

MICROSOFT EXCHANGE BACKUP & RECOVERY SOLUTIONS

Mark E. Donaldson

How does the retention of backed up data differ from that of archived data?

Unfortunately, the answer depends a lot on the context. In general, when someone says "backup retention policies," they are referring to a backup application's definition of a retention policy, which is typically established at the backup media level.

Fundamentally, if a backup tape is created and managed by the backup application, the backup retention defines how long data on a given tape or tapes will be preserved prior to being eligible for tape overwrite, and therefore data removal. In this model, after the retention period of the media has expired, the backup media space is made available for overwrite; new backups (tape recycling) can then use the same media.

In most implementations, if the tape is not present in the tape loader, or is set up to prefer new media first, expired tapes are never overwritten, and data can be accessed by scanning/or cataloging the tape data. A variation on this theme is that each backup session is given a specific retention period and is expired first from the catalog; when all sessions are expired, that tape is (eligible) for recycle. The data in most cases could be recovered if absolutely needed. Some products combine both methods.

Traditional backup products also leverage disk as a target, but in many cases the retention model is the same. If you are performing hot backups of the Exchange databases, the retention is at the database level, not the individual message level. If you are also performing brick-level backups, in most cases, the retention period is at the session level; this means all mailboxes backed up at that time are retained and disposed at the end of that period.

Again, depending on context and implementation, an archive retention period should use date attributes within the data, for example a file's creation date, or a messages "sent or received" date. In this model, the retention period is managed by collecting and persisting metadata at archive time, and the application manages and disposes of the data or messages based on this time, regardless of when the archiving application first saved it.

Is there a way to create a hot swappable backup file for Exchange and save that file on a backup Exchange server as a source of failover protection?

Creating a usable Exchange backup requires utilizing a key Microsoft technology that allows for online backup of Exchange at the storage group level. These APIs are also referred to as the "ESE Backup APIs." Backup and storage vendors implement these APIs in their hot backup agents. One key function of these APIs is to properly "quiesce" the Exchange database so that all data is committed to disk. Then, the API allows for the data movement of the EDB, STM and associated logs. In this model, when the hot backup is done, the data files are encapsulated in the backup agent's tape format. From this backup, the data can be restored by sending it back through the ESE backup API.

There is also Exchange server clustering that provides another method for failover; however, it is not able to prevent logical corruption.

The ESE backup API, when running on Exchange 2003 and Windows 2003, provides new functionality in VSS (Volume Shadow Copy Services).

"The Volume Shadow Copy service coordinates communication between Requestors (backup applications), Writers (applications in Windows services like Exchange Server 2003, and SQL Server

MICROSOFT EXCHANGE BACKUP & RECOVERY SOLUTIONS

Mark E. Donaldson

2000), and Providers (system, software or hardware components that create the shadow copies). To use the Volume Shadow Copy service feature to backup Exchange Server 2003, the backup program must include an Exchange Server 2003 aware Volume Shadow Copy service requestor. Because the backup program that is bundled with Windows Server has no such requestor, organizations must use third-party backup applications."

These VSS hardware and software requestors can provide the appropriate calls to create an Exchange consumable snapshot, as it was properly quiesced, and move the data appropriately. For more information see KB article 822896. .

Bottom line: Without the use of this API, there is no Microsoft supported way of moving the file-level data safely. Be wary of third mirror break-off solutions that do not utilize the aforementioned technology. These would provide data that is application-inconsistent and would require both physical (ESEUTIL) and logical (ISINTEG) repair prior to use, and cannot guarantee data preservation.

Is it possible to use VSS/shadow copies of shared folders with Windows 2003/Exchange 2003 to get some previous version of one store group/Information Store in a day?

Good question. Yes, you can set up VSS to take a snapshot of your stores on a regular basis (i.e. hourly, every two hours, etc.). Then, if you have a VSS API-aware solution, you can read straight into the backup media to recover individual mail or attachment items. You can also search across all mailbox and attachment content throughout the store(s) if you're looking for information with specific keywords or other attributes.

What are "brick-level" Microsoft Exchange e-mail files?

Good question. "Brick-level" refers to a class of backup software.

Traditional Exchange backups focus on backing up the Exchange database in such a way that does not permit granular recovery of individual mail items. Most companies use this class of backup software. If individual items need to be recovered (i.e., as part of a compliance or Human Resources driven investigation, or because messages have been lost and no longer exist in the 'dumpster'), then recovery options are limited to:

Exchange 5.5 and Exchange 2000

- Building a recovery Exchange environment.
- Creating a MAPI profile to enable an Outlook client to log into the respective mailbox(es) or using ExMerge to log on.
- Exporting relevant content to PSTs.
- Importing relevant content back into the production environment or passing it on to Legal or HR for action as appropriate.

Exchange 2003

- Using a Recovery Storage Group (RSG) to recover the relevant database.
- Using ExMerge to recover the desired mailbox contents and merge them into the relevant production mailbox.

MICROSOFT EXCHANGE BACKUP & RECOVERY SOLUTIONS

Mark E. Donaldson

Brick-level backups use a different backup process in which they perform a MAPI logon to each mailbox as part of the backup process; this gives them the ability to recover individual mail items directly from backup media. It also facilitates recovery of single mail messages or mailboxes without having to build a recovery environment and without having to resort to RSGs.

One caution: Brick-level solutions are substantially slower at backing up your servers than traditional backup solutions. They also cost more and require significantly more backup media than traditional backup media.

If item-level recoverability is a requirement for your company, you may want to consider a hybrid solution instead of brick-level, namely either Quest Recovery Manager for Exchange (disclaimer: I work for Quest), Ontrack PowerControls or Mimosa NearPoint. All permit item-level recoverability using traditional backup methods without the long backup windows, licensing costs and backup media costs associated with brick-level solutions. I have seen many companies move away from brick-level recovery in favor of these solutions because their brick-level software was exceeding their nightly backup windows.

My question is on a single mailbox restore. If I am doing brick-level backups of the mailbox store (using Brightstor software), am I able to restore a single mailbox from a backup tape? The users do not have PST files. All Outlook clients are pointed at the mailbox on the Exchange 2000 server.

Yes, brick-level backup software will allow you (typically) to restore either a mailbox or an individual item from within a mailbox (i.e., message, post, contact, task, journal entry, appointment, etc.) from a single backup tape without having to build a recovery server.

That said, I actually recommend looking around at the solutions available ... there are other options. Brick-level backup software is expensive and slow. There are one or two vendors out there who provide the ability to get brick-level restore functionality *without* actually performing brick-level backups. In other words, these vendors can extract mailboxes or items directly from a standard backup tape/media.

I've heard of a number of cases where organizations are abandoning brick-level backup software because they have overrun their regularly-scheduled backup window -- in every case they are choosing brick-level recovery solutions as an alternative. Search for "message-level recovery" in your favorite Internet search engine and you should find some of these solutions.

An Exchange server has gone down. Is it possible to re-make the public files and mail with just the MDBDATA folder with a fresh install? If so, how?

I'm assuming that you are referring to recovering data in Exchange 2000. There are two primary ways to recover mailbox data, and one for public folder data.

Mailbox data can be restored back to the recovery storage group (RSG). It can also be recovered on a hot spare server.

To recover the public folder data, you would need to mount the database on a hot spare server that is isolated from production. Once you have the data back online, you can use EXMERGE or PUBMERGE to extract the data into .PST files -- then you can import that back into your production mail environment. Within the standard recovery context, you will lose the public folder data if you try to

MICROSOFT EXCHANGE BACKUP & RECOVERY SOLUTIONS

Mark E. Donaldson

recover it through the Mailbox Recovery Center in Exchange System Manager, because it only allows you to mount mailbox stores.

How can I get back my old Inbox after deleting it from Outlook 2003?

If Exchange Recover Deleted Items is enabled on your server, you may be able to recover your deleted items by selecting Deleted Items, going to Tools and then Deleted Items Recovery. If it is not enabled, it will be grayed out.

