Integration of SAP central user administration with Microsoft Active Directory

Chris Kohlsdorf, Senior System Architect SAP NetWeaver, REALTECH AG Walldorf
André Fischer, Project Manager Collaboration Technology Support Center, SAP AG

Summary

As system landscapes become more and more complex efficient identity management becomes a key success factor in IT organizations.

Often the same identity information has to be maintained in lots of different IT systems. This leads to a great administrative overhead for creating, updating and deleting user data in all involved systems.

Focussing on an entire SAP system landscape the integration of SAP CUA (central user administration) with Microsoft Active Directory Services can be the first step in implementing identity management in your IT infrastructure. The benefit is a huge reduction of administrative efforts and more consistent data across the different participating systems.

Applies to

- SAP Web Application Server
- Microsoft Active Directory 2000
- Microsoft Active Directory 2003

Keywords

Directory synchronization, identity management, central user administration

Level of difficulty

Technical consultants, Developers

Contact

For feedback or questions you can contact the Collaboration Technology Support Center at ctsc@sap.com. Please check the .NET interoperability area in the SAP Developer Network http://www.sdn.sap.com/sdn/developerareas/dotnet.sdn for any updates or further information. You can contact REALTECH at customer-services@realtech.de.

Contents

Introduction

As already mentioned in the short summary above the scenario used for this collaboration brief deals with two key components: Microsoft Active Directory and SAP Central User Administration.

Active Directory, being the integrated, distributed directory service included with Microsoft Windows Server 2003 and Microsoft Windows 2000 Server, provides a central user repository used to centrally maintain user data, thus avoiding the redundant, error-prone maintenance of user information in several systems. Most organizations already use Active Directory to organize and manage information about all kinds of their different resources like users, computers, applications and so on.

While the user management engine (UME) used by SAP Enterprise Portal can use a central Active Directory as its user persistence store ABAP systems use their own database as user store. SAP's central user administration (CUA) can be used to maintain SAP user master records in one central system and distribute this information in a consistent way to connected child systems. This provides a single point of administration of all SAP user data in the entire SAP system landscape in one central system.

This document describes the benefits of a synchronization of user data between an LDAP directory (e.g. Microsoft's Active Directory) and SAP systems. In the outlined scenario MS Active Directory will become the leading system for storing common user data. As a result users newly created in the directory will be synchronized and created in the SAP CUA. For user data that has been updated in the directory this new information is also synchronized into the SAP system and updated there as well.

The SAP CUA will be used to distribute all the user data that has been "imported" from the directory to all its connected child systems.

Scenario

The following screenshot provides an overview of the outlined scenario discussed in this guide:

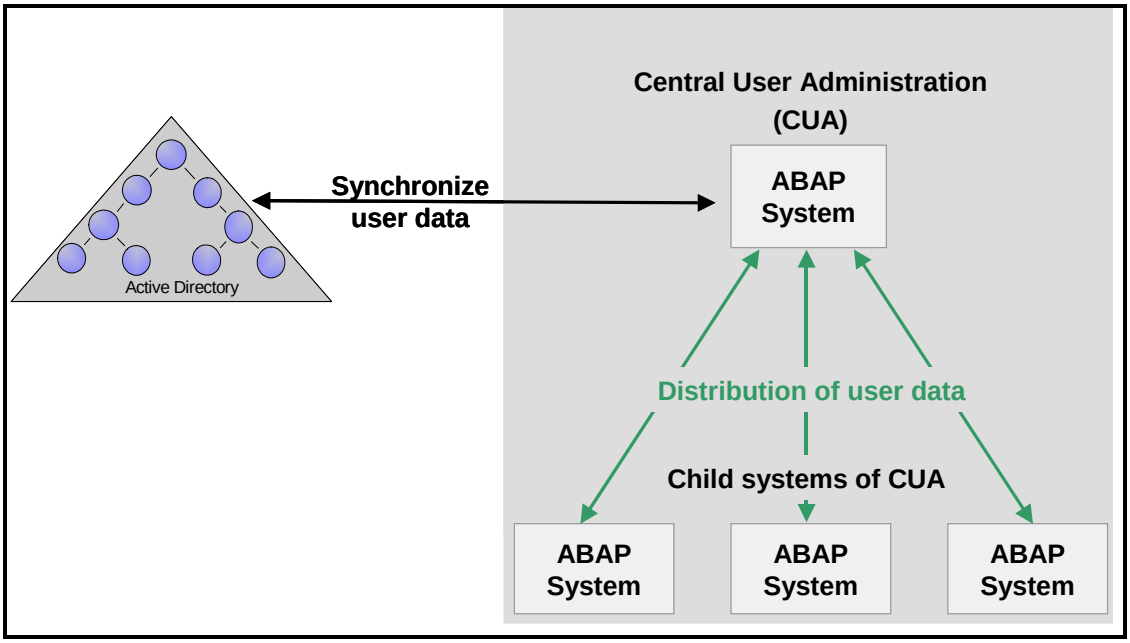


Figure 1 - Scenario overview

Technical Basis

The SAP LDAP Connector

The following part gives a short introduction to the technological mechanism providing the synchronization functionality between the directory service and the SAP system – the so-called SAP LDAP Connector.

