Owner of the content within this article is www.msexchange.org
Written by Marc Grote – www.it-training-grote.de

Understanding and using the External Associated Account in Windows Server 2003 and Exchange 2003

Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this article I will give you some information about the External associated Account in Windows Server 2003 and how to use it.

Let's begin

There are some special cases in which you want to separate your Active Directory Forest from your Exchange configuration. Without a separate Forest the separation of administration from Exchange and Windows objects could be very difficult. So it is possible to create a dedicated Exchange Forest, called the Resource Forest. An Exchange Resource Forest is a Forest running Exchange and hosting mailboxes. With a Resource Forest you place only Exchange resources in this Forest and the user accounts, groups and so on resists in the normal Active Directory Forest, called the Account Forest. To establish this scenario you must create a Windows Trust between the Exchange Resource Forest and the Windows Account Forest. In most environments you will also need a provisioning process that synchronizes created Active Directory Accounts in the Account Forest to the Exchange Resource Forest. The provisioning process creates a disabled user with an Exchange Mailbox in the Resource Forest.

One other reason for the implementation of an Exchange Resource Forest is the sharing of FreeBusy informations and the possibility to enable the delegation features in Exchange between to different Active Directory Forests which doesn't trust the other in all ways.

Please note: If you only need to share FreeBusy information, you can use the InterOrg replication tool which is free from Microsoft. For more information about the InterOrg Replication tool, read the following article.

Please note: If any Account in the Account Forest has an SID History, you must turn off SID Filtering in the Trust between the Account Forest and the Resource Forest. The question is: When does a user account have a SID History? The answer is simple. If you migrate from Exchange 5.5 to Exchange 2003 with an external migration method each new Active Directory Account retains its old SID in the SIDHistory attribute. With SID History it is possible that the new created accounts have access to the resources in Exchange 5.5 organization. One other reason for a SID History attribute is the use of ADMT – Active Directory Migration Tool when you move Accounts from one Forest to another Forest.

Advantages / Disadvantages of a Resource Forest

The main reason why to deploy a dedicated Exchange Resource Forest are Security reasons because it is possible to separate Exchange and Active Directory Administration.
The primary disadvantage is the significant Administration overhead and the investment in additional Domain Controllers, Global Catalog Servers and Exchange Servers. You will also need a provisioning process if you don't want to create every account manually in both the Account and Resource Forest.

The External Associated Account

You can associate an Account with the External Associated Account attributes. Although it is displayed in the list of permissions in Active Directory, the Associated External Account attribute is not a true permission. The External Associated Account attribute is only associated with a disabled user account in the Exchange Resource Forest and this disabled User Account is associated with a User Account in the Active Directory Account Forest. **Figure 1** gives you more information about the External associated Account. In **Forest A** there are users – for example **USER01**. In **Forest B** there are associated User Accounts from **Forest A** but this accounts are disabled but have an Exchange Mailbox in the dedicated Exchange Forest. **Forest B** trusts **Forest A** so that User Accounts in **Forest A** can access their Exchange Mailboxes in **Forest B**.

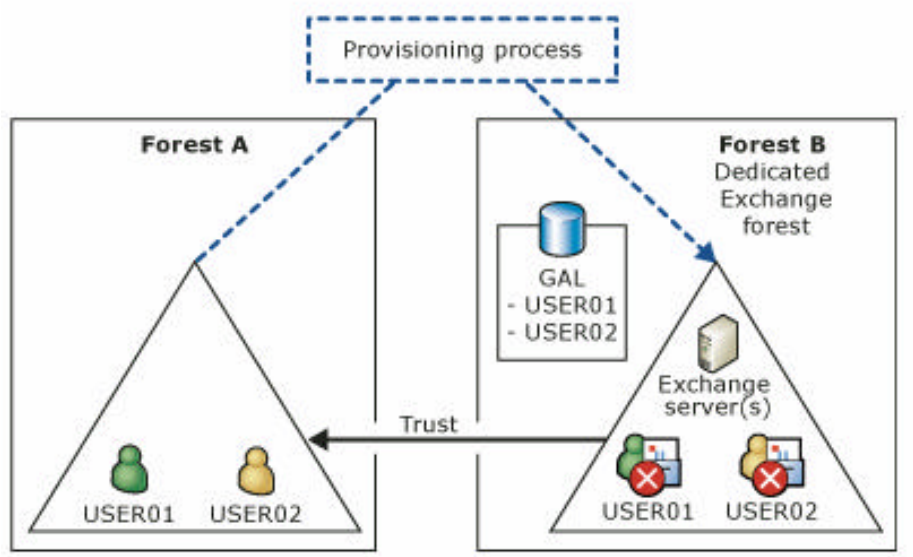

Figure 1: Resource and Account Forest with Trust relationship

Prerequisites

- The external account must be a Windows NT User or a User in an Active Directory that is in a different forest from where the Exchange 200x server resides.
- There must be a trust relationship between the domain where the Active Directory Forest where the real accounts exist and the Exchange Resource Forest where the Exchange user object resides. The Exchange Resource Forest must trust the Active Directory Account Forest.

