Microsoft Exchange 2003 – Overview of the ADC (Active Directory Connector)

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

Abstract

In this article I will give you an overview of the Microsoft Active Directory Connector (ADC). I will give you some background information about the ADC and his functions.
For a detailed Step by Step Guide how to migrate Exchange 5.5 to Exchange 2000 see Amit Zinman's article
http://www.msexchange.org/tutorials/Exchange_2003_Active_Directory_Connector.html

Let's begin

What ist the ADC

The task of the ADC is to replicate directory information (such as mailboxes, users and groups) between the Exchange 5.5 directory and Active Directory.

The ADC service itself relies on the administrator to define connection agreements. These agreements name the servers involved in the replication cycle, which direction to replicate, which objects to replicate, and when to replicate the data.

The ADC uses LDAP to contact both the Exchange 5.5 and Active Directory. LDAP works efficiently over all types of network links, regardless of whether the connection is fast, slow, or high latency.

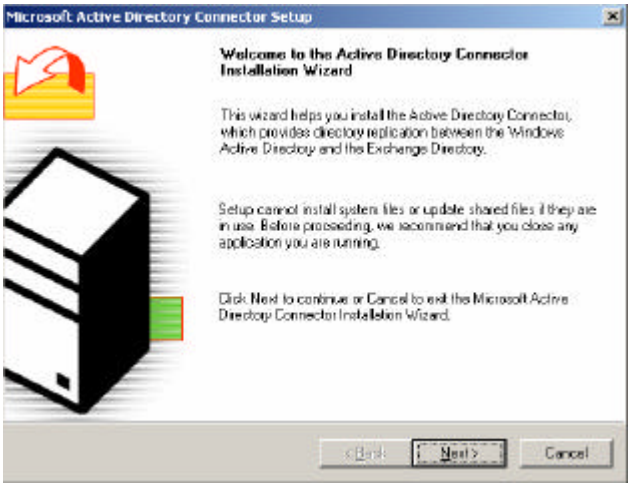

Figure 1: ADC wizard

With the help of the ADC, you can create the following CA (Connection Agreement):

- Recipient Connection Agreement
- Public Folder Connection Agreement

Recipient Connection Agreement

The Recipient Connection Agreement creates a connector to replicate mailbox information, distribution lists and custom recipients from Exchange 5.5 to Active Directory.

Public Folder Connection Agreement

The Public Folder Connection Agreement creates a connector to replicate Public Folder information (not the content of Public Folders) from Exchange 5.5 to Active Directory.

It is important to know that whether the Recipient Connection Agreement and Public Folder Connection Agreement **doesn't** replicates the content of Public Folders and Mailboxes.

Organizations deploy Active Directory Connector (ADC) for four main reasons:

- To replicate Microsoft Exchange directory information (from DIR.EDB) to Microsoft Active Directory (NTDS)
- To replicate existing Microsoft Exchange Server version 5.5 directory data to Active Directory so that third-party applications can take advantage of it.
- To replicate directory information between Active Directory and the Exchange directory for coexistence from one management application.
- To deploy Exchange 2003 Server in an existing Exchange 5.5 environment for consolidation and migration purposes.

Versions of ADC

The basic replication functionality of ADC is included with Windows 2000. However, when you install Exchange 2000, an update is installed.

Windows 2000 ADC

The Windows 2000 ADC, which is included with Windows 2000, replicates directory information in Exchange 5.5 to Active Directory and vice versa. Through synchronization, the administrator can perform basic management functions for Exchange 5.5 users. The Windows 2000 ADC can only replicate the site naming context. It will synchronize additions or modifications on Exchange 5.5 mailboxes, distributions lists, and custom recipients.

Exchange 2000 Server ADC Update

The Exchange 2000 Server ADC update is an enhanced connector included with Exchange 2000. The Windows 2000 ADC replicates objects in the Exchange site-naming context to Active Directory, the Exchange 2000 ADC also replicates data from the configuration naming context,
Exchange 2000 ADC Service Packs

Exchange 2000 Service Pack 1 and Service Pack 2 include an update to Active Directory Connector. Both Updates includes basic functionality as the RTM version but have some additional features.