The protocol used for communicating with a directory is usually the Lightweight Directory Access Protocol (LDAP). The SAP LDAP connector allows direct access to directories within ABAP applications using the LDAP protocol. It provides this functionality in form of an API for connecting and searching, reading and editing of directory entries. This API has already been shipped with the basis release 4.6. But this release does not provide any functionality to synchronize user master data between SAP and the Active Directory. This functionality was first introduced with basis release 6.x that is used for SAP's Web Application Server architecture and is therefore also available for all components based on SAP's NetWeaver platform.

The following figure shows the architecture of the LDAP connector:

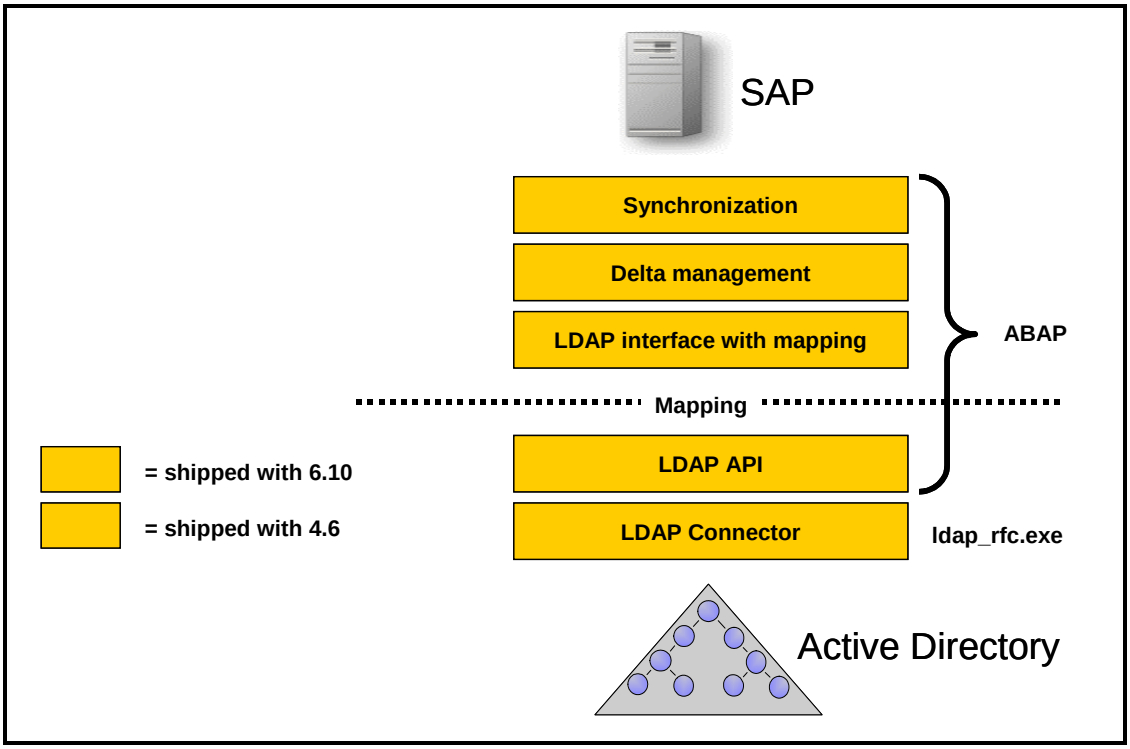


Figure 2 - Architecture of SAP LDAP Connector

LDAP_RFC

From technical point of view the LDAP connector is represented by the program *"ldap_rfc"* that is running as a *registered server program*. The communication between the Active Directory and the executable *ldap_rfc* is performed using the standardized access protocol LDAP. The LDAP protocol is normally using the TCP/IP port 389.

There are two possible options how to set up the LDAP Connector:

a) The LDAP connector can run as part of the SAP Application Server. In this case the executable in the directory usr\sap\<SID>\SYS\exe\run (Windows) or /usr/sap/<SID>/sys/exe/run (UNIX) is used.

b) The LDAP connector can run as a standalone program on a dedicated server with access to the Active Directory.

Option a) is shown in the following figure "LDAP Connector as part of the SAP application server":

