SysOp Tools Learning Guide:
Find and List Duplicate UPN (userPrincipalName) Entries in Active Directory

Updated December 12, 2009

Symptom:

Users are unable to log in to Password Reset PRO, OWA (Outlook Web Access), MOSS (SharePoint), domain computers, or any other system by using their UPN (universalPrincipalName, e.g. **user@domain.com**). An error event is logged on domain controllers referring to the following AD attribute "DS_USER_PRINCIPAL_NAME":

Cause:

You may have one or more duplicate user account UPNs in AD, which must be cleaned up. Here is a KB link from Microsoft which covers the issue: **http://support.microsoft.com/kb/251359/EN-US/** . If you have duplicate UPNs (or missing UPNs), a lot of things may not work right in your domain in regards to user logons- e.g OWA logons, SharePoint logons, any system that uses the newer UPN authentication method (like our self service software), domain trusts, etc.

About the UPN attribute: **http://msdn.microsoft.com/en-us/library/cc220979(PROT.13).aspx**

Resolution:

Ensure that UPNs are configured and unique on all employee user accounts in the domain. System Accounts and the Builtin accounts may not need a UPN since they are typically not used by a human user for logon purposes (e.g Administrator, Guest, etc). An easy way to clean up your AD of duplicate UPNs is to use scripting, an LDAP search in Active Directory Users and Computers, or the Microsoft LDP.exe utility that ships with the Windows Server 2003 Support Tools. Information on the ldp.exe utility can be found here: **http://technet.microsoft.com/en-us/library/cc772839(WS.10).aspx**

Next pages:

Using LDP.exe to search and find all UPNs (Pages 2-4)

Using Active Directory Users and Computers to find all UPNs (Pages 5-7)

Using LDP.exe to list all UPN (userPrincipalName) account information in the domain

Run ldp.exe from any domain member server, it is fastest if you run it on the primary DC directly. Launch ldp.exe and configure to connect to your primary DC (Connection > Connect)

Then you must bind to LDAP with proper permissions (Connection > Bind):

It may take a few minutes at this point to load LDAP data from the DC, just wait until it is done.

Now set your search parameter (Browse > Search): Set your configuration the same as the highlighted areas below to run this search on entire domain.

Click “Options” in the screen above, the screen below opens. Here we will add the “userPrincipalName” property to the beginning of the search string:

First, copy the existing search parameters and paste into notepad for safekeeping. Then delete the search parameters and type in “userPrincipalName;” **Make sure to add a semicolon after userPrincipalName**

Viewing Results:

Now click “OK” to close the options screen, then click “Run” on the search screen to execute the search, then click “Close”. Your results will look like below, you can copy the screen text for distribution / sorting. This search only lists UPNs in the domain making it easy to spot duplicate or missing UPNs on your employee user accounts.

Next page:

Using Active Directory Users and Computers to find UPNs

Using ADUC to find all UPNs in domain

We'll need to set up two things here, first define a custom LDAP search and then set up a custom view in ADUC

Open ADUC, right click on the Saved Searches folder.

Select "new" > "query"

Continued on next page…

Now configure the name of your search and the query root, then click “define query”

Select “Custom Search” from the drop list and select the Advanced tab:

In the “Enter LDAP Query” field, paste this query string exactly as shown:
(objectCategory=person)(objectClass=user)(userPrincipalName=*)

Click OK, then OK to save. You should see a new saved query on left, and all of the query results on right.

Define your custom view in ADUC:

In ADUC, add the column called “User Logon Name” to the list of Displayed Columns in order to see the found UPN data from your custom search. In ADUC, Click the “User Logon Name” column to sort data and look for duplicates. Remove any duplicates by editing the Account tab of the duplicate account and setting the UPN to something unique.

Provided by:
SysOp Tools, Inc
www.sysoptools.com