Exchange Server 2003 ADC

The Exchange 2003 ADC is included on the Exchange 2003 CD. It has many improvments from his predecessor. The most used features are the ADC tools which gives an Administrator a grahically Wizard for every Step in the ADC deployment process. I will explain the ADC tools later in this article.

Exchange Server 2003 SP1 ADC

Microsoft Exchange Server 2003 Service Pack 1 (SP1) introduces changes to ADC Tools. These changes provide better control over the Connection Agreements. These changes include the ability to start initial replication after you have reviewed the Connection Agreements.

In the updated ADC Tools, there are two new files that you can use to control Connection Agreement settings. The files are named …

- Ca_defaults.xml and
- Activate_cas.vbs.

The new ADC Tools functionality is especially useful for large, complicated Exchange environments. With the Ca_defaults.xml file, you can configure the default settings that the Connection Agreement Wizard will use when it creates the Connection Agreements. This gives you the chance to review the new Connection Agreements before they are in use. After you confirm that the settings are correct, you can use the Activate_cas.vbs file to change the Connection Agreement schedule to "Always."

The Ca_defaults.xml file and the Activate_cas.vbs file are located in the folder where you installed the Exchange Server 2003 SP1 ADC.

Initial ADC Installation

When you first install an ADC in a Windows 2003 forest, the ADC Setup program extends the Active Directory schema with the Exchange 2003 schema extensions.

To do this, the account that you are running Setup from must belong to a member of the Schema Administrators group or otherwise have permissions to extend the schema.

Note:

Microsoft has changed the Active Directory Schema expansion in Exchange 2003 / ADC so that both versions use the same Schema. This reduce the replication workload because the schema has to be extends once.

The ADC Setup creates objects in the Active Directory Configuration container. This requires that the the Administrator who installs ADC belong to the Enterprise Administrators group. This permission is a prerequisite of the ADC installation process and Setup cannot succeed without it.

ADC Setup creates two security groups in the local domain called "Exchange Services". This requires that the account you are running Setup from belongs to a member of the Domain Administrators Group or has permissions to create objects in the Users container. If you delete these groups, you have to reinstal ADC.

If you install additional ADC instances, the schema doesn’t need to be extended and so the account must not be a member of the Schema Administrator group.
Subsequent installations do require either Domain Administrator permissions or other specific permissions that allow you to create new objects under the Sites and Services containers in the configuration naming context.
Additional installations in the same domain do not require the creation of either the Exchange Services or the Exchange Administrators groups. The first ADC installation into any other Windows 2003 Server domain requires the creation of these groups and subsequently the proper permissions.

ADC Tools

ADC Tools are available in the Active Directory Connector Services console. ADC Tools help you correct resource mailbox problems, create connection agreements, and verify replication between the Exchange 5.5 directory and Active Directory. ADC Tools consist of the following tools and wizards:

Step 1:

Tool Settings allows you to set the Exchange 5.5 server, LDAP port, and log file path for ADC Tools. The account you use to run this step must have the View Only Admin role assigned at the local Exchange 5.5 site level.

Step 2:

Data Collection scans your Exchange 5.5 directory and Active Directory and gathers data for use in subsequent steps. The account you use to run this step must be a member of the Domain Administrators group in Active Directory. In addition, the account must have the View Only Admin role assigned at the local Exchange 5.5 site level.

Step 3:

Resource Mailbox Wizard allows you to match Active Directory accounts to the appropriate primary mailboxes and stamp other mailboxes with the NTDSNoMatch attribute, which designates the mailboxes as resource mailboxes. The account you use to run this step must have the Admin role assigned at the Exchange 5.5 site level for all Exchange 5.5 sites that contain resource mailboxes.

Step 4:

Connection Agreement Wizard recommends connection agreements based on object matching data collected in step 1. You can review the list of recommended connection agreements and select those you want the wizard to create. The account you use to run this step must be a member of the Domain Administrators group in Active Directory.