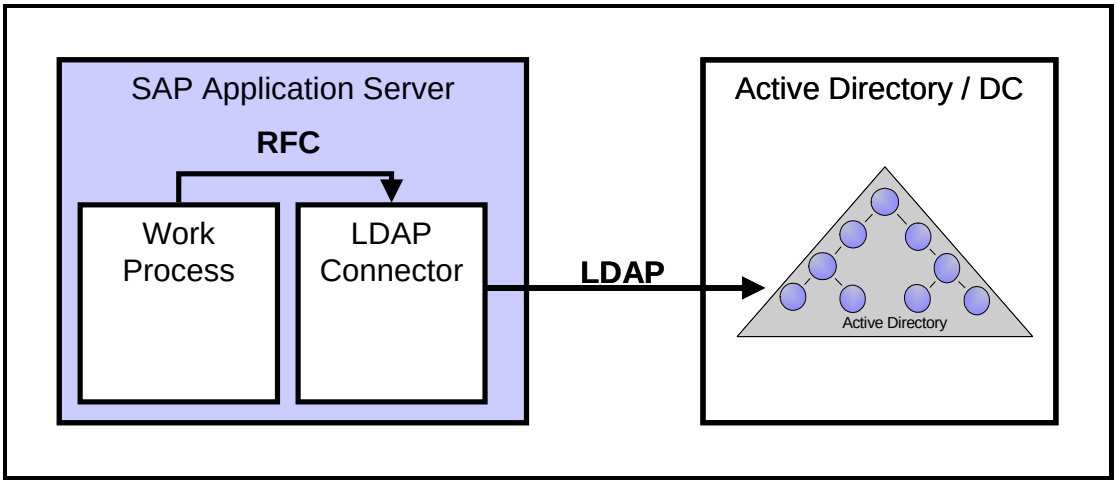


Figure 3 - Option a) LDAP Connector as part of the SAP application server

If the LDAP connector is running as part of the SAP application server it can be monitored and managed using the CCMS. The CCMS alert monitor can monitor the load (percentage of used LDAP- connections) and the status (UP or DOWN) of the LDAP Connector. CCMS will also start the LDAP connector if it is down.

Since the LDAP connector loads the LDAP library of the operating system at runtime it is a prerequisite that the operating system is offering such an LDAP library. This prerequisite is fulfilled by Windows 2000/2003 since Windows 2000/2003 is shipped with the required DLL.

Option b) can be used as a workaround if no LDAP library for the desired operating system is available. In such a case there is the option to run the LDAP Connector as a "standalone program" on a dedicated server as shown in the following figure:

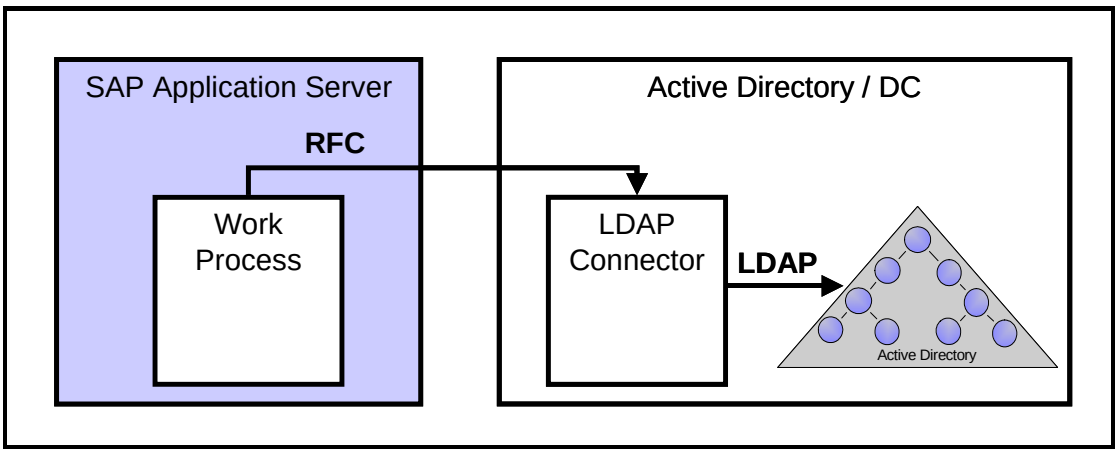


Figure 4 - Option b) LDAP Connector as standalone program on dedicated server

The drawback of using option b) is that the LDAP connector is not part of the SAP Application Server and can therefore not be monitored and managed using the CCMS. However, since the LDAP connector can be implemented as a service on the Windows operation system it can be monitored by common monitoring tools.

SAP CUA

As mentioned above, SAP systems, which should be connected to the Active Directory directly, must be based on basis release 6.x of SAP Web Application Server. If the systems are based on release 4.6 or lower it is possible to implement the SAP Central User Administration (CUA) on a SAP Web Application Server, which then acts as a kind of LDAP gateway.

Since also SAP Systems that are based on the Web Application Server can be added as child systems to the SAP CUA the directory enabled SAP CUA can be used to distribute data across the whole SAP system landscape while still offering the possibility to maintain SAP specific data in the central system rather than in the Active Directory.

Implementation

Transaction LDAP

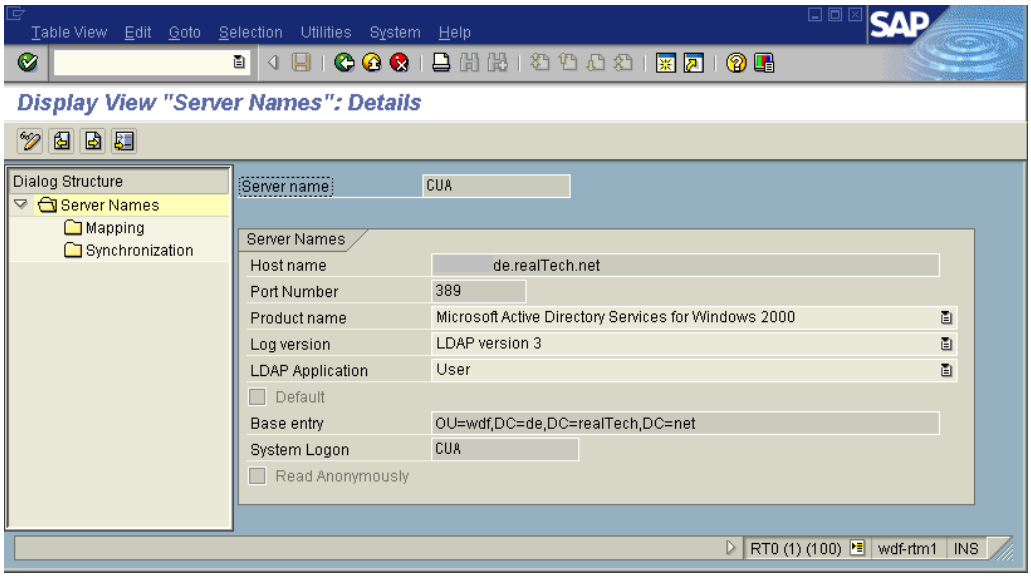
Central point of administration for all settings regarding SAP's LDAP Connector is transaction LDAP. Here you can configure the required RFC destinations, set up a new LDAP connector, create a new logical LDAP server, maintain communication users as well as maintain the mapping and synchronization details.

