SAP Active Directory Integration – SSO and Usermanagement

André Fischer (andre.fischer@sap.com)
Project Manager CTSC

Michael Sambeth (michael.sambeth@sap.com)
NetWeaver Practice Unit Enterprise Portal
<table>
<thead>
<tr>
<th>Agenda</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
</tr>
<tr>
<td><strong>User Management</strong></td>
</tr>
<tr>
<td><strong>Single Sign-on</strong></td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
</tr>
</tbody>
</table>
What the user wants ...

- ERP
- CRM
- ESS
- Groupware
- Intranet
- Workflow
- Internet
- Portal
- Logon
- Access
What the administrator wants ...

Central user management
- Single point of administration
- Assign user rights in various applications with one keystroke
- Lock or Delete users centrally

Central user repository
- Avoid redundant user information
What are the prerequisites?

Integrated Cross-Application User Management

- Central storage of user information
  - Group assignment
  - Basic user data
  - Application specific user data

- Standard Access protocol
- Interoperability, Multi vendor and platform support

Solution: LDAP

- LDAP Directories serve as central repository for user master data.
- Access to this data is provided using the standardized Lightweight Directory Access Protocol (LDAP).
- Applications from multiple vendors and platforms can work as LDAP clients -> Interoperability
- Authentication
What are the prerequisites?

**Single Sign-On (SSO)**
- User authenticates once against a security system
- User is afterwards automatically authenticated to access other systems
- Authentication against external applications is transparent for the user
- Logon-Procedure for initial authentication must be secure

**Solution**
- SAP Logon Tickets
  - E.g. with SAP Enterprise Portal, SAP WebAS,...
SAP

- Enterprise Portal / Web AS can use LDAP Directories as User Repository (User Persistence Store)
- Enterprise Portal provides SSO to SAP and MS backend systems using SAP Logon Tickets
- SAP provides a Directory Interface for User Management via LDAP
  - mySAP HR can create / update users in LDAP Directories
  - SAP user data can be synchronized with user data in LDAP Directories

Microsoft Active Directory

- Supports LDAP
- Active Directory is SAP certified (BC-USR-LDAP)
- Windows authentication can be used as external authentication for mySAP Enterprise Portal (SSO to EP)
The big picture

3rd party Applications  Microsoft based applications  mySAP HR  WebDynpro  CUA  mySAP Systems

- SAP ISAPI Filter
- UME (Web AS Java)
- SAP ISAPI Filter

- Create and modify users
- Use as user repository
- Synchronize user data
- Use as user repository

- SAP Enterprise Portal
- UME (Web AS Java)

Active Directory

SSO  Authentication

© SAP AG 2004, MS ADS & SSO, Andre Fischer / Michael Sambeil
Agenda

- Introduction
- User Management
- Single Sign-on
- Conclusion
User Management (step 1)

mySAP HR
- Create modify Directory users

Active Directory
- Assign groups and password

SAP EP & SAP J2EE
- Use Directory as user repository for EP and JAVA users

CUA
- Create / Synchronize SAP ABAP users using BC-LDAP-USR interface
mySAP HR LDAP interface

Goal
- Create / modify users in the directory server automatically from employee data stored in mySAP HR

Reason
- mySAP HR is master system for (basic) employee data
  - First name
  - Last name
  - Employee number
  - Manager
  - ....
- Optimize Administration of users
  - Reduction in operational costs
  - Correctness of data
  - Speed of the process

Restriction
- Only export of data
User information in Active Directory

Attributes that can be provided by mySAP HR

distinguishedName: CN=Andre Fischer, CN=Users, DC=MSCTSC, DC=SAP, DC=CORP;
sn: Fischer
givenName: Andre
employeeNumber: 0123456
sAMAccountName: M0123456
userPrincipalName: andre.fischer@mstsc.sap.corp
... ...

Attributes that are provided by Active Directory and Exchange Administration

mail: andre.fischer@sap.com
memberOf: CN=Users, DC=MSCTSC, DC=SAP, DC=CORP;
CN=Domain Admins, CN=Users, DC=MSCTSC, DC=SAP, DC=CORP;
... }
Data export from mySAP HR using LDAP interface

SAP HR

WebAS

RFC

LDAP

Active Directory

<=4.6C

Extraction

Employee data:
Personel number
First Name
Last Name
...