Another way to recover items is by using the Microsoft Inbox Repair Tool. You will need to ask your administrator to back up your mailbox to a .PST file and then run the scanpst.exe utility against the .PST file. There is also third-party software, such as 'Recover My Mail,' that may be worth a try.

We have public folders running on Exchange 2003. A user has deleted a subfolder within public folders. Although deleted item retention is enabled, the folder cannot be recovered -- even with full control permissions through the public folder hierarchy.

We receive the error, "Outlook was unable to recover some or all of the items in this folder. Make sure you have the required permissions to recover items in this folder and try again. If the problem persists contact your administrator."

I have full owner rights right through the tree and still cannot recover this folder. Any advice would be appreciated.

One thing you may want to look into is whether there were nested public folders *beneath* this public folder, and what permissions were set on the public folders nested *inside* of the folder you are trying to recover.

From what I understand, you need rights for the public folder that you are trying to recover, and all nested public folders *beneath* that public folder.

For example, if you had the following public folder hierarchy:

```
Top Level Public Folder #1
  L Public Folder A
    L Public Folder B
      L Public Folder C
```

Let's say you had permissions on Public Folder A and Public Folder B -- but no permissions on Public Folder C. If Public Folder A was deleted, attempting to recover it by viewing the dumpster contents, while highlighting Top Level Public Folder #1, will fail with the message you refer to. This is because you don't have rights on Public Folder C.

I suspect this is what you're experiencing, in which case you will need to resort to a backup. The two ways of recovering the folder from backup are (a) building a recovery server or (b) using a third-party solution to recover the public folder from backup to your production environment.

MICROSOFT EXCHANGE BACKUP & RECOVERY SOLUTIONS

Mark E. Donaldson

I need to recover all e-mails sent and received by two employees who recently deleted the entire contents of their mailboxes (before being fired). Since we want ALL of the messages sent/received, a particular backup won't do, since it would essentially provide a glimpse of what the mailbox looked like when the backup was run.

We do, however, have all the log files from the time the server was installed. Is there a way to reconstruct these users' inboxes and sent items entries (even for things that were subsequently deleted) from the log files only?

This is a great question. There is a field called "e-discovery" (electronic discovery) that applies to the kind of investigation you are performing. I have been doing a lot of thinking and writing in this area of late, as pretty well any investigation these days is touching on e-mail.

I'm not positive I understand which log files you are referring to (I am assuming you mean transaction log files), but that said, there is no feasible way to re-construct a comprehensive view of all messages for these two employees. The only way you would have this information is if you had a compliance archive in place for the duration of these employees' tenures with your company; and if you had explicitly configured the compliance archive to bifurcate all messages sent/received by these mailboxes.

That said, I'll explain what I believe are the best steps, given the data you're working with. Essentially, you need to make sure you are addressing all e-mail content from each of the following four "silos" of Exchange storage:

1. Online data: Whatever is in their mailboxes and dumpsters today.
2. Backup data: Whatever mailbox instances you have, for every generation of backup tape in you possess that relate to the servers hosting these mailboxes.
3. To manage these first two "silos," you may need to locate and recover mailbox instances for these two employees from all your daily, weekly, monthly and yearly tapes, spanning whatever number of months or years these employees worked for your company.

This can be extremely costly and time-consuming, so you may want to look at third-party solutions on the market to assist in search-and-recovery, rather than building recovery servers corresponding to all these backups. Two solutions exist that I'm aware of, Quest Recovery Manager for Exchange (disclosure: I work for Quest Software) and Ontrack PowerControls.

Numerous outsourcing companies also provide recovery services that you may wish to consider, depending on the priority of this content and the budget you have available.

Silos two and three focus on stray data.

4. PSTs: If you have access to any PSTs on the workstations these employees used, or on their network shares, search these as well.
5. Offline data: Finally, if you're trying to be really thorough (which is my assumption), search computers and network shares associated with these accounts for .msg files. You should also inspect any mobile devices (such as iPAQs, BlackBerrys, smartphones, etc.) that were used by these users to see if any additional messages exist that have gone under the radar.

