Authority

EXCHANGE TO OFFICE 365
ARCHIVING CONSIDERATIONS

by Brien Posey

As an organization prepares to migrate mailboxes from an on premise Exchange Server to Office 365, it must carefully consider how the migration process will impact message archives. There are a number of different gotchas that administrators must be on the lookout for as they prepare for an Office 365 migration.

MESSAGE SIZE LIMITS

One issue that is easy to overlook is that Office 365 has a size limit of 25 MB per message. Most organizations probably don't have a lot of messages with 25 MB+ attachments, but if such messages exist, they can derail the migration process. Depending on the method that is being used, such messages could be omitted from the migration process, or the mailbox containing the migration of those messages might fail.

Similarly, mailbox size can also be an issue. The maximum size of an Office 365 mailbox varies depending upon the organization's Office 365 plan. An organization must ensure that none of the users' mailboxes exceed the capacity of an Office 365 mailbox. If local mailboxes are larger than the maximum Office 365 mailbox size, then archiving will need to take place prior to the migration process. This allows the mailbox size to be reduced so that it adheres to the Office 365 requirements.

Again, depending upon the organization's Office 365 plan, the archive mailbox might also have capacity limitations. Conversely, however, some Office 365 plans offer unlimited storage for archive mailboxes. If an organization's subscription plan has archive size limitations, then the administrator must make sure that each user's archive adheres to the Office 365 requirements.

This white paper details five considerations to keep in mind when deciding to migrate a message archive from Microsoft Exchange to Office 365.

They include:

1. MESSAGE & MAILBOX SIZES

2. UPLOAD TIME

3. RETENTION POLICIES

4. EDISCOVERY

5. THIRD-PARTY ADVANTAGES

ACCORDING TO IBM, EVERY DAY PEOPLE GLOBALLY

SEND

294

BILLION EMAIL MESSAGES

PUBLISH

230

MILLION TWEETS

UPLOAD

100

TERABYTES OF DATA TO FACEBOOK

UPLOAD TIME

Another common problem that an organization often experiences when migrating Exchange Server mailboxes to Office 365 is that the migration process can take longer to complete than what was initially estimated.

Microsoft offers two main types of migrations from Exchange Server to Office 365. Smaller organizations are able to perform a *cut over migration*. The simpler of the two migration types, cut over migration allows all of the Exchange Server mailboxes to be migrated at once without the organization having to establish coexistence between the two environments. It is worth noting, however, that cut over migrations are only supported for organizations that have fewer than 1,000 mailboxes and that plan to perform a full migration of all mailboxes.

The other primary migration technique that is supported by Microsoft is called a *staged migration*. A staged migration requires an organization to establish full-blown coexistence between the on-premise Exchange Server and Office 365, thus deploying the Active Directory Federation Services (AD FS) to manage identities across the two environments and setting up a dedicated physical or virtual server that will coordinate the migration process.

Staged migrations are a much bigger undertaking than cut over migrations. Even so, the advantage of a staged migration is that, unlike cut over migrations, mailboxes can be migrated in batches, allowing the administrator to pick and choose which mailboxes to migrate at a given time. Because staged migrations require coexistence to be established between the two organizations, there is no requirement to complete the migration process quickly. The on-premise Exchange Server deployment can coexist with Office 365 for an indefinite period of time.

As previously mentioned, however, the duration of the migration process can sometimes be problematic. There is no getting around the fact that larger mailboxes take longer to migrate. This simple fact can prove problematic regardless of whether or not an organization is performing a cut over migration or a staged migration.

In the case of a cut over migration, there really isn't a lot that an organization can do to prevent the migration process from taking an excessive length of time. When performing staged migrations, an organization has the ability to create migration batches that are sufficiently small, and can therefore be easily handled.

According to some estimates, Office 365 is able to handle about 400 GB of migration Data per day. While this figure can serve as a guideline, it should not be taken as absolute. Occasionally, Office 365 runs at a reduced capacity when Microsoft is performing maintenance. Furthermore, it's not always Office 365 that proves to be the limiting factor. An organization's own Internet bandwidth (or lack thereof) can significantly limit the volume of mailbox data that can be migrated within a 24-hour period.

As a best practice, administrators should begin the migration process by creating very small migration batches. Doing so will not only allow the migration process to be tested to make sure that it's working properly, but the duration of the initial migration batches can serve as a benchmark that can assist in determining the most appropriate size to use for later migration batches. Of course, this best practice assumes that an organization has IT staff with the expertise required for establishing coexistence between an on-premise Exchange Server deployment and Office 365. Establishing and maintaining coexistence is a complex undertaking that often warrants getting help from someone outside of the organization such as a third-party archive software vendor.