Mapping

SAP data field -> LDAP attribute

Create / update users

User attributes
Cn
Sn
givenName
...

>=4.7

>= 6.10
Results of export using mySAP HR LDAP interface

=> New users are created as deactivated accounts in Active Directory

=> Existing user accounts will be updated
User Management (step 2)

mySAP HR
- Create modify Directory users

Active Directory
- Assign groups and password

SAP EP & SAP J2EE
- Use Directory as user repository for EP and JAVA users

CUA
- Create / Synchronize SAP ABAP users using BC-LDAP-USR interface
Active Directory - Useradministration

- Activate account
- Assign groups
- Set / Reset password
- Perform additional administrative tasks …
User Management (step 3)

mySAP HR
- Create modify Directory users

Active Directory
- Assign groups and password

SAP EP & SAP J2EE
- Use Directory as user repository for EP and JAVA users

CUA
- Create / Synchronize SAP ABAP users using BC-LDAP-USR interface
Architecture: User Management Engine

Portal Server

User Persistence Store
- LDAP or
- Portal Database or
- SAP System

Basic user data
Basic group data
User → group assignment

Portal Database

UM Instance
- User/group → role assignment
- User mapping (for SSO purposes)

PCD Instance
- User Roles (Metadata)
- Content → role assignment
- User’s personalization data

Store portal-specific data
Portal Users are stored in the Directory

Active Directory groups can be assigned to Portal Roles

Portal specific information is stored in portal database

- group <-> role assignment
- User <-> role assignment

Portal User Id = sAMAccountName (default)

Multiple domains are supported if an attribute is used as portal user id that is unique in the complete forest (the sAMAccountName is only unique in a domain)

LDAP access of the portal to the directory should be secured by SSL
UME result

User can log on to SAP EP immediately.

User is assigned to roles that are assigned to the user or the groups the user has been assigned to.
User Management (step 4)

**mySAP HR**
- Create modify Directory users

**Active Directory**
- Assign groups and password

**SAP EP & SAP J2EE**
- Use Directory as user repository for EP and JAVA users

**CUA**
- Create / Synchronize SAP ABAP users using BC-LDAP-USR interface

---

© SAP AG 2004, MS ADS & SSO, Andre Fischer / Michael Sambeth / 22
Overview SAP LDAP user synchronisation

SAP ABAP user management data can be synchronized with a LDAP directory with systems based on WebAS 6.10 or higher.

SAP Systems with Release 4.5 and higher can be integrated into LDAP using CUA.

LDAP directory interface provides mapping capabilities LDAP attributes and SAP data fields.

SAP User synchronisation and distribution can be performed by background jobs.

Mandatory for 4.5 & 4.6, optional for 4.7 and higher.
LDAP Connector

SAP Application Server

Work Process
Call Function 'LDAP_XXX'
Function 'LDAP_XXX'

LDAP Connector
Connection with LDAP Server

Domain Controller: Active Directory

✓ Executable LDAP_RFC shipped since Release 4.6A
✓ Loads LDAP Library of operating system at runtime
LDAP Connector as Service on Windows

- If operating system of SAP Application Server does not provide a LDAP Library
- LDAP connector runs as Service on Windows
Result of SAP user LDAP synchronisation

User is created / updated with basic user data from LDAP directory

- First Name
- Last Name
- eMail
- Roles (optional)
- ...

Users are created without password

- Passwords are not needed if SSO using SAP Logon Tickets is used
- No security risk since users cannot log on without using SSO via Enterprise portal using an initial password
Q&A: Usermanagement with Microsoft Active Directory
What is Single Sign-on (SSO)?

Single Sign-on
- User authenticates once against a security system
- User is afterwards automatically authenticated to other systems

Authentication
- Initial check of user credentials (for example username/password)
Why using Single Sign-on?

**Typical situation**
- In a complex system landscape an employee has many user IDs with different passwords
- Different procedures for each system to roll-out, reset and change new/existing passwords
- Users find continuous password changing for many systems annoying

**Problems**
- High administration cost and effort
- Security risk: Users write passwords down and store them where they can easily be found

**Solution: Single Sign-on**
- Users only have to remember one password to gain access to every system
- Administration costs and effort are drastically reduced
Authentication Methods – Initial Logon Procedure

Enterprise Portal 6.0 supports various authentication methods

- User ID / password
  - LDAP Directory (for example Active Directory)
  - Portal Database
  - SAP System
- X.509 digital certificates
- Third-party authentication
  - Integrated windows authentication
  - SAP authentication (SAP Web AS or R/3)
  - Others through JAAS interface (pluggable JAAS login modules, e.g. RSA)

SAP integrates into existing Active Directory landscapes

- Initial logon procedure to authenticate user can be delegated to Active Directory
- No additional costs since no 3rd party software is required
- Authentication methods can also be used if portal runs on UNIX
- SAP provides necessary interfaces and tools
  - UME: LDAP Adapter for Active Directory
  - ISAPI Filter for IIS (IISProxy.dll)
Integrated Windows authentication –
SSO Microsoft Windows Logon to Enterprise Portal

Prerequisites
- Separate Webserver: IIS with IISProxy.DLL filter
- Browser: Microsoft Internet Explorer

Authentication of users is delegated to the operating system
- Previous logon to Windows operating system can be reused
- User is not required to reenter his or her Windows authentication credentials

Limitations
- Multiple domains are now supported*. In this case an attribute that is unique in all domains has to be used as portal logon id (for example userPrincipalName)
- Can only be used in Intranet scenarios

*Solution is available for EP 6.0 SP2 on project basis
** EP <=EP6.0 SP2 Patch4: NTLM header is used
Authentication Methods – User Id / Password (LDAP)

Prerequisites

- User Persistence Store: Active Directory

Authentication of users is delegated to the operating system

- User must enter his or her Windows authentication credentials

Typical scenarios

- Extranet scenarios
- Intranet scenarios where a second login using the same username / password should be used
Overview – SSO from EP to backend systems

SAP EP provides SSO to backend systems using
- SAP Logon Tickets
- Account Aggregation

SAP Logon Tickets can be used for SSO to:
- SAP Applications
- Web based applications with the SAP Web Server filter
- JAVA and C applications using SAP’s shared library
- Microsoft Applications using SSO2KerbMap Module *

* Active Directory 2003 required
SSO – Account Aggregation

Features:
- Account aggregation can be used if the external system does not support SAP logon tickets
  - System is maintained in portal system landscape
- Portal components connect to the external system with the user’s credentials (user ID and password), e.g. with SAP ApplIntegrator
  - Credentials submitted via HTTP GET Query String or HTTP POST body
- User mapping and credentials information are securely stored in the Portal Database

Drawbacks and Limitations:
- Redundant administration of credentials
- Stored credentials have to be changed if password changes in a backend system
  - Administrative overhead
- Security update of MS IE [http://user:pwd@server.com](http://user:pwd@server.com)
  - Username and password must not be sent in a URL via the network

Conclusion:
- Seamless SSO technique such as SAP Logon Tickets is preferred
Portal Server issues an SAP logon ticket to a user after successful initial authentication

SAP logon ticket is stored as per session cookie on the client browser

SAP logon ticket is used to authenticate user to applications
- User gets access to multiple applications and services
- After initial logon no further user logons required

SAP logon tickets contains user name(s)

SAP Logon Ticket is signed using digital signature
Verifying the SAP Logon Ticket

**Step 1:**
Verification of the digital signature provided with the SAP logon ticket.

=> Application needs access to issuing server’s public-key certificate

**Step 2:**
Retrieval of the user ID which is stored in the SAP logon ticket.

=> No additional authentication necessary.
SSO to SAP Backend Systems using SAP Logon Tickets

SAP User ID‘s must be equal in all SAP backend system

Portal UserID = SAP UserID in backend systems
- Logon Ticket issued by the portal server contains the portal userID only
- Initial portal authentication is sufficient

Portal UserID ≠ SAP UserID in backend systems
- The user has to logon once initially to the SAP Reference system
- Logon Ticket issued by the portal server contains both, the portal userID and SAP userID in backend systems

If SAP User ID‘s of a portal user are not equal in all SAP backend system SSO via account aggregation has to be used
SAP Reference System

Contains the SAP User ID‘s

Used for mapping between SAP Users and Portal Users in EP

SAP Users can be created / modified using LDAP directory interface

Users have only to logon once to the SAP reference system

SAP CUA system can be used as SAP Reference system
SSO to SAP components using SAP Logon Tickets

Portal

SSO

WebDynpro

BSP-Pages

SAPGUI for HTML

SAPGUI for Windows

Web Dynpro

WebAS

ITS

SAP

© SAP AG 2004, MS ADS & SSO, Andre Fischer / Michael Sambeth / 40
Web Server Filter
- available for several Web Servers (IIS, Apache, iPlanet)
- verifies SAP Logon Ticket and extracts portal user id
- Adds portal user id to http header
- Example: Use by ASP applications

Shared Library
- Dynamic Link Library for verifying SSO Tickets in third party Software
- Native support of SSO using SAP Logon Tickets for applications written in C, Visual Basic
- SAP provides C samples

Java Classes
- Java Classes provided by SAP
- Operating System independent
- Javadoc on SDN contains JAVA samples
SSO to MS based backend systems innovation

Goal:
- Use of Kerberos for authentication on MS backend servers

Windows authentication (Kerberos) is the preferred authentication method in Microsoft environments

Problem:
- Kerberos does not work well across the Internet (firewall config)
- Windows integrated authentication can only be used in intranet scenarios (firewall config, trusted domains)
- To perform Kerberos on a client’s behalf the server needs to have the client’s primary credentials (RFC 1510)
  - Client’s password OR
  - Client’s ticket granting ticket (TGT) and the corresponding session key
- But, Windows Server must NOT know the client’s password which would be a severe breach of trust
Solution: SSO22KerbMap Module

Kerberos Constrained Delegation with Protocol Transition

- Authentication
- On behalf of an end user
- Managability / Constraints
- Applicable where Kerberos would not work natively, e.g. over the Internet
Microsoft has enhanced its implementation of the Kerberos protocol

- Constrained delegation: Service may request a (constrained) Kerberos ticket on behalf of a user for specified services only
- Protocol transition: Client may be authenticated using other methods than Kerberos

SAP has developed the SSO22KerbMap Module (ISAPI Filter)

- Protocol transition: Filter allows authentication using SAP Logon Tickets
- Constrained delegation: Filter can acquire Kerberos Tickets on behalf of user that is authenticated by a SAP Logon Ticket
1. Client with (valid) SAP Logon Ticket
2. Authentication to IIS. ISAPI Filter DLL checks validity of SAP Logon Ticket
3. Identification: ISAPI Filter searches for a user in Active Directory with the user id contained in SAP Logon Ticket.
4. Impersonation as user (LogonAsUser)
5. Constrained Delegation managed by ADS
6. Kerberos Authentication when connecting to backend service as fully qualified Windows Domain User
7. Windows backend application/service accepts constrained kerberos ticket
Sample configuration in ADS for Outlook Web Accesss
Microsoft Exchange Front-End and Back-End Server Architecture

Client – Extranet

Firewall

Global catalog server

Exchange back-end servers

Client - Intranet
Outlook Web Access using SSO22KerbMap Module

Exchange Frontend Server

1. Check SAP Logon Ticket

2. Check if server is trusted for delegation

3. Impersonation Kerberos ticket

Exchange Backend Server(s)

Active Directory

passthrough authentication
Outlook WebAccess for Exchange 2003
Portalized Outlook WebAccess

* German localization
Summary

Kerberos Constrained Delegation with Protocol Transition

- ADS 2003
- SAP Logon Tickets for Authentication on IIS web server
- Authentication to backend
- Microsoft S4U2-Kerberos Extensions
- SAP Logon Tickets for Authentication on IIS web server
<table>
<thead>
<tr>
<th>Agenda</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔ Introduction</td>
</tr>
<tr>
<td>✔ User Management</td>
</tr>
<tr>
<td>✔ Single Sign-on</td>
</tr>
<tr>
<td>✔ Conclusion</td>
</tr>
</tbody>
</table>
Conclusion

SAP Enterprise portal supports open standard LDAP
- integrates into existing LDAP Directories
- Existing groups can be used for role assignment

SAP Enterprise portal provides SSO using SAP Logon Tickets to
- SAP systems
- MS based applications

SAP provides DLL to use integrated windows authentication as SSO to EP

SAP Enterprise Portal serves as an end-to-end SSO solution
Q&A: Single sign-on to Microsoft Systems
SSO2KerbMap Module Download & Dokumentation:

- SAP Software Distribution Center: [http://service.sap.com/swdc](http://service.sap.com/swdc) -> Search and search for the string „sso22kerbmap“

SAP Application Integrator HowTo:


Customizing MS Outlook Web Access:


Microsoft 2003 Kerberos Constrained Delegation:
