IBM Software Group

BPM Security & LDAP - Concepts and Troubleshooting

Sridhar Edam , Shinsou (Al) Wang
sedam@us.ibm.com , wangsh@us.ibm.com
BPM L2 Support Engineers

06/11/2013

WebSphere® Support Technical Exchange

ON DEMAND BUSINESS™

Agenda

- Introduction - background of BPM security LDAP configuration.
- Security Providers
- User and Group Tables
- Entity type mapping
- BPM user Cache
- Configuration files
- Common Problems and solutions
- Mustgather
- References
- Questions

Introduction

- BPM integrates with user repositories which enables utilizing the existing organizational structure to facilitate its human workflow processing.
- The human centric workflow is designed to route the tasks based on the design of a Business Process (BPD). An LDAP integration facilitates using the existing organizational tree to be used for such routing.
- This presentation will focus on concepts , scenarios and troubleshooting of LDAP integration with BPM.

security providers

- Default File Based Repository
  a. Websphere default security provider for users and Groups
- User Repository
  a. LDAP based repository. External to WAS
- BPM Internal Security Provider
  a. BPM internal users stored in the database

Repositories in the realm:

Add Base entry to Realm... | Use built-in repository | Remove

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
☐	o=defaultWIMFileBasedRealm	InternalFileRepository	File
☐	o=mycompany.org	MyTDS	LDAP:IDS
☐	o=twinternal	urbtwinternal	Custom

BPM User and Group Tables

LSW_USR - store default user, BPM internally created user.

LSW_USR_XREF - all available user, historical user.

LSW_USR_GRP_XREF - where LDAP group is/ Ad-hoc group

LSW_USR_GRP_MEM_XREF - defines the relation between user and group

LSW_GRP_GRP_MEM_XREF - defines the hierarchy of group.

When does the group table gets populated?
a) startup b) Manual synch c) system components requesting a JMS cache reset

Sample of Group Sync after starting of the system:

[10/29/12 11:03:24:575 PDT] 00000001 WsServerImpl A WSVR0001I: Server server1 open for e-business

...

[10/29/12 11:05:34:984 PDT] 00000044 wle I CWLLG0446I: Group Alsgroup is being checked for new updates

...

Sample of When user log in to Portal

[10/29/12 11:05:35:078 PDT] 00000044 wle_security I CWLLG1088I: Initializing session is done for user alwangaa

BPM security tables

Table - LSW_USR

Schema : BPMADMIN
Creator : BPMADMIN
Columns : 7

Actions:

Open
Query
Show Related Objects
Create New Table

Columns

Key	Name	Data type	Length	Nullable
🔑	USER_ID	DECIMAL	12	No
	USER_NAME	VARCHAR	200	No
	PASSWD	VARCHAR	1000	No
	FULL_NAME	VARCHAR	200	No
	IS_DISABLED	CHARACTER	1	Yes
	LAST_LOGIN_DATETIME	TIMESTAMP	10	Yes
	OLD_PASSWORDS	CLOB	2147483647	Yes

Table - LSW_USR_XREF

Schema : BPMADMIN
Creator : BPMADMIN
Columns : 4

Actions:

Open
Query

Columns

Key	Name	Data type	Length	Nullable
🔑	USER_ID	DECIMAL	12	No
	USER_NAME	VARCHAR	256	No
	FULL_NAME	VARCHAR	1020	Yes
	PROVIDER	VARCHAR	512	Yes

Table - LSW_USR_GRP_XREF

Schema : BPMADMIN
Creator : BPMADMIN
Columns : 7

Actions:

Open
Query
Show Related Objects
Create New Table

Columns

Key	Name	Data type	Length	Nullable
🔑	GROUP_ID	DECIMAL	12	No
	GROUP_NAME	VARCHAR	404	No
	DISPLAY_NAME	VARCHAR	512	No
	PARENT_GROUP_ID	DECIMAL	12	Yes
	GROUP_TYPE	DECIMAL	2	No
	DESCRIPTION	VARCHAR	1020	Yes
	GROUP_STATE	DECIMAL	2	No

BPM security tables

Table - LSW_USR_GRP_MEM_XREF

Schema : BPMADMIN
Creator : BPMADMIN
Columns : 2

Actions:
Open

Columns

Key	Name	Data type	Length	Nullable
🔑	USER_ID	DECIMAL	12	No
🔑	GROUP_ID	DECIMAL	12	No

Table - LSW_GRP_GRP_MEM_XREF

Schema : BPMADMIN
Creator : BPMADMIN
Columns : 2

Actions:

Columns

Key	Name	Data type	Length	Nullable
🔑	GROUP_ID	DECIMAL	12	No
🔑	CONTAINER_GROUP_ID	DECIMAL	12	No

