Delegate Resolver
Priasoft

Delegate Resolver?

What is the Delegate Resolver? Priasoft provides a utility that can restore folder delegates in a user's mailbox and can restore Send-on-Behalf-Of rights. Outlook + Exchange provide a feature to allow a user to specific one or more other users that have permission to access a folder in their mailbox. Although this may not be a feature that is commonly used, when it is used it is often between VIPs and Executives and their assistants – typically a very important group. The ability to restore delegate assignments quickly becomes a valuable feature.

How it works

The Delegate Resolver (DR) works by analyzing information collected during the migration of a mailbox. The DR is typically run automatically at the end of a migration batch (a list of mailboxes migrated with specific options).

The Priasoft Mailbox Migration Manager (MMM) is responsible for the collection of the delegate information from the source mailbox and for storing the info in the target mailbox for later use by the DR. When the MMM is migrating a mailbox it enumerates all the visible folders for the user's mailbox. During that process, it reads all the delegated permissions on each folder, and stores similar information on the matching target folder for later use. Note that the MMM does not actually restore the permissions on the target folder, it merely places the recorded information from the source in a hidden property on the target folder.

After a migration batch completes, the DR is started. The DR on startup first connects to a Domain Controller in the target environment and performs an LDAP search for mailboxes that have unresolved delegates. The DR is able to determine such by data placed on the target AD user accounts by the MMM. For each mailbox found to have unresolved delegates, the DR logs on to the mailbox and begins to enumerate the target mailbox's folders. For each folder, the previously recorded information about delegates is analyzed and a secondary search is performed. This secondary search is used to find users in the target environment that match each delegate that was collected during the migration. When a match is made, that user is restored as a delegate on the folder.

To visualize this process, refer to the diagram below:

Specifics

As the diagram shows, the DR leverages information in Active Directory to determine which mailboxes to process. What is important to consider is that AD replication can impact the ability of the DR to find matching delegates and ultimately can affect whether or not a delegate can be restored.

Active Directory Replication

For instance, if Joe and his assistant are migrated and the Domain Controller upon which changes were made was in Site1, but the DR is connecting to a DC in Site2, the DR may not be able to find a match for some of Joe's assistant because the relevant changes that the DR is looking for have not replicated to the DC in Site2. You can always run the DR again after a migration has completed for such a case.

Global Catalogs

The DR uses GCs when it is searching for a matching delegate. As such, if the GC that the DR is using does not have matching information (again, possibly due to replication), the delegate will not be restored. However, the unmatched delegate will be looked at again the next time the DR runs.

Self Balancing

This term is to highlight the fact that the DR looks at ALL unresolved delegates for ALL mailboxes that still have them, not just the last batch of mailboxes migrated. This means that if you migrate a user today that has a delegate, and you migrate the delegate tomorrow, the DR will be able to restore the relationship after tomorrow's migration. It is best from a user experience to try to identify groups of users that have delegate relationships and migrate them in the same batch, however sometimes such relationships are not easily discovered. In such cases, know that when the delegate is migrated, its relationship will be restored, even if there are many days between when the delegate and the related mailbox are migrated.

Delegate Info

It is important to understand the information collected about delegates in order to understand how delegates can fail to be restored. The MMM looks at the list of delegates on each source folder and collects specific information. It does that by using information provided solely by MAPI/Exchange. For each delegate, the display name, the rights, and one of 3 unique identifiers is collected.

In Exchange, the Global Address List is a critical resource for nearly every activity. This is also true for delegate permissions on user's folders. The key identifier for objects in the GAL is the X500 address. This address is seen in Active Directory on the property **legacyExchangeDN**. This is one of the 3 values that might be available to identify the delegate, and is the most common. When the MMM migrates a mailbox, the X500 address of the source mailbox is added to the target mailbox as an additional email address. When the DR runs and finds an unresolved delegate, this is one of the values for which it searches. This search leverages a Global Catalog so that a delegate can exist anywhere in the target forest and still be restored. However, if the search does not find the value, the DR cannot restore that delegate. The reasons for the search not finding a match are few and most commonly are because the delegate has not yet been migrated.

There are 2 other types of value that can exist to identify a delegate on a folder: the user account name or the SID. These other 2 value types only exist if the delegate's mail properties have been removed or if the user account has been deleted. A mail user in the Global Address List is associated with an AD user account. There is a property on a mail user that links an AD account to the address book entry. However, if the mailbox of a user were deleted (leaving only the user account), the link is broken. However, when a mailbox is deleted, no operation is performed to clean up any folders that the user had access to on any other user's mailbox. In truth, the user account is still listed with permission to a folder, however because the link is broken there is no X500 address for the delegate. What is left of the delegate is either the user account – in the form of DOMAIN\username – or the SID (see: Security Identifier) of the original object if the user account was deleted. In most cases these are seen as orphaned delegates, but Priasoft does not try to assume such.

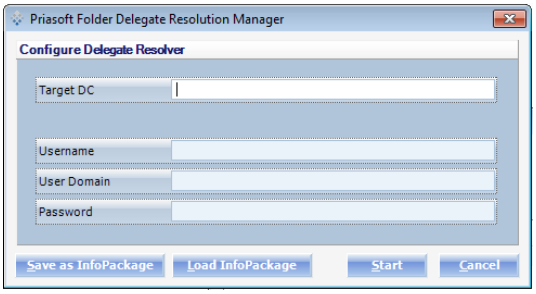
When a mailbox is migrated by MMM, in addition to the X500 address being copied, it copies the user account name and SID of the AD account that is associated with the source mailbox. These values are placed in the target mailbox's email address list so that the DR can find the same. These additional values are seen on a target mailbox as: NTUSER:DOMAIN\username and NTSID:S-1-5-00000... (the series of zeros represent a long string of text that uniquely identifies the user account). Since each migrated mailbox will contain the X500 address, the NTUSER value, and the NTSID value of the original source object, the DR – regardless of the value collected about a delegate – will be able to find a match.

Usage

In most cases, usage of the Delegate Resolver is automatic. Its execution starts automatically after a batch of users completes a migration. However, there are times when it may be necessary or desirable to run the DR manually, such as when there is a delay in AD replication. The following will explain how to do such.

To run the DR manually, execute its shortcut from the Priasoft start menu folder:

```
Start -> Priasoft -> Mailbox Migration Manager -> Tools -> Mailbox Delegates Update Processor
```



Target DC

This should be a Domain Controller in the target environment. In most cases this should be the same target DC that was used by MMM.

Username, User Domain

These should be the username and domain of an account in the target domain, the same domain for which the Target DC supports. The account should have sufficient permission to query AD and to make changes to target AD user accounts. It is typical to use a Domain Admin account for this purpose. Ideally, you should use the same account that was used by the MMM for the same Target DC.

Password

The password for the username

Save as InfoPackage

This button is used to save the above details to a secure file for reuse.

Load InfoPackage

This button is used to load a saved InfoPackage. Note that an InfoPackage is automatically saved with each migration batch. If you need to run the DR at some time after a migration has already completed, you can use this option to load the same parameters that were used for the migration batch. The file will be located in the root of the batch folder. Batch folders are located in c:\ProgramData\Priasoft and are named by date and timestamp. The file will have an extension of *.drpkg.

Troubleshooting

The DR rarely has issues but sometimes a delegate that existed on a source folder will not be restored on a target folder. The DR creates logs in the windows event log system. These logs can be reviewed to analyze the activity performed and to determine why a delegate might not have been restored.

The DR must be able to logon to user mailboxes with system privileges. It is important to understand that the account that is used to launch the DR must have appropriate permissions. The account used in the dialog when the tool is run manually is only used to access Active Directory – that account has no interaction with access to users' mailboxes. Always ensure that the account used to logon to the migration host has sufficient MAPI/Exchange permissions.