

Re: LegacyExchangeDN is wrong for a user

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange2000.active.directory.integration/2004-05/0>

From: Dave Howe [MSFT] (daveh_at_online.microsoft.com)

Date: 05/20/04

Date: Thu, 20 May 2004 10:48:16 -0400

On Mon, 17 May 2004 21:30:18 -0700, "mmac" <no@thank.you> wrote:

>You are right on target, the EX5 Value is Ztest (geez you folks are smart!)
>what now?
>
>As a side question, can you give me an example of why someone would want to
>deal with this nightmare by having more than one mailbox?
>I have several that I use but they are all different accounts that I just
>have rights to. and I have several addresses in my properties tab. All that
>suits me fine, why could I possibly want more than one?
>

Sorry about the delay in getting back to you. I'm glad you were able to better isolate how this happened within your environment.

The cleanup for a crosslinked account is relatively easy for a single user, but in some instances where you have dozens or hundreds of these, it can be one of your worst nightmares. And, if the cleanup is not done correctly, you may end up with mail loss.

IMPORTANT – An Exchange 5.5 object that has been replicated to Active Directory via a two-way Recipient CA will have a total of 4 msExchADCGlobalNames/ADC-Global-Names values stamped on it. These values establish a link between the AD user account and the Exchange 5.5 mailbox, and any changes on either side will replicate to the other.

This is how PSS would advise you to clean up a cross-linked account should you call in on a support incident for this issue:

1) Perform an Exchange 5.5 backup or use ExMerge to access the two crosslinked mailboxes and export the contents to PST files. Consider this "ulcer insurance" ... ;)

2) The next thing you need to do is set the replication Schedule for the Recipient CA that replicated this information into Active Directory to NEVER. If you can't figure out which one you need to

temporarily disable, simply stop all instances of the Microsoft Active Directory Connector service.

3) Next, find the two accounts that are cross-linked in Active Directory Users and Computers from the Exchange server or from any server that has the Exchange System Manager installed. Once you locate them, right click on them, choose Exchange tasks, and choose Remove Exchange Attributes.

WARNING – If you have not disabled the Recipient CA responsible for replicating these objects, the Exchange 5.5 mailbox will effectively be deleted after the next ADC replication cycle. Why? Because when you Remove Exchange Attributes, you are basically breaking the "link" between the AD object and the Exchange 5.5 mailbox. We do NOT want this to replicate back to the Exchange 5.5 side right away and delete the mailbox.

4) Open the Exchange 5.5 admin program in raw mode and connect to the Exchange 5.5 server specified under the Connections tab of the responsible Recipient CA. You can do this by typing admin.exe /r from the Exchsrvr\BIN folder. Once the Admin program is loaded, locate the two mailboxes that have been crosslinked, select one of the accounts and click File > Raw Properties. This will load up an interface that shows the individual attributes of the mailbox object. Scroll up and you should see ADC-Global-Names, which should be populated with 4 values. Remove these values for each affected account.

This effectively breaks the link between the AD account and the Exchange 5.5 mailboxes.

5) Now, on the Resource Mailbox (I'm assuming is Ztest), open the properties (not Raw Properties), click on the Custom Attributes tab, and populate Custom Attribute 10 with the value NTDSNoMatch. What this will do is prevent Ztest from ever linking to the wrong account once we enable ADC replication again. Click Apply/OK.

6) If you notice a duplicate account was created in AD, you may want to go ahead and remove the duplicate. You can check that by using the LDP dump taken earlier and look at the When Created date which should read YearMonthDay format... 040520. The one created recently will most likely be the duplicate AD account. You can also look at the logons value to see if the AD account has ever been logged into before.

7) Verify that you have completed Steps 1 – 7 successfully, then start up the ADC service again or set the Recipient CA replication Schedule back to Always.

- Ztest should create a new disabled account and link to it.
- Your user should link to correct AD account based on (objectSID==Primary Windows NT Account).

microsoft.public.exchange2000.active.directory.integration: Re: LegacyExchangeDN is wrong for a user

... if all goes well. :)

Let me see... articles... here's a few:

256862 XADM: How to Correct Mismatched Accounts After Active Directory

<http://support.microsoft.com/?id=256862>

316886 HOW TO: Migrate from Exchange Server 5.5 to Exchange 2000 Server

<http://support.microsoft.com/?id=316886>

274173 XADM: Documentation for the NTDSNoMatch Utility

<http://support.microsoft.com/?id=274173>

Please let me know how this turns out. If you need additional assistance with this, just ping me by email (daveh@microsoft.com).

Have a good day!

Dave Howe

Microsoft PSS

This posting is provided "AS IS" with no warranties, and confers no rights.