The Process

- Create a Mail enabled User Account in the Exchange Resource Forest and disable this Account.
- Create a User Account in the trusted Windows 200x Active Directory Account Forest
- Set the msExchMasterAccountSID attribute of the Mailbox enabled User Account in the Exchange Resource Forest to the Security Identifier of the Active Directory User Account of the Active Directory Account Forest. Some Third Party tools allows you to automatically set the msEXchMasterAccountSID. You can also set the msEXchMasterAccountSID with tools like ADSIEDIT.

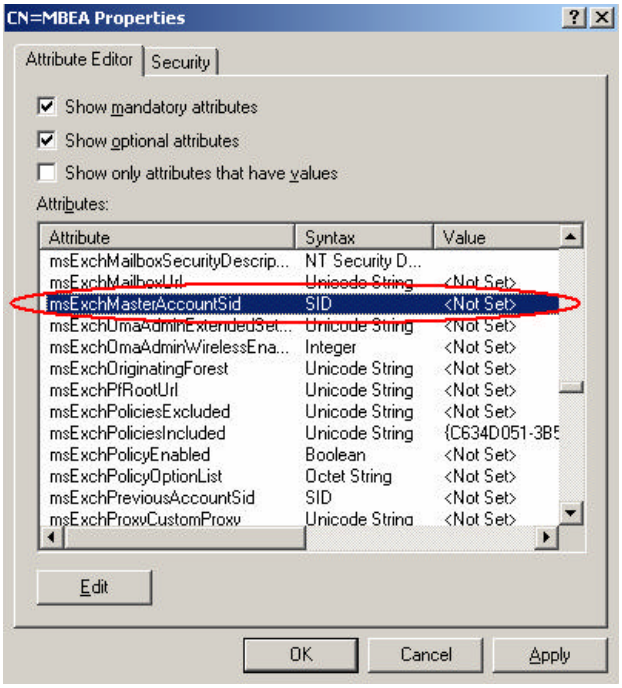

Figure 2: msEXchMasterAccountSID in ADSIEDIT

- On the Mailbox enabled User Account that you created modify the Security Descriptor to add an Access Control Entry (ACE) with the trustee set to the User Account from the Active Directory Account Forest with the rights to Read, Associated External Account and Full Mailbox Access.

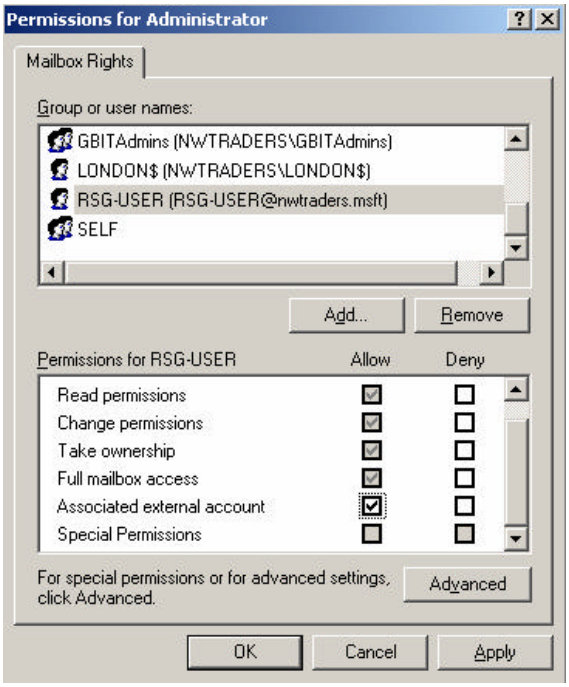

Figure 3: Associate the External Associated Account

Please note: Don't use the External Associated Account attribute for a enabled Active Directory Account with an associated Mailbox because this can cause odd behaviour such as lost permissions and some other problems.

Provisioning

To give you complete information's about the provisioning process is out of the scope of this article but I will give you some basics information's. If you don't want to create every Account in the Active Directory Account Forest and in the Exchange Resource Forest you must use some scripts to automate this process or use Third Party Software which automates this process for you.

Conclusion

In this article I tried to give you an overview about the External Associated Account and why to implement a separate Exchange Resource Forest and an Active Directory Account Forest.

Related Links

Granting Access to External Accounts
http://www.microsoft.com/technet/prodtechnol/exchange/guides/WorkingE2k3Store/8c4befe3-3815-4b6b-a759-1e5a2878499d.mspx
How to associate an external account with an existing Exchange 2000 mailbox
http://support.microsoft.com/kb/322890/en-us
The NoMAS Tool
http://www.msexchange.org/articles/NoMAS-Tool.html