Understanding the LegacyExchangeDN

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

Abstract

In this article I will show you the meaning of the LegacyExchangeDN and how to use the free LegacyExchangeDN tool from the Microsoft website.

Let's begin

In Exchange 5.5 every object has a unique Object Distinguished Name (obj-Dist-Name). You can think about the obj-Dist-Name like a SID (Security Identifier) in Windows. To give permissions in Exchange 5.5 the obj-Dist-Name will be used.

Beginning with Exchange 2000, the Exchange configuration is stored in the Active Directory database and there is no obj-Dist-Name. Exchange 200x uses the LegacyExchangeDN for every "Exchange activated" (mail-enabled users, public folders, and Exchange system configuration objects) object. The Exchange Recipient Update Service (RUS) is responsible for filling the LegacyExchangeDN attribute.

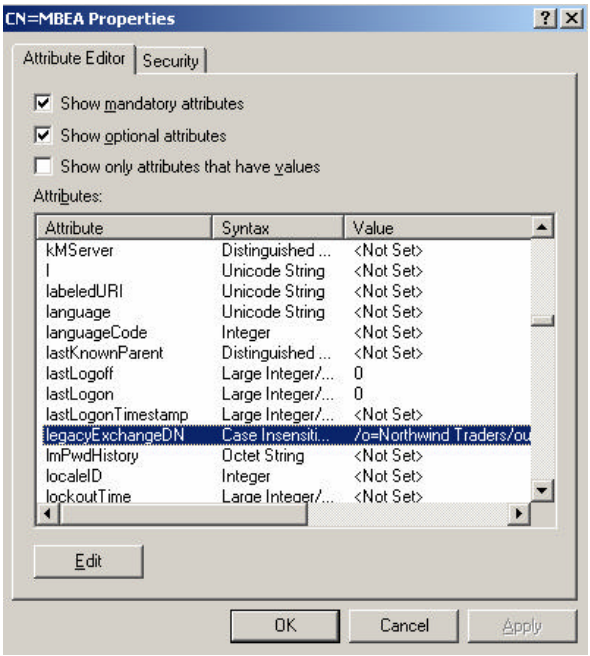

Figure 1: e-mail activated acccount and the LegacyExchangeDN

Normal Active Directory objects which aren't e-mail activated have a LegayExchangeDN but have no value.

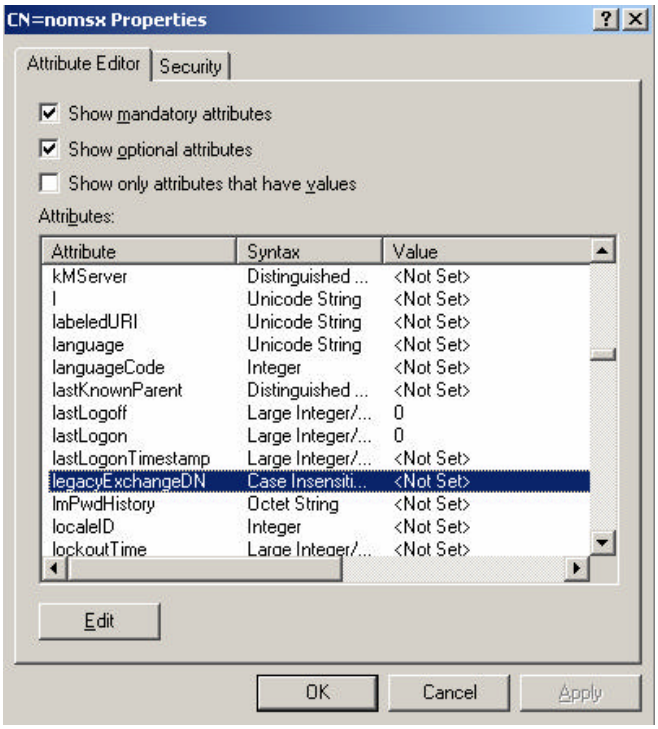

Figure 2: Normal Active Directory user object without LegacyExchangeDN value

Why do we need to change the LegacyExchangeDN?

The LegacyExchangeDN value provides backward compatibility with Exchange 5.5 by mapping an object to a naming system that is understood by Exchange 5.5. The legacyExchangeDN attribute for each object translates the object's Active Directory naming into a format suitable for representation and identification in Exchange 5.5.

