Environment Access Necessary for Success
for Hosted and Untrusted Sources

Priasoft Inc. 2014

Access?

Migration of Exchange requires permissions?

This question should actually seem a bit silly. It should be well expected that specific permissions are necessary to be able to migrate data and settings from one environment to another. This document will serve to provide some deeper detail as to the permissions the Priasoft solution requires and the reason and justification for the same.

Very often when the source environment exists in a hosted platform or exists in a less trusted environment (like a recent acquisition or partial acquisition of another entity) a discussion forms with regards to access and permission to the source environment. Priasoft fully understands the need and importance of protecting access to an environment and has worked with many large and high-security environments and therefore understands the complexities and policies often in place to provide such protection.

Source Environment Protocols

When accessing a source environment for migration, there are several communication protocols used by the Priasoft solution:

- LDAP: Used to access Active Directory objects and information
- MAPI: Used to access mailbox and public folder contents
- DNS: Used to perform name to address lookup for source servers

Active Directory

The Priasoft solution needs to read, modify, create, delete, and search Active Directory. Given these activities, an account is needed with enough permissions to do those things. If all of the source user accounts,

distribution lists, contacts, and any other Exchange related object is contained under a specific container in AD, then it will be enough to have permissions at that container and allow it to inherit to all children objects and containers. Additionally, the tools in the solution must also be allowed to search a Global Catalog as well for conflict analysis and safety checks.

Furthermore, the tools need to be able to search, and read data from objects in the Configuration container of AD as this partition contains Exchange server info, AD site information, and so on. This data is used by the Priasoft solution to do readiness checks and to create connection points to Exchange servers, databases, and mailboxes.

The tools will also need the ability to create (or access) a container named "Priasoft" under the Exchange Org object with which the solution can "own" so as to store configuration information specific to the Priasoft applications. This will be the ONLY read/write container needed in the Configuration partition.

In summary, for Active Directory work, the solution needs the following:

- Permissions to either the Domain, or a specific container holding ALL of the source objects for the organization exiting the environment.
    - Search
    - Read all attributes of objects
    - Modify attributes of objects
        - When a production migration occurs successfully, the tools will modify the source user account so that users cannot logon to that source mailbox and so that transports no longer deliver mail to the mailbox.
        - The tools will only modify user accounts that are successfully migrated.
    - Create objects – this is in support of co-existence whereby a forwarder is created in the source pointing to the migrated mailbox in the target.
    - Delete objects – this is only to support the deletion of the forwarder objects mentioned above in the case of a rollback.
- Permissions to search and read info from other objects in the Domain
    - There are object in the Microsoft Exchange System Object container, for example, that we validate as part of the migration
    - There are other containers that we also use for validation and readiness checks
- Permissions to search and read info from objects in the Configuration Partition of AD.
- Permission to create a "Priasoft" container
    - Optionally, this container can be created manually ahead of time as long as the product has full control over that container
- Permissions to search the Global Catalog

Mailbox Content (MAPI)

The solution uses MAPI to access mailbox content. As such, the solution needs to be able to make a successful MAPI connection to source exchange servers, databases, and the mailboxes in those databases.

Our solution uses an administrative account to access mailboxes, not the user itself. As such, this administrative account needs permission to open mailboxes. The permissions that allow for this are Receive-As and Administer Information Store.

There are only 4 object types in Exchange for which these specific permissions can be set:

- Exchange Organization object
- Exchange Admin Group object
- Exchange Server object
- Exchange Database object

Setting permissions on the Exchange Org object is ideal since that permission can be inherited down thru all the other object types and if a new server or database were to be added, the permissions would already be in place.

However, in a more restrictive environment, the lowest boundary would be the Exchange Database. If there is concern about permissions being too broad by being applied at an Org level, it is sufficient to apply them at a Database level.

Specifically, Receive-As allows for the opening of a mailbox where "Administer Information Store" allows for the opening of a mailbox with administrator privileges. "Administer Information Store" does not mean that we will be able to dismount or otherwise perform system changes to a database. It is a leftover term from Exchange 5.5 and Exchange 2000 and by itself does not provide more than what we need.

Opening a mailbox with "admin" privileges is the same method used by the Microsoft tools and gives our solution full access to mailbox content without interference by "user" permissions (like delegate access to folders).

In summary, the solution needs the following ability and permissions for mailbox content:

- Open mailboxes with "admin" privilege.
  - Receive-As
  - Administer Information Store
- Lowest level object at which this can be set is the Exchange Database.

It should also be noted that the account used to access ActiveDirectory should be a separate account from the one used to access mailbox contents. Many times the groups used to provide necessary rights in AD also contain "Deny" rights to mailboxes and databases.

In summary, for the source environment the following should exist:

- A user account specifically used for ActiveDirectory work
- A user account specifically used to access mailbox contents

Throttling Policies

Exchange 2010 and 2013 have throttling policies that can control consumption of resources by users. These policies control things such as:

- How many concurrent PowerShell sessions can be open by a user
- How many concurrent MAPI sessions can be open by a user
- How much CPU time can a user consume in a given period
- And many other metrics

Exchange 2010/2013 have 2 default throttling policies: a modifiable policy and a hard-coded policy that cannot be changed. Furthermore, a user can only be associated with one policy and only accounts in the same forest as the Exchange servers can be associated with a policy. Since performance is often a key attribute of migration, understanding the impact of throttling policies is important. Priasoft recommends that a new throttling policy be created (and has a PowerShell script here that does this) which has no limits and that the aforementioned accounts be associated with this policy.

Failure, or refusal to use such a policy can quickly turn a single-event migration to a multi-month endeavor since the bottleneck created by the policy will create a situation in which only a portion of accounts can be migrated in a given period (typically a 40-48 hour window over a weekend). Furthermore, if the accounts used

for the migration are not associated with ANY policy, there is greater chance of being associated with the hard-coded default policy which is severely restricted.

Firewalls

In many cases a source environment that is untrusted, or has limited access has a firewall in place to limit intrusion and to protect the resources of the source environment from activities on the Internet. However, that same protection often create an access problem for Exchange migration projects.

It is important to understand that given the many protocols involved in a migration and which are established mainly by Microsoft, there is a need to allow access to the source environment. Many of the protocols are easy to work with and only use one or a few well known ports – like LDAP using port 389 or 636. However, and typically of most concern is MAPI.

By default, standard TCP mapi connections use random ports (much like FTP) as well as one or a few static ports. The range for the random ports varies by Exchange version and Service Pack and is beyond the scope of this document to attempt list the all. Regardless of version, it is common that the range of ports used by Exchange is very wide – often many hundred ports.

Microsoft Exchange does have an ability to narrow down that port range, but such is not trivial and requires a reboot of servers. Detail about such can be found here: TECHNET-270836 and TECHNET-331973.

It is often best and more controllable to create bypass filters locked down to either a set of MAC addresses or IP addresses of the migration hosts being used. Attempting to "poke holes" in the firewall for every possible port that could be used can create difficult symptoms, during a migration, that do not immediately surface as firewall issues. It should be understood that Priasoft is merely leveraging Microsoft technologies to perform migrations and port range and protocol use is at the mercy of Microsoft. Priasoft has no direct control over the ports used.

Protecting Source Environment Access

Priasoft recognizes the importance of protecting access to an environment. Creating service accounts often entails elevated permissions and knowledge of those credentials should be limited to very trusted individuals.

The Priasoft solution includes the ability to pre-cache credentials needed so that team-members that need to use the Priasoft tools do not need to know the credentials but merely need to select them from a list. There are 2 separate "vaults" in which credentials can be cached. Priasoft provides an encrypted cache for Active

Directory credentials (using public-private key encryption) and Windows provides a credential cached used for Exchange mailbox access.

In addition, Priasoft, by design, provides NO mechanism to perform any administrative functions against Active Directory or Exchange. There are no "accidental" ways in the Priasoft tools to cause system changes or broad, sweeping changes to a source environment. Priasoft treats all source environments as a "gracious host" and as an environment from which to read data. Although there are required changes made to support a great end-user experience, those changes are ONLY on selected accounts and only for attributes that are Exchange related. The Priasoft solution does not attempt to manage or modify permissions or any security related aspects of a source environment.

The caching of credentials can be performed either by using remote access to the migration host(s), or by a transfer mechanism. In the context of Priasoft's specific cache (for AD access), the tools have a function whereby a temporary and dynamic web session can be created at which a source environment administrator can connect via a web browser. A full explanation of the request and the ability to enter credentials can be submitted via the page and the credential RSA (public-private key) encrypted and send back to the tools.

For Exchange credentials, windows provides a mechanism to export cached credentials from one computer to another with a password. As such, the "MAPI" credentials can be created on a host in the source environment, exported to an encrypted file, and then imported to a migration host.

Through both of the above processes, no user in the target environment will ever know the credentials used to access the source environment, but will be able to use them.

Furthermore, because the cached credentials are static, a source environment administrator can take additional precaution changing the state or password of the accounts being used. A couple of options exist on how to implement this additional protection, as follows:

1. Initially, the source accounts are disabled in Active Directory. They are then only enabled during an approved window of time for use by the target migration team. After the window of time expires, the accounts are then disabled again.
2. Or, initially, the source account passwords are different than the cached versions. Then, only during an approved window of time, the passwords are change to match those that are cached. After the window of time expires, the passwords are changed back to a non-matching value.