BPM User Cache

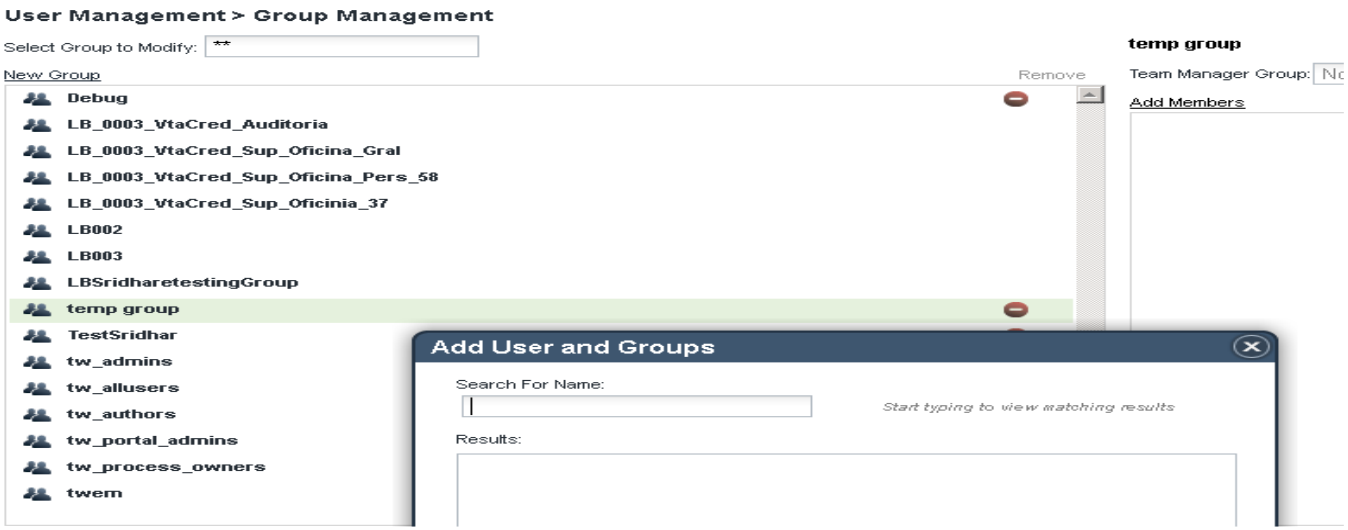
When does user gets cached into BPM?

a)full sync

b)log in

c)Process Admin search.

*If user is not known to BPM, error might occurs when routing task to it.

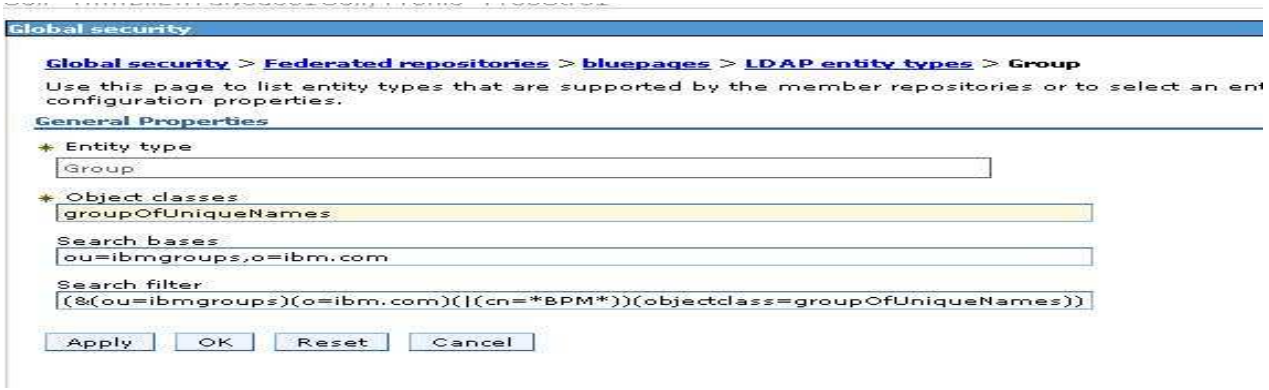


WAS - LDAP Mapping


```
cn=BPML2_US,ou=memberlist,ou=ibmgroups,o=ibm.com
objectClass=ibm-nestedGroup
objectClass=groupOfUniqueNames
objectClass=top
ou=memberlist
ou=ibmgroups
o=ibm.com
cn=BPML2_US
uniquemember=uid=          ,c=us,ou=          ,o=ibm.com
```

LDAP Search Filters

- http://bpmwiki.blueworkslive.com/display/commwiki/Configure WLE 7.1 LDAP Filters