MICROSOFT EXCHANGE BACKUP & RECOVERY SOLUTIONS

Mark E. Donaldson

I have a query about how to restore/recover a Microsoft Exchange 2000 server public and private folder to another Exchange server information store. My server SCSI drive is damaged and I can't re-install or repair. I used ESEUTIL.EXE to check and repair the said databases, but it's not working. Is there any third-party tool to recover all old mails and addresses to the new Exchange server?

Sounds like you're in a pickle. Well the standard response would be to restore from backup, but I'm assuming from your question that you weren't making backups. If that's a correct assumption, then first of all, put in that requisition to acquire some good Exchange-aware backup software. Then, have a look at an Exchange recovery solution.

Since your ESUTIL exercise failed, there's a chance that these tools may not be able to read your database either. If that's the case, and if you really need the mail, then you're left with having to take the database into a forensic recovery company to see if they can get the data out. That's typically pretty pricey, but it may be your only option.

I had to restore my computer and reinstall Norton Antivirus and firewall. I was able to set up three of our four e-mail accounts, but now I can't get the "real" e-mail for my account. Roadrunner was unable to help. I'm at a loss -- why do three accounts work and the other does not?

If you are using Outlook, I suggest you try to create a new profile with just the "real" e-mail account and no others. When you restored your computer, it's possible that some of the profile information pertaining to your e-mail account was damaged or lost. If this is the case, creating a new profile should fix the problem. If that works, you can then add the other accounts to the new profile.

If you are using Outlook Express, the article OLEXP: How to troubleshoot Outlook Express in Windows 2000 may help you.

My boss clicked yes to "auto archive" not knowing it was set to permanently delete. There is NOTHING in .PST, trash, etc. Microsoft said it's somewhere in the hard drive. Can you help?

It sounds to me like your boss has an Archive.PST file located somewhere on his hard drive or network home directory. Search the hard drive and home directory for all .PST files. Once you find them, take note of where they are saved, their size and their last modified date. Chances are the largest one with the most recent 'last modified' date is the one you want. Open it within Outlook and you should find the messages.

If you end up searching and not finding any more .PST files in the locations I specified, then it sounds like you are out of luck. You will need to recover your boss's mailbox from backup tape and then restore them into his production mailbox or into a .PST for his reference.

(As a last ditch effort you could also try asking whoever you spoke with at Microsoft what they meant when they said "it's somewhere on the hard drive," though I suspect they were just trying to point you to a local Archive.PST file.)

MICROSOFT EXCHANGE BACKUP & RECOVERY SOLUTIONS

Mark E. Donaldson

We have six Exchange servers with multiple storage groups and stores per server. Suppose we are asked to restore the mailbox of a user who was terminated six months ago. How would we know what server/storage group/store to restore from? What can we do now to ensure that we will be able to retrieve the information that will tell us the location of the former user's mailbox?

I recommend using some sort of standard mailbox provisioning philosophy in assigning mailboxes to the different stores on your Exchange servers, then documenting and tracking these configurations in a central Exchange configuration history document (you do have change management procedures in place for Exchange, right?).

As an example, you could assign all users with surnames A-F to store 1 on server 1, and so on. Or, you could provision all users in a given office to the same store. Then, when you're recovering mailboxes for whatever reason, you'll be able to figure out which server the mailbox was on simply by what you know about the user.

I have one domain and I would like to add another Exchange 5.5 server for redundancy; in case one Exchange server fails, the other can take over. What do I need to do for this to be successful?

Depending on the overall priority and budget associated with this project and the size of your company, there are several options.

First, you will want to have a good look at clustering technologies (and you'll want to consider moving to Exchange 2000 or Exchange 2003 at the same time), which essentially provide the ability to fail over from one set of back-end databases on one "node" of the cluster to another set of identical back-end databases on a "cold standby" node of the same cluster.

If your budget is sufficient and you require greater availability, you could investigate some of the third-party high-availability solutions that exist, including geoclusters (clusters in which the nodes are in different geographic locations), faster backup and recovery solutions (i.e., Windows Volume Shadow Copy Services (VSS)) or similar products.