Figure 5 - Transaction LDAP

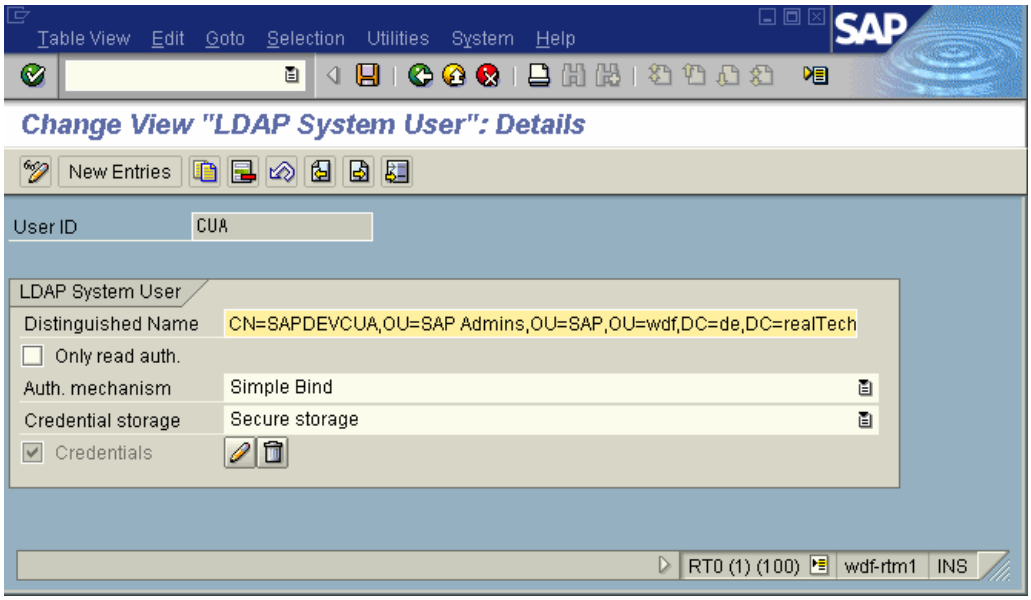
The required steps are in detail:

- Create an RFC Destination to the program "LDAP_RFC"

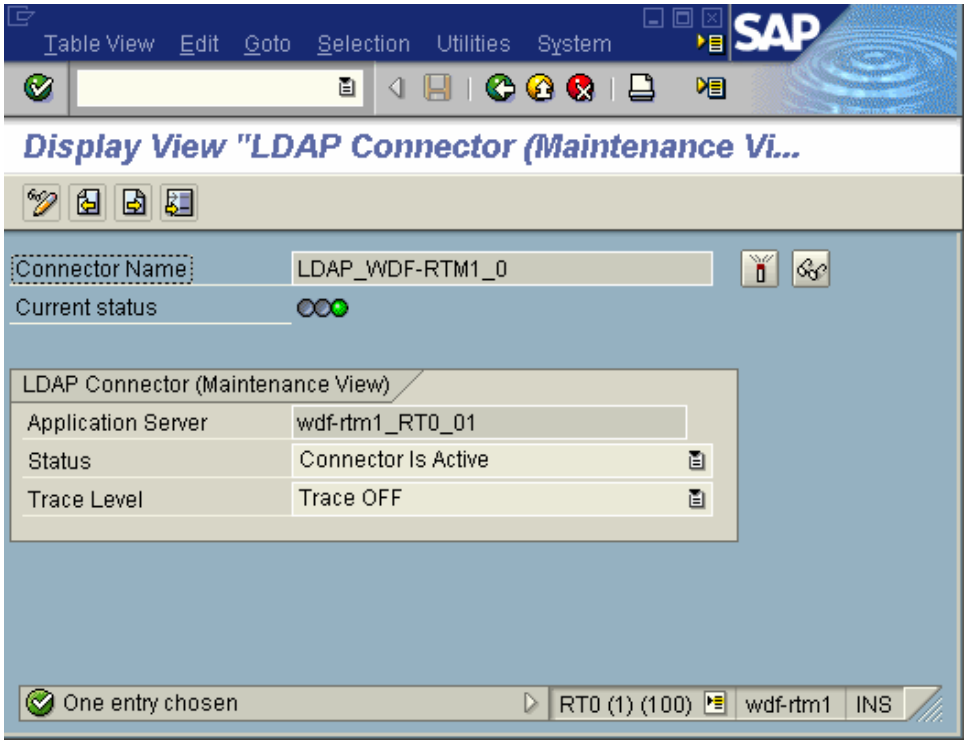
- Create a new LDAP Connector that utilizes the RFC destination maintained before
- Create a new logical LDAP Server. Here you have to maintain the connection details to the physical directory



- Maintain the communication user that is used by the LDAP connector to bind the LDAP Directory Server. The binding information (username and password of a Active Directory user) is stored in the secure storage.