BPM security configuration files

security.xml

```
<?xml version="1.0" encoding="UTF-8" ?>
- <security:Security xmi:version="2.0" xmlns:xmi="http://www.omg.org/XMI"
    xmlns:orb.securityprotocol="http://www.ibm.com/websphere/appserver/schemas/5.0/orb.securityprotocol.xm
    xmlns:security="http://www.ibm.com/websphere/appserver/schemas/5.0/security.xmi"
    xmi:id="Security_1" useLocalSecurityServer="true" useDomainQualifiedUserNames="false" enabled="true"
    cacheTimeout="600" issuePermissionWarning="true" activeProtocol="BOTH" enforceJava2Security="false"
    enforceFineGrainedJCASecurity="false" appEnabled="false" dynamicallyUpdateSSLConfig="true"
    activeAuthMechanism="LTPA_1" activeUserRegistry="WIMUserRegistry_1"
    defaultSSLSettings="SSLConfig_mitchtestNode02_1">
    <authMechanisms xmi:type="security:SWAMAuthentication" xmi:id="SWAMAuthentication_1" OID="No OID for
      this mechanism" authContextImplClass="com.ibm.ISecurityLocalObjectGSSUPImpl.WSSecurityContext"
      authConfig="system.SWAM" simpleAuthConfig="system.SWAM" authValidationConfig="system.SWAM" />
  - <authMechanisms xmi:type="security:LTPA" xmi:id="LTPA_1" OID="oid:1.3.18.0.2.30.2"
      authContextImplClass="com.ibm.ISecurityLocalObjectTokenBaseImpl.WSSecurityContextLTPAImpl"
      authConfig="system.LTPA" simpleAuthConfig="system.LTPA" authValidationConfig="system.LTPA"
```

wimconfig.xml (wim = Websphere identity manager)

```
<config:repositories xsi:type="config:LdapRepositoryType" adapterClassName="com.ibm.ws.wim.adapter.ldap.LdapAdapter"
    id="WLE AD" isExtIdUnique="true" supportAsyncMode="false" supportExternalName="false"
    supportPaging="false" supportSorting="false" supportTransactions="false" certificateFilter=""
    certificateMapMode="exactdn" ldapServerType="AD" translateRDN="false">
  <config:baseEntries name="DC=supp,DC=bpm,DC=ibm,DC=com" nameInRepository="DC=supp,DC=bpm,DC=ibm,DC=com"/>
  <config:loginProperties>uid</config:loginProperties>
  <config:ldapServerConfiguration primaryServerQueryTimeInterval="15" returnToPrimaryServer="true"
      sslConfiguration="">
    <config:ldapServers authentication="simple" bindDN="CN=Administrator,CN=Users,DC=supp,DC=bpm,DC=ibm,DC=com"
        bindPassword="{xor}MywoPjsyNjE=" connectionPool="false" connectTimeout="0"
        derefAliases="always" referal="ignore" sslEnabled="false">
      <config:connections host="pants.supp.bpm.ibm.com" port="389"/>
    </config:ldapServers>
```

BPM security configuration files (Cont'd)

admin-authz.xml
Stores WAS Administrative user roles.

Administrative user roles

Use this page to add, update or to remove administrative roles to users. Assigning administra
the administrative console or through wsadmin scripting.

Logout | Add... | Remove

Select	User	Role(s)
	admin	Primary administrative user name
☐	admin	Administrator
☐	bpmAuthor	Operator, Deployer
☐	tw_admin	Operator, Deployer
☐	tw_author	Operator, Deployer
☐	wangsh@us.ibm.com	Administrator, Admin Security Manager

Total 6

Common Problems and Solutions

- Redlight for an App in Process Designer.
  Network connection issue will result Process Designer displaying red-light.
  A Process App opened in process designer initiates a deploy of that App into process Center.
  Lacking WAS Admin Roles when developing application with Advanced content will result redlight as well.
  http://pic.dhe.ibm.com/infocenter/dmndhelp/v8r0mx/topic/com.ibm.wbpm.admin.doc/topics/deploying_introduction.html

- Unable to login to any BPM console including WAS Admin console when repository is down
  http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=%2Fcom.ibm.websphere.wim.doc%2FUnableToAuthenticateWhenRepositoryIsDown.html

- Switching Login attribute may result new users generated on LSW_USR_XREF table.

- Process Admin does not show groups from LDAP after configuration.
  Process Admin synchronizes all visible group by sending a query “*” for group. If LDAP is configured not accepting wild card character. LDAP timeout.

- Active Directory may have a default value for a maximum search result. Change MaxPageSize according to attaching technote:
  http://www-01.ibm.com/support/docview.wss?uid=swg21439593

Common Problems and Solutions (continued)

- Error during start up (com.ibm.websphere.wim.exception.MaxResultsExceededException: CWWIM1018E '4501'search results exceeds the '4500' maximum search limit.
  a) wimconfig has a variable of maxSearchResults which can be changed.
  b) We also recommend using search filter
- SqlIntegrityConstraintViolationException gets thrown during group replication process. Additionally, upon server startup, LDAP groups are not visible from WebSphere Application Server Administrative Console and Process Admin Console.
  http://www-01.ibm.com/support/docview.wss?uid=swg21619620
- JS API tw.System.org.FindUserByName() throws NPE when user has not log on to BPM.
  http://www-01.ibm.com/support/docview.wss?uid=swg1JR42912
- