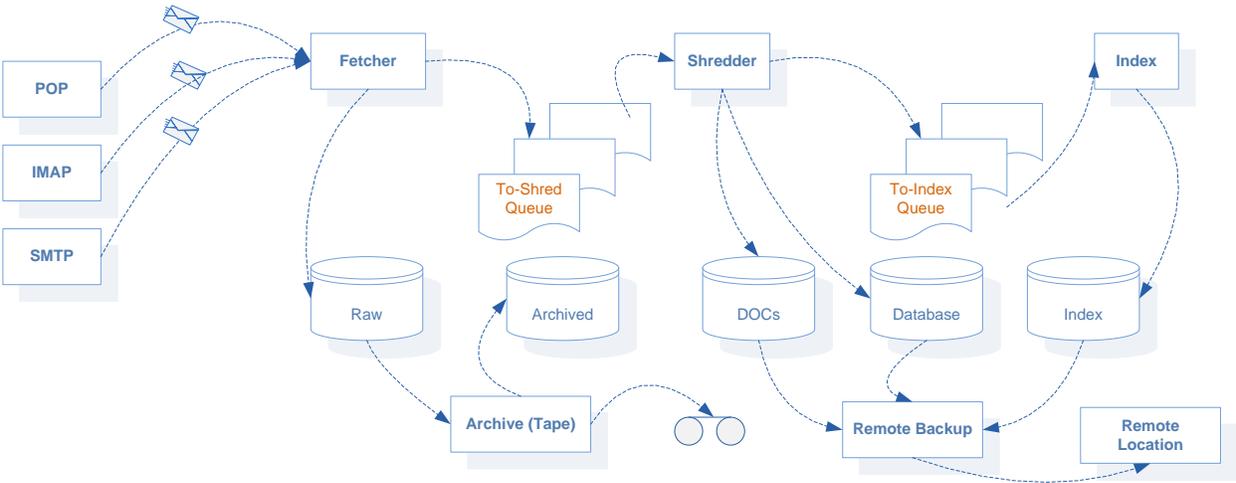


Figure 1: Email Lifecycle

TAPE BACKUP SOLUTION

RazorSafe comes with a native backup solution. It is a backup solution built in accordance to the nature and requirement of compliance archiving. What it does is to backup the “raw form”, specifically the Outlook .eml form, of the emails to the tape which can be set in WORM (Write Once Read Many) mode. Since they are backed up in the raw form, when the emails are read or restored from the tape, they come back in raw form.

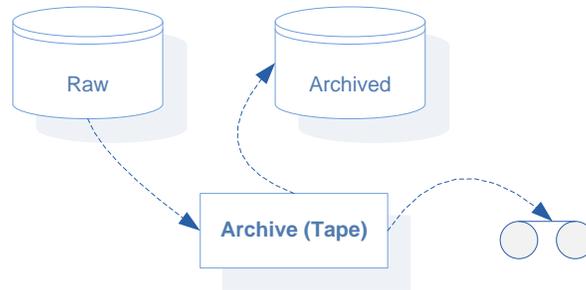


Figure 2: Tape Archiving

RAW EMAIL BACKUP

The RazorSafe’s raw email backup can be scheduled using the “Daily Backup” functionality. Despite the naming, the backup schedule can be set up as per-day or at a more granular interval such as every 2 hours. Since RazorSafe is built for compliance, the emails are not supposed to be modified in any way, so the built-in tape backup facility simply back the ‘delta’, (essentially the newly added items) up to the tape.

So, it is different from the typical backup solutions offered by the vendors such as Symantec Veritas, EMC Legato or Windows backup. Those backup solutions will allow full backup and incremental backup. For RazorSafe, it is always incremental. For this particular reason, there is no concept of full backup, which is a normal practice for the customers, especially during the weekend.

THE CHALLENGES

Because of the compliance nature of the RazorSafe's native backup, it comes with a few challenges:

1. The tape cartridge cannot be recycled. The backup is always the delta, and more importantly, they can be set as WORM.
2. When the emails are restored from the tape, they are in raw email format. These emails will need to be reindexed before they become searchable. This can take a week for a Terabyte of data to be processed.
3. Due to the nature of the tape and tape library, for any emails that are to be retrieved (the functionality in the search facility), the RazorSafe will query against its inventory and load the specific tape (with the specific label) into the drive, and load the emails from there. This could be a lengthy process especially when the tape is not already in the drive, or in the magazine of the tape library.
4. Choice of the tape library is limited to the list of certified tape libraries.

FILESYSTEM BACKUP

The NAS based backup is basically an echo of the RazorSafe’s file system onto the NAS. The backup image is encrypted, so there is no concern of the email content being exposed directly from the NAS. On the other hand, because of the nature of the filesystem backup, RazorSafe’s NAS restore is always a full restore.