- Now you can already test the connection to the directory:



Mapping

In transaction LDAPMAP specific SAP data fields can be mapped to the desired directory attributes.

SAP offers directory specific proposals for the mapping of the directory attributes to the SAP data fields. After importing the proposal the mapping details can be customized as desired.

Active Directory users, which should be selected for the synchronization with the SAP system, are identified by one specific so-called filter attribute. If this attribute is set for an Active Directory user object the synchronization report RSLDAPSYNC_USER will either create a SAP user with that SAP username in SAP system (here SAP CUA) if it does not already exists or it will update the SAP user if the user has been changed in the Active Directory for example because the phone number of that user has changed.

The following screenshot shows a default mapping:

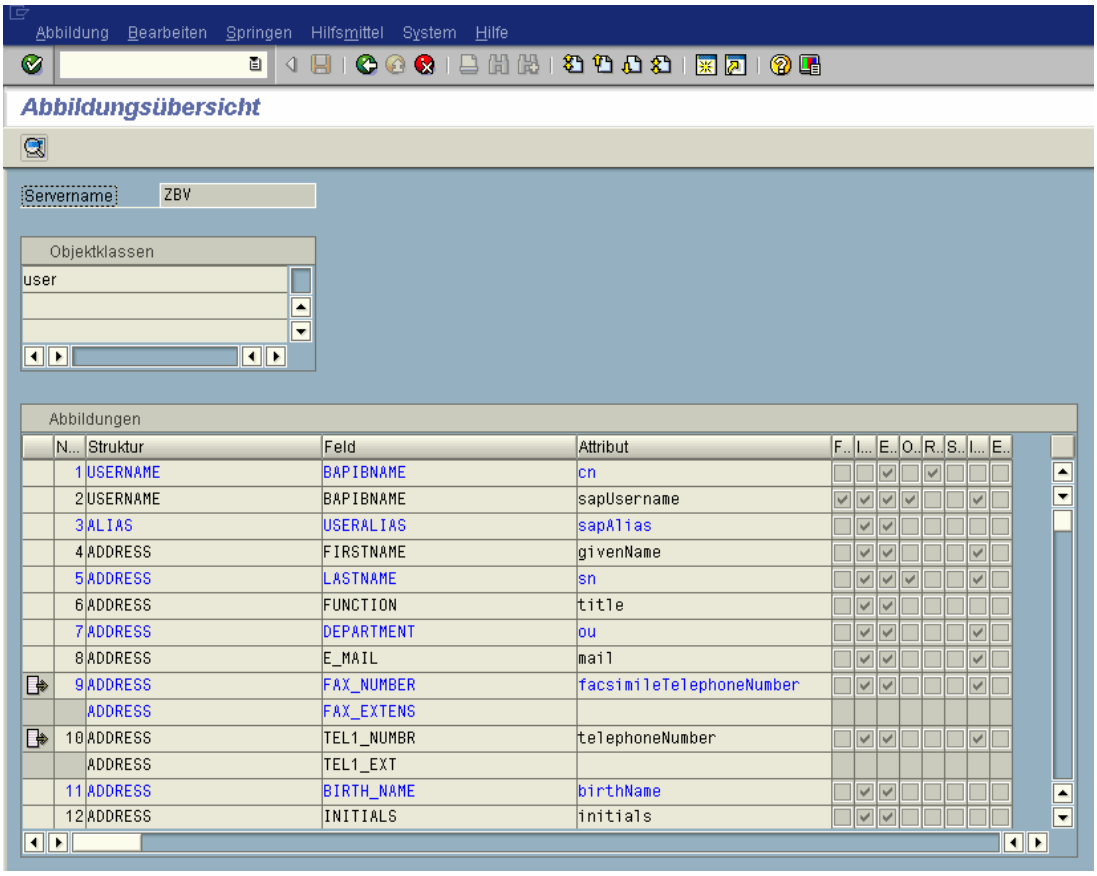


Figure 6 - Mapping of SAP data fields to directory attributes

For each attribute there is the option to specify whether the customized mapping is only valid for import, export or for both ways of synchronization.

Mapping using function modules

If the desired mapping is not a simple 1:1 relationship, function modules can be used to enable a more complicated mapping procedure. A simple example is the telephone number. The telephone number of a user is stored in the directory attribute “telephone” (in MS Active Directory). The extension is normally split by a hyphen ‘-‘. In SAP the telephone number of a user is stored in two data fields ADDRESS-TEL1_NUMBR and ADDRESS-TEL1_EXT. Therefore the function module MAP_SPLIT_CHAR can be used. This module reads the value for the telephone number from the directory attribute telephone. The extension is split at the position where the system finds a hyphen ‘-‘ in the string and the two values are stored in the SAP data fields ADDRESS-TEL1_NUMBR and ADDRESS-TEL1_EXT.