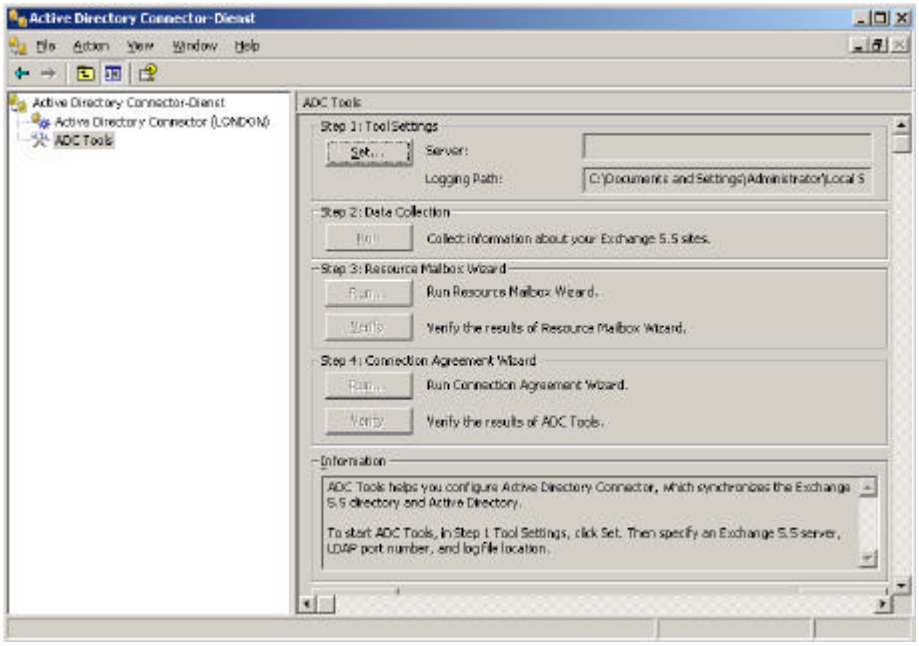

Figure 2: ADC Tools

Important

To check the version of your ADC server, open the Active Directory Connector Microsoft Management Console MMC. Click About Active Directory Connector under the Help menu on each Active Directory Connector Management Console. This will show you the version of the ADC on the machine.

To check the version of all the Active Directory Connectors (ADC) in your organization, use either LDP tool or the ADSI tool to find the "versionNumber" attribute on the ADC servers in Active Directory. The versionNumber attribute should be 16973843 or greater for Exchange 2003 Service Pack 1.

Exchange 2003 Deployment Wizard

Exchange 2003 has a nice Deployment Wizard to deploy Exchange 2003 into an existing Exchange 5.5 organization. The wizards guides you through every step (includes ADC creation) which is neccessary to deploy Exchange 2003.

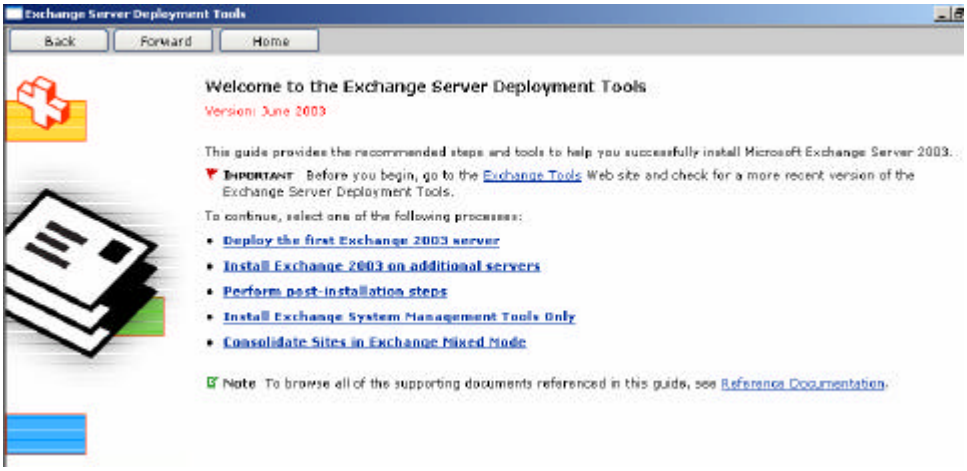

Figure 3: Exchange Deployment Tools wizard

ADC Tools Log File

ADC creates a log file called ADCTOOLS.LOG for advanced troubleshooting purposes. The ADCTOOLS.LOG file is generated when you run ADC Tools in Active Directory Connector. The ADCTOOLS.LOG file is saved in the directory you specify when you run the ADC Tools. Most of the messages that appear in the ADCTOOLS.LOG file also displays in the Information box in ADC Tools.

Connection Agreements

Installing ADC on a server defines a service within Windows 2003. To create a replication agreement between an existing Exchange 5.5 site (named Routing Group in Exchange 2000/2003) and Active Directory, you must configure a connection agreement. The connection agreement holds information, such as the server names to contact for replication (Windows 2003 and Exchnage 5.5), object classes to replicate, target containers in Active Directory, and the replication schedule.

It is possible to define multiple connection agreements on a single ADC server, each of which can go from Active Directory to a single Exchange site or to multiple Exchange sites. For optimal performance, it is recommended that each ADC server manages no more than 50 to 75 connection agreements, depending on the specifications of the computer and the number of objects in each directory.

In large environments it is possible to deploy multiple ADC servers to improve performance and to optimize replication traffic through the placement of ADC servers near the location of Exchange servers and domain controllers.

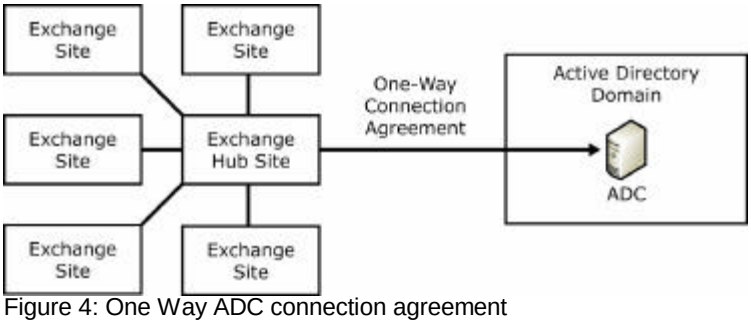

Figure 4: One Way ADC connection agreement

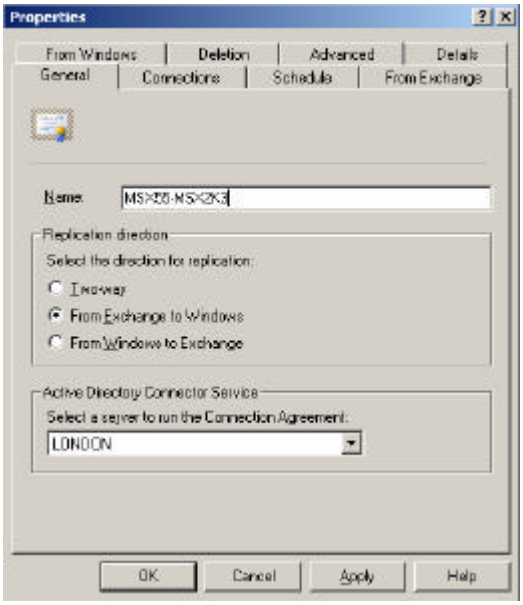

Figure 5: One example of the ADC wizard

Deactivated Users in the Active Directory Users and Computers SnapIn (MSExchangeMasterAccountSID)

ADC creates disabled Active Directory users. If the account is disabled, the Exchange information store will look for an msExchangeMasterAccountSid attribute. If it sees that attribute, it will use that SID (the NT4 account SID) as the account that it will verify, authenticate the user, and grant them access.
Sometimes when users are unable to get into their mailboxes after their mailboxes have been migrated, administrators will notice that there is a disabled mailbox-enabled user in the Active Directory. When they activate this account the msExchangeUserAccountControl value will be set to 0, which means that that user has been enabled, and that it should not look at the msExchangeMasterAccountSid - it looks for an Active Directory SID. Because this users belong to an NT4 domain (the object in AD is only a place holder object), they don't have an Active Directory SID. Therefore, when they try to access their mailbox on Exchange 5.5 the access will be denied.

ADCGlobalName und msExchADCGlobalNames

The ADC uses the *ADCGlobalName* mechanism to keep track of which objects in Microsoft Exchange Server 5.5 are matched to which objects in Active Directory. The ADC marks objects with *ADCGlobalNames* so that when the ADC wants to replicate changes from a source object to its target object, it can faster determine which object should be replicated to the target directory.

The *ADCGlobalNames* attribute has multiple values and contains a unique name for the object in each directory. For Exchange Server 5.5 directory, this name is the DN of the object combined with the object's objectclass attribute. For Active Directory, ADC uses the ObjectGUID attribute. The *ADCGlobalNames* attribute also contains a value that uniquely identifies the Exchange organization or Active Directory Forest that the object come from.