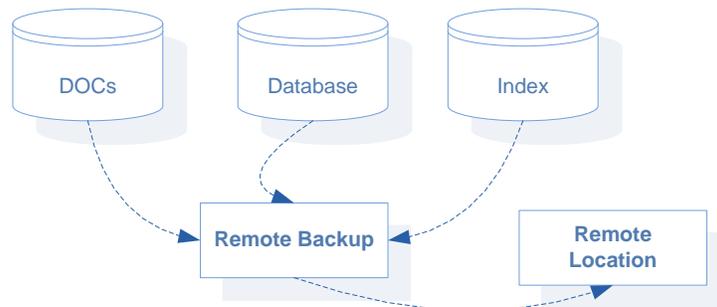


Figure 3: Remote Backup

NAS BACKUP CONFIGURATION

The configuration is fairly straightforward. The following is the screenshot of the NAS configurations, all the necessary settings are indicated in the fields below.

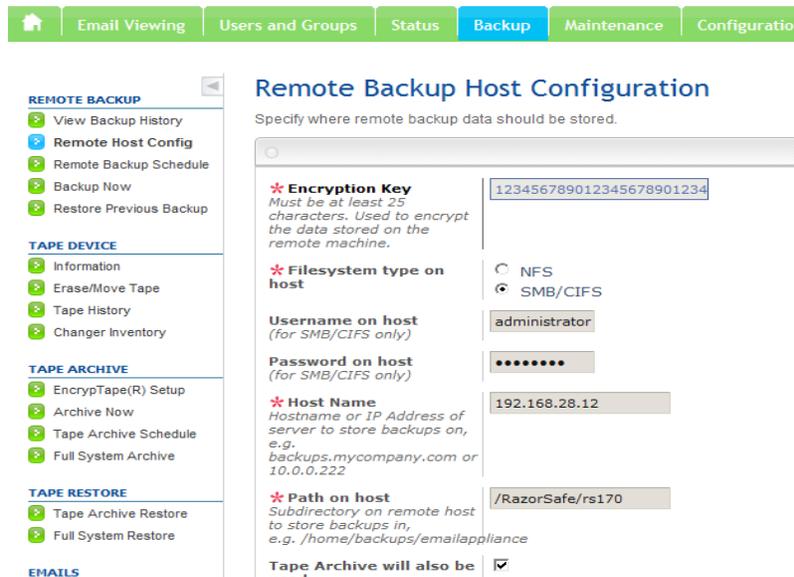


Figure 4: Configuration

ENHANCED SEARCH RETRIEVAL

NAS is based on random accessed disk based storage, direct email retrieval becomes straightforward, comparing to the sequential access nature of the tape. In AOS (Archiving OS) 5.x, Mirapoint made further improvement on the retrieval so that the retrieved emails will be presented at the native Search's returned table, rather than a separate "retrieval items" under the tape retrieval facility. As a net result, end user doesn't have to traverse away from the search menu to view the items that are not on the primary storage.

FULL RESTORE WITHOUT INDEX REBUILDING

Since the NAS backup image is already in the post-index form (i.e. the backup image contains the indices and database), RazorSafe will not need to rebuild the indices. So, for a full restore, it is about how fast the RazorSafe copies back the backup image. It is normally within a day for a Terabyte restore.

TERTIARY STORAGE - OFF SITE BACKUP

For the customer who wants to perform off-site tape backup, instead of backing out of the RazorSafe directly, we suggest a backup out of the NAS. The NAS can be accessed using the standard CIFS/SMB or NFS clients, the Windows filesystems or Unix filesystems backup utility can treat the RazorSafe's NAS just likes any other file servers. With this, customer can then apply the same company's data protection policy on RazorSafe.

DATA LIFECYCLE

The following table illustrates the data movement when secondary and tertiary storage subsystems are deployed. The secondary storage is basically the NAS based backup solution built within the RazorSafe system. While the tertiary storage is outside the scope of a RazorSafe solution, it can easily be achieved using the conventional file based backup solution.

Canonical order	Primary Storage 	Secondary Storage - NAS backup 	Tertiary Storage - Tape backup of NAS 
Before NAS backup	All items		
After NAS backup	All items	All items	
After Tape backup (e.g. off-site requirement)	All items	All items	All items
After retention policy	All items – Aged items	All items	All items
Full restore from NAS	All items – Aged items per last backup image	All items	All items

Figure 5: data Lifecycle

REQUIRED COMPONENTS

1. RazorSafe 7series, AOS 5.0 (no software license needed)
2. Annual maintenance subscription
3. RazorSafe's NAS system

CONCLUSION

The coming of AOS 5.x brings a higher level of flexibility that we can now perform a full restore without the prolonged index rebuilding process. In addition, the aged content that reside on the NAS can be accessed by the RazorSafe system and made available to the search subsystem. Essentially, the end user will be able to directly view the search results even though those items have already expired by the data retention policy. This eliminates the lag time in email retrieval when tape backup is utilized. Ultimately, customers are getting the benefits on both the data protection and search extension.