In Exchange 5.5 and Exchange 200x you can restore a backup of an Exchange database from one Exchange server to another Exchange server when the Exchange organization name, name of the Storage Group, and the Server name match the names of the original server.

Please note:

Beginning with Exchange 2003 you can use the Recovery Storage Group to restore private information store databases to the same Exchange Server without building a separate recovery Server like in Exchange Server 5.5 and 2000.To recover mailboxes you don't need to use the ExchangeLegacyDN. If you want to recover public folder data it is still necessary to build a reovery server and you might need to use the LegacyExchangeDN tool.

Why is the ExchangeLegacyDN important in recovery scenarios?

To recover databases in Exchange 5.5, the recovery server must match only the organization and site name. In Exchange 200x there must be a match for the Exchange organization name, the name of the administrative group and the legacyExchangeDN values for several Exchange system objects in the Active Directory database.

When an Exchange 200x database is created, the legacyExchangeDN value of the administrative group is stamped into the new database. It is only possible to start an Exchange database when the ExchangeLegacyDN matches the ExchangeLegacyDN from the Exchange administrative group from where the Database was created.

When you install Exchange server on a test server, the legacyExchangeDN values are set to a default of /ou=First Administrative Group (every Exchange installation has a default administrative group called "First Administrative Group"). You will run into problems when this setting doesn't match. You have three Possibilities:

- Generate the correct LegacyExchangeDN by entering the correct name of the Administrative Group during Exchange installation on the Recovery Server. To do so you must run setup three times. First run Exchange setup with the /Forestprep option that matches the Exchange LegacyDN for the Exchange organization. Next you must run the Setup again and install only the Exchange administrative tools. Start the Exchange System Manager and create a second administrative group that matches the LegacyExchangeDN of the database to recover. As a last step you can install the Exchange recovery server in the second created administrative group.
- Manually correct all LegacyExchangeDN values in the default administrative group by using tools like ADSIEdit or LDIFDE
- Use the LegacyExchangeDN tool to determine the required values and to change values through a graphical interface.

LegacyExchangeDN and ADCDisabledMailByADC

Did you ever see some objects which LegacyExchangeDN field contains a value called "ADCDisabledMailByADC" or "ADCDisabledMail"? If an object contains one of these values the Recipient Update Service doesn't handle this object.
The setting of this value depends on ADC (Active Directory Connector) settings:

ADC setting	Disabled account	Enabled account
Delete active	Object will be deleted in Active Directory	The Object is "Exchange disabled". ADC writes the value "ADCDisabledMailByADC" to LegacyExchangeDN
Delete not active	Object will not be deleted The Object is "Exchange disabled". ADC writes the value "ADCDisabledMailByADC" to LegacyExchangeDN	The Object is "Exchange disabled". ADC writes the value "ADCDisabledMailByADC" to LegacyExchangeDN

LegacyExchangeDN Tool

The LegacyExchangeDN tool enables you to:

- Change Exchange 2000 and 2003 organization names.
- Change Exchange 2000 and 2003 administrative group names.
- Change legacyExchangeDN values on critical system objects.

You can download the LegacyExchangeDN tool for free here.

One of common use of the ExchangeLegacyDN tool is to use it to help you rename attributes as part of the process of recovering an Exchange database to a test server when Exchange data is not recoverable using other Standard methods.

After downloading and "installing" the LegacyExchangeDN tool, you can execute the tool, enter credentials to logon and test the changes. The LegacyExchangeDN tool runs per default in read only mode.
You can change the Exchange organization name, the name of the administrative group and the LegacyExchangeDN for a value.