6 LESSONS LEARNED FROM EXCHANGE TO OFFICE 365 MIGRATIONS

Authority has assisted in countless migrations from on-premise solutions and other cloud-based products to Office 365. What did we learn from these projects? Here are some common lessons that we experienced when helping organizations make the move to Office 365.

1.

CREATE OR REVIEW YOUR RECORDS MANAGEMENT POLICY.

When migrating to Office 365, it's a great time to review or create a retention policy and best practices for email and document management. If you do not have a records management policy, now is the time to create one. The migration of legacy data into a new system can be costly in both time and money.

2.
HAVE A MIGRATION PLAN AND KEEP IT SIMPLE.

Change is always disruptive. Often, in the effort to mitigate the disruption, organizations either wing it, or overthink the process. Your migration plan should not be by committee. The more stakeholders that you involve, the more exceptions will be created to accommodate those who are adverse to change. The migration plan should accommodate areas of change management common to the entire organization, not just one department.

3.
MANAGE YOUR HYBRID ENVIRONMENT.

Especially when moving from Exchange to Office 365, most organizations will create a hybrid of the two systems to ease the transition. Be careful not to make this transition period too long. Email in two separate systems can be more disruptive than just flipping the switch to a new system.

If you choose a hybrid approach, think about leveraging your archive provider to help. You can archive both the Exchange environment and the Office 365 environment, and upon the completion of the hybrid environment, have the archive provider push email from the exchange system into Office 365 to assist with change management.

4.
MOST ON-PREMISE LEGACY ARCHIVING SOLUTIONS DON'T WORK WITH OFFICE 365.

It's very likely that you'll need to upload PST files directly into the new Office 365 environment. Having all historical data in the new environment is cumbersome and confusing. Look for a provider that can migrate the data from your legacy system into their archive and then push a period of the historical data into the new Office 365 environment.

5.
GIVE YOU USERS ACCESS TO AN ARCHIVE.

Users will want, or need, content from the prior system. By giving your users access to their own archive, they can find that content on their own and reduce he burden on an overworked IT department. By selecting an archive provider that has the ability to redeliver the content, users can easily restore that content into their accounts will minimal IT staff involvement.

6.
TRAIN. TRAIN. TRAIN.

Yes, Office 365 is similar to Exchange, but it's not the same. Make the investment to train your staff on the differences. This investment will result in an increase in productivity and morale.

Source: *Authority*, 2014

RETENTION POLICIES

The biggest archive related pain point that is often encountered when migrating to Office 365 has to do with the default retention policies. Unless an administrator understands the retention policies that are in place (and makes any required changes prior to migration), there is a possibility that data loss could occur shortly after the migration completes. Even if there's no actual data loss, unsuspecting end users could be left with the perception that a data loss event has taken place.

Retention policies have existed in Exchange Server for quite some time. However, an organization planning a migration from Exchange Server 2007 might be surprised to find out that managed content is handled much differently in Office 365.

Office 365 Exchange uses the concept of retention policies (just as Exchange Server 2013 does). A retention policy is a collection of retention tags that apply to various mailbox folders. These tags specify the age when folder content will expire, as well as the action that will be taken against expired items within the specified folder. The retention policy is assigned at the mailbox level. This architecture is designed to prevent administrators from having to perform granular folder level management on a per mailbox basis. Instead, the folder level settings all exist within the retention policy, and only the retention policy is applied to mailboxes.

Although retention policies (and the retention tags within them) are designed to provide administrators with control over message retention within various mailbox folders, administrators must be aware that Office 365 has a default retention policy that might not meet an organization's needs.

The default Office 365 retention policy is named *Default MRM Policy* and is located within the Office 365 Exchange Admin Center under Compliance Management | Retention Policies. Although the default retention policy contains a number of different retention tags, there are two tags in particular that tend to be problematic.

THE AVERAGE AMERICAN OFFICE WORKER CREATES

1.8 MILLION MEGABYTES

OF ELECTRONICALLY STORED INFORMATION (ESI) EACH YEAR.

Source: *Corporate Counsel*, October 22, 2014

The first of these tags (which you can view through the Office 365 Exchange Admin Center under Compliance Management | Retention Tags) is *Deleted Items*, which specifies that items within the Deleted Items folder are to be removed after 30 days.

Some organizations have policies in place that require deleted items to be retained for a longer period of time in case they are needed. For example, an organization might want to retain deleted items for 90 days. The problem is that if a mailbox is migrated to Office 365, then any items within the Deleted Items folder older than 30 days will automatically be purged soon after the migration process completes.

One way of getting around this problem is to apply a legal hold to mailboxes prior to migration. This gives administrators the opportunity to create a retention policy that is more appropriate for the organization, and then apply that retention policy to user's mailboxes prior to releasing the legal hold.

The other retention tag that has sometimes proven to be problematic is called *Default 2 Year Move to Archive*. Unlike the Deleted Items tag, this particular tag is not actually destructive. As the name implies, the tag moves mailbox items that are more than two years old to the user's archive mailbox.

The reason why this particular tag can be problematic is because it can give users the perception that mailbox items have been deleted. Archive mailboxes (otherwise known as *personal archives*) were not introduced until Exchange Server 2010. As such, users in organizations that are migrating from Exchange Server 2007 have never been exposed to archive mailboxes (at least not natively).

Even if an organization uses Exchange Server 2010 or Exchange Server 2013, there is no guarantee that users are currently making use of archive mailboxes. An administrator might have chosen to not enable archive mailboxes, or there might be some users who simply do not know what the archive mailbox is and what it does.

With that in mind, consider a situation in which messages that users have held onto for a specific reason are suddenly moved to an archive mailbox. Although the messages have not been deleted, users may be left with the perception that their messages are gone. This will likely result in confusion and calls to the help desk.

OTHER CONSIDERATIONS FOR MESSAGE ARCHIVING

When organizations evaluate message archive solutions, they must consider the eDiscovery process. It is extremely important for organizations to be able to perform eDiscovery against their message archives, to be able to place items on legal hold, and to export messaging data. Although Exchange Server and Office 365 do offer such capabilities, most Office 365 plans do not include access to the *eDiscovery Center*.

Even if an organization does subscribe to one of the Office 365 plans that includes access to the eDiscovery Center, the organization might find the eDiscovery process to be inefficient due to the amount of time that it takes to export large quantities of messaging data from a remote Exchange server.

This is especially true for products that store archived data outside of the Exchange Server mailboxes. Such a solution would allow an organization to keep the archives on premises while avoiding the complexities of Office 365 retention policies and mailbox quotas.

TRUSTING A THIRD PARTY

If an organization's on-premise Exchange Server deployment is making use of third-party message archival software, administrators must check to make sure that the solution is supported for use with Office 365.

Administrators should be aware of how the third-party message archiving solution stores archived data outside of Exchange Server. Some vendors rely on the use of PST files while others use databases or proprietary file structures. Understanding this will help prevent the link between the mailbox and any external archives from breaking thus creating an orphaned collection of archives.

Although Office 365 includes personal archives, organizations might be better off investing in an Office 365 compatible archiving solution from a third-party vendor than using the native Office 365 message archiving capabilities.

Only the Office 365 E3 and E4 plans currently provide archive mailboxes with unlimited capacity. Most of the other plans have a 50 GB limit.

With that in mind, imagine a situation in which a user exceeds the archive mailbox's maximum capacity. The user would essentially be required to purge data from the archive mailbox in order to make room for more data. This is obviously problematic if the data within the archive mailbox had been retained in an effort to satisfy operational or regulatory requirements. In contrast, a third-party archival solution eliminates the possibility that data will ever need to be purged simply to comply with Office 365 plan limits.

Migrating Exchange Server data to Office 365 is a complex undertaking that requires extensive planning. A big part of the planning process involves determining how the migration process will impact message archives, and how the organization can work around any undesirable consequences.

ABOUT BRIEN POSEY

Brien Posey is a 13-time Microsoft Most Valuable Professional (MVP) with two decades of IT experience. He has published thousands of articles and has written or contributed to dozens of IT books. Prior to becoming a freelance writer, Posey served as chief information officer for a national chain of hospitals and healthcare facilities. He has also worked as a network administrator for some of the nation's largest insurance companies and for the Department of Defense at Fort Knox. Reach him at Brien@brienposey.com.

ABOUT AUTHORITY

Authority provides cloud-based archiving, backup and disaster recovery solutions that help organizations manage risk and meet compliance requirements, including open records laws and eDiscovery requests. Authority supports popular systems and platforms, including Google Drive, Gmail, Exchange, Office 365 and OneDrive, and also helps organizations reduce the burden of switching providers with easy and affordable account and data migration.

CONTACT US

📞 855.298.5200

✉ sales@authority3.com

🌐 www.authority3.com

FOLLOW US

🐦 @AuthorityThree

Auth3rity