The LDAP attribute that is used in the Exchange Server 5.5 directory and Active Directory is the *msExchADCGlobalName*s attribute. If you use the Exchange 5.5 Administrator program in Raw mode (Admin.exe /r) to view the Exchange Server 5.5 directory, the attribute is displayed as ADC-Global-Names.

Inter-Organization Connection Agreement

You can set the inter-organization connection agreement option on the Advanced tab of a ADC connection agreement properties sheet. This option allows Microsoft Exchange Server version 5.5 and Microsoft Exchange 2003 servers that are in two separate Exchange organizations to replicate directory information. The inter-organization option doesn't handle how objects are created; it only handles how proxies are generated. If the inter-organization option is not selected, ADC does not:

- Match Custom Recipients to a mailbox enabled user.
- Stamp msExchMasterAccountSID or legacyExchangeDN.
- Matches a mailbox to a user that is only mail enabled.

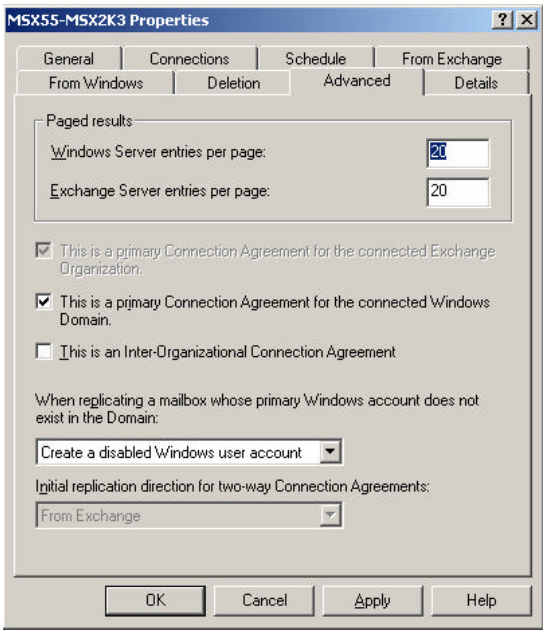

Figure 6: Checkbox to make this ADC connection to an Inter-Organizational Connection Agreement

Server Resources Consumed by ADC

Depending on the replication time set and the number of objects changed, the server on which (ADC) is running and the other directory servers it interacts with may need to process large amounts of data.

For network connectivity it is recommended to deploy ADC in a LAN environment and not over slow WAN links.

When the ADC is working the Threads consume roughly 50 percent of the CPU. This consumption level is constant until all replication is complete. However, the load placed on the CPUs of the computers running the directories is relatively low by comparison.
The memory consumption of ADC is about 6 MB + 2 MB per connection agreement.

Conclusion

The ADC is a powerful tool to implement a directory connector to replicate directory information between Exchange 5.5 and Exchange 2003. The ADC is a must have when you want to migrate from Exchange 5.5 to Exchange 2003.
The ADC is a complex process that requires a deep knowledge of the functions by the Exchange and Windows administrators.

Related Links

Differences Between the Windows 2000 ADC and Exchange 2000 ADC
http://support.microsoft.com/default.aspx?scid=kb;en-us;260902
ADC Installation Requirements
http://support.microsoft.com/default.aspx?scid=kb;en-us;253286
Description of the changes to ADC Tools in Exchange Server 2003 Service Pack 1
http://support.microsoft.com/?id=867627
ADC Service Account Requirements
http://support.microsoft.com/default.aspx?scid=kb;en-us;249817
Exchange 2003 Active Directory Connector Resource Center
http://support.microsoft.com/default.aspx?scid=fh;%5bln%5d;exc2003adc&product=exch2003
Understanding and Deploying Exchange 2000 Active Directory Connector
http://www.microsoft.com/downloads/details.aspx?familyid=c763b584-c511-4687-b27f-a13a8f82d4c8&displaylang=en
Streaming Video - Advanced Active Directory Integration
http://www.microsoft.com/seminar/shared/asp/view.asp?url=/seminar/en/20001121mec1-400/manifest.xml
HOW TO: Troubleshoot Issues with the Active Directory Connector Tools
http://support.microsoft.com/default.aspx?kbid=821828&product=exch2003