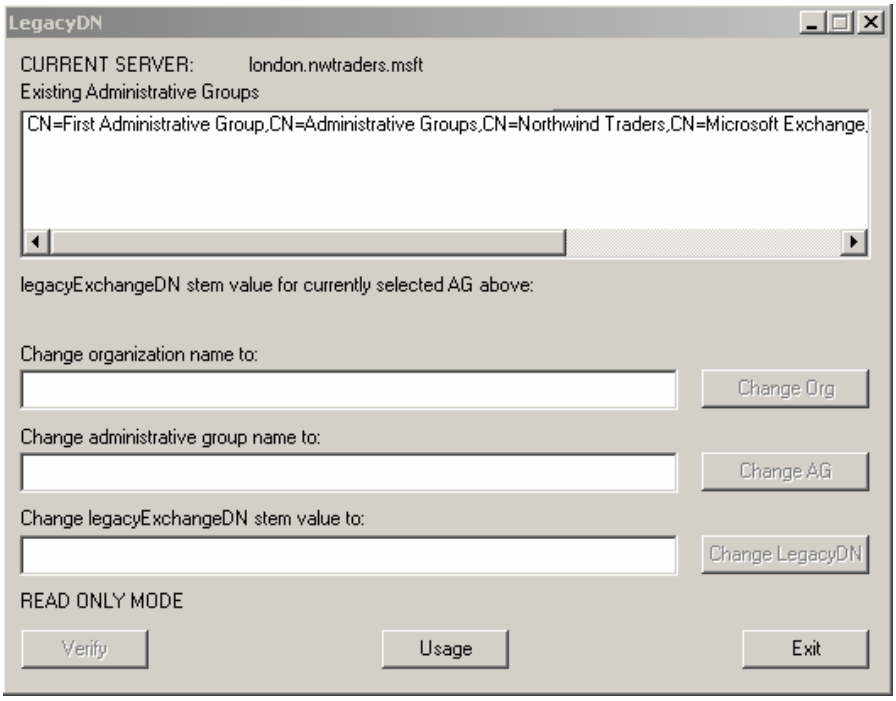

Figure 3: LegacyExchangeDN tool

Click *help* to see the available command line switches to use with the ExchangeLegacyDN.

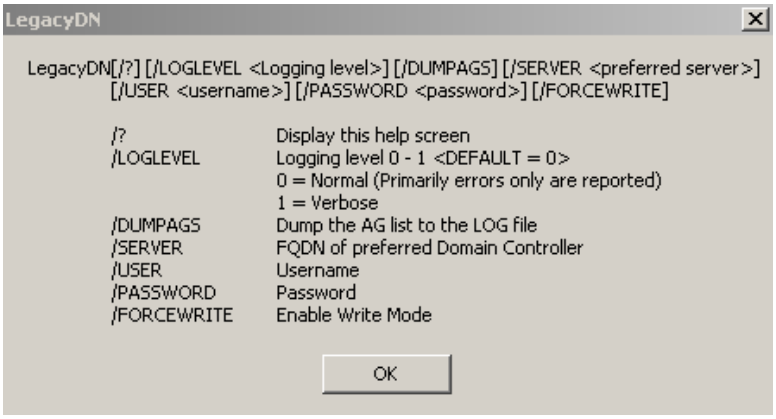

Figure 4: LegacyExchangeDN command line options

LegacyExchangeDN tool command line syntax

LegacyDN [/DUMPAGS] [/LOGLEVEL <logging level>] [/SERVER <preferred server name>] [/USER <username>] [/PASSWORD <password>] [/FORCEWRITE
/DUMPAGS. This option dumps the administrative group list to the log file.
/LOGLEVEL. The default logging level is 0 (Normal), and you can also set the logging level to 1 (Verbose).
/SERVER. Fully Qualified Domain Name (FQDN) of preferred Windows domain controller
/USER. User name
/PASSWORD. Password
/FORCEWRITE. Must be used to run in edit mode

Conclusion

I hope you understand the meaning of the ExchangeLegacyDN and how to use the ExchangeLegacyDN tool. Pay attention when you use this tool. Under normal circumstance you don't have to use this tool.

Related Links

Microsoft Exchange Server LegacyDN Utility
http://www.microsoft.com/downloads/details.aspx?FamilyId=5EF7786B-A699-4AAD-B104-BF9DE3F473E5&displaylang=en
How to use Legacydn.exe to correct Exchange organization names or Administrative Group names in Exchange Server 2003 or in Exchange 2000 Server
http://support.microsoft.com/default.aspx?scid=kb;en-us;324606
How to Change the LegacyExchangeDN Attribute in Native Mode with ADSI Edit
http://support.microsoft.com/kb/273863/en-us
LegacyDN Property
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/e2k3/e2k3/_wmiref_pr_Exchange_MailboxLegacyDN.asp