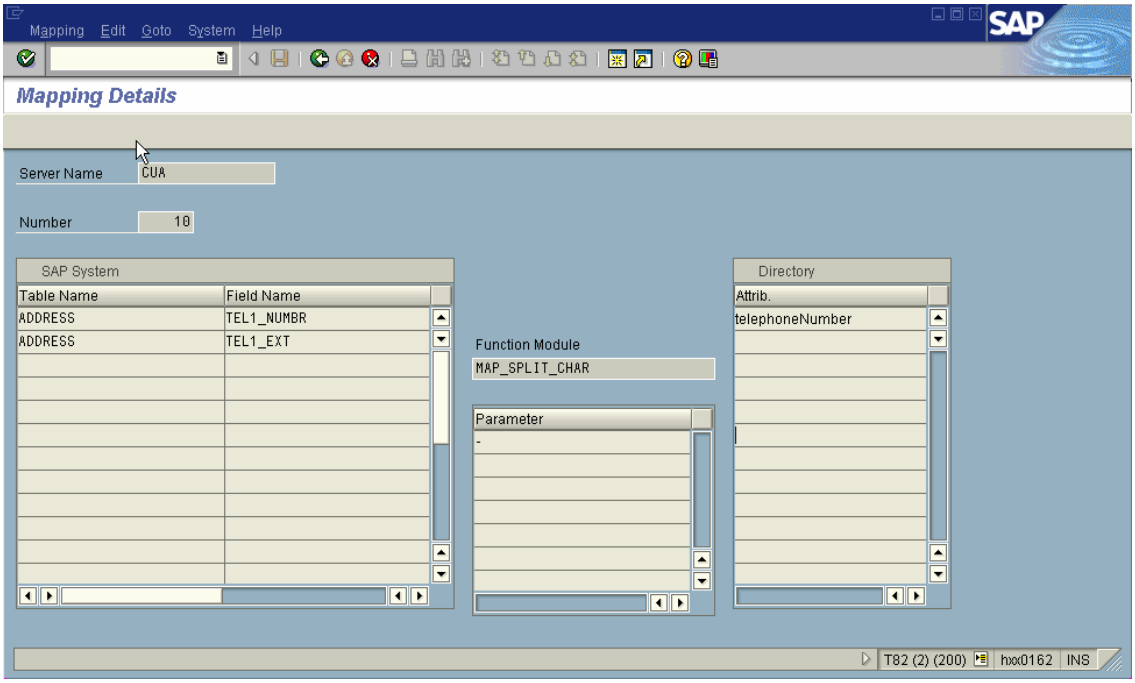


Figure 7 - Mapping using function modules

Synchronization

The report RSLDAPSYNC_USER selects all the users, which are to be synchronized with Active Directory. It is to be scheduled regularly. Furthermore the report can be scheduled as an event triggered job that can be started by the user administrators using the external SAP program *"sapevt"*.

The following screenshot shows report *RSLDAPSYNC_USER*:

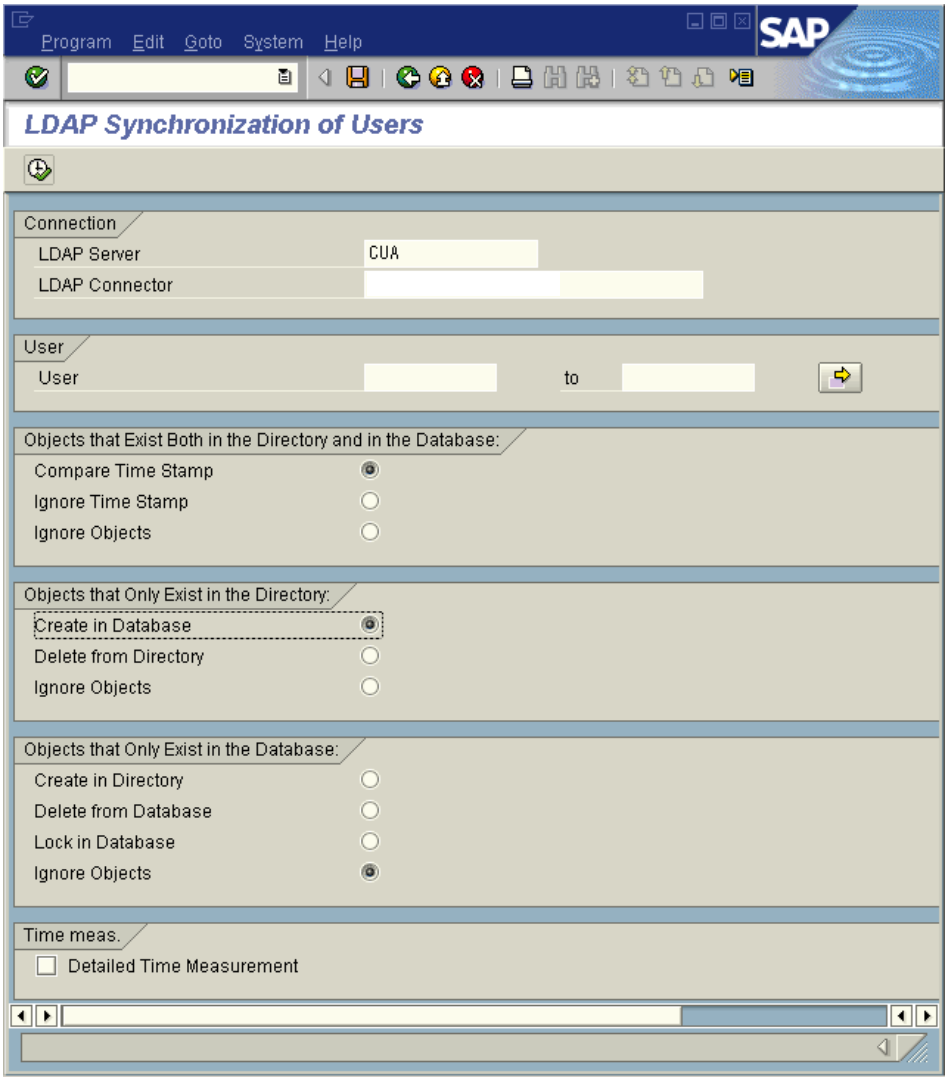


Figure 8 - Report RSLDAPSYNC_USER

Using transaction *LDAPLOG* the protocols of the LDAP synchronizations can be monitored.

Extensions to the standard

Assigning Active Directory Groups to SAP ABAP roles

To provide synchronisation of role assignments the interface BC-LDAP-USR expects the name of the SAP roles to be stored in a multi-value attribute called *SAProles*. The problem with using this setup is how to fill this attribute with the appropriate information.

The SAP user management engine (UME) offers the option to assign portal roles to groups stored in Active Directory if Active Directory is used as user persistence store.

To achieve a comparable functionality out of the box it must be possible to map SAP roles to Microsoft Active Directory groups.

Therefore REALTECH has developed a special report which creates Active Directory groups from SAP roles. Users in Active Directory can now be assigned to these groups which correspond to roles in the SAP system. During synchronization a custom function module retrieves the information about the user's group membership and assigns the corresponding SAP role to the user.

Using this mechanism described above it is possible to leverage Active Directory group memberships for SAP role assignment also for SAP ABAP user management. As a result Active Directory users and SAP users can be administered at a single location.

The following screenshot shows the exported SAP roles that appear as groups in the directory:

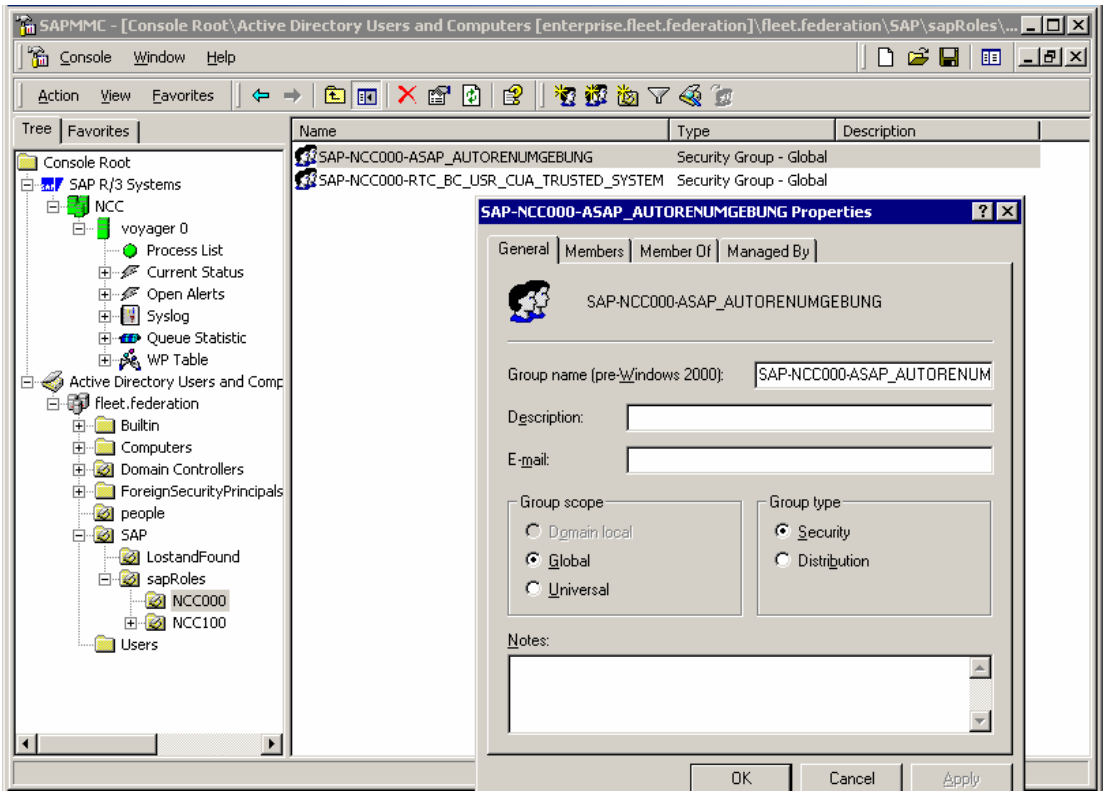


Figure 9 - Exported SAP roles appear as groups in the AD

Maintain SAP specific attributes in Active Directory

Using Microsoft's MMC Snap-In "Users and Computers" it is not possible to maintain attributes others than those delivered as standard attributes by Microsoft. Though it would be possible to use a low level LDAP editor such as the MMC Snap-In "ADSI Edit" this is no user-friendly solution since it would be necessary to use a different tool in the AD for the SAP user administration. Because of this REALTECH has developed a Property Page extension DLL for the Users and Computers Snap-In that makes it possible to maintain the attribute sapUsername (which can be imported into the directory using a schema extension delivered by SAP) in a separate property page SAP of the Users and Computers Snap-In.

The following screenshot shows the new property page "SAP" in the MMC:

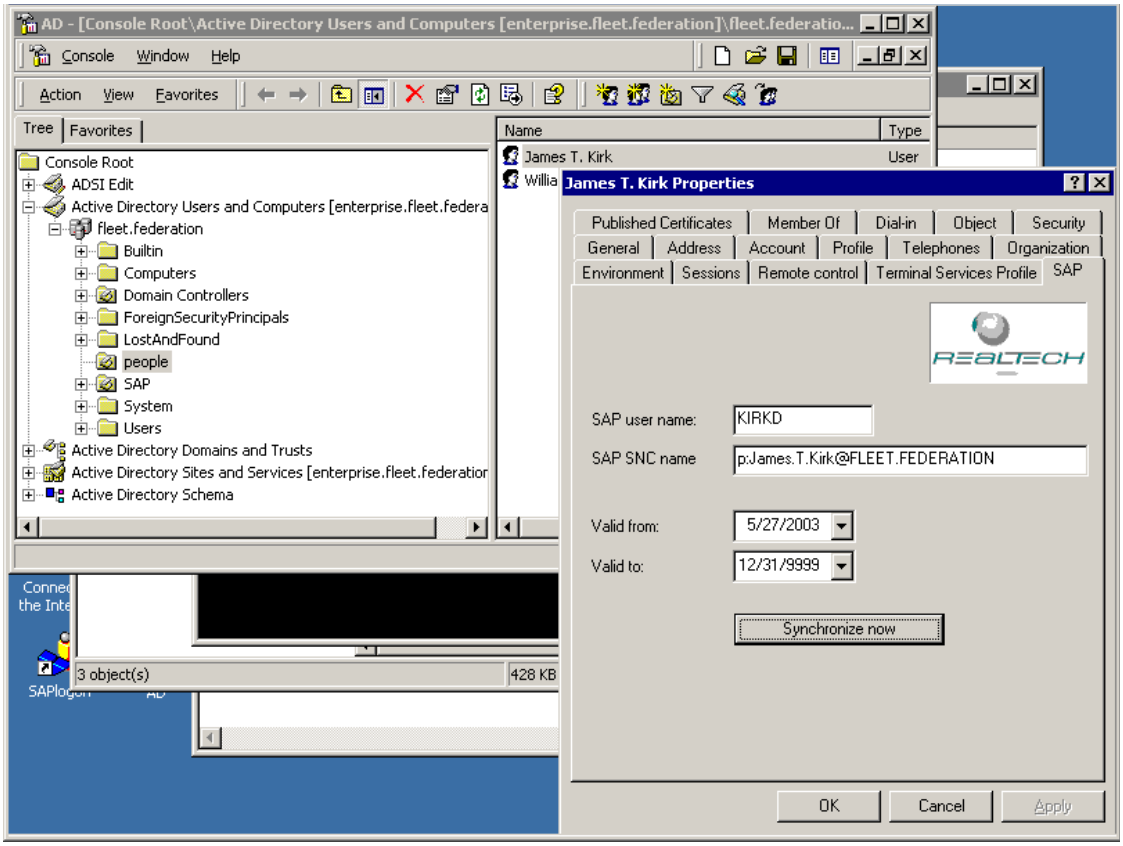


Figure 10 - Extension of MMC Snap-In Users and Computers

The property page also provides a button for immediate synchronization. The button triggers a corresponding event in the SAP system, which then starts the report for user synchronization.

Conclusion

Implementing synchronization between SAP CUA and MS Active Directory provides an easy way to reduce administrative effort and helps to raise the quality of available user data across the entire system landscape.

SAP's LDAP Connector can easily be configured and works seamless with Microsoft Active Directory as it does with other common directory services available on the market.

Limitations

Please keep in mind that the LDAP Connector is only available on SAP systems based on Web Application Server.

Sometimes a schema extension to the relevant directory might be necessary. Please be aware that schema extensions to directories can often not be reverted (e.g. MS Active Directory).

The *Extensions to the standard* described in this collaboration brief are only available as a consulting solution by REALTECH.

References

- SAP Online Help http://help.sap.com
- http://service.sap.com/security → Security in Detail → Identity Management → Directory Services
- Success Story EnBW http://wwwsmart.sap.com/d/0066086_Energie_Baden_Württemberg_AG_S..pdf
- SAP Technical Brief on SAP NetWeaver Platform and Microsoft Active Directory https://www.sdn.sap.com/irj/servlet/prt/portal/prtroot/com.sap.km.cm.docs/documents/a1-8-4/SAP%20Technical%20Brief%20on%20SAP%20NetWeaver%20Platform%20and%20Microsoft%20Active%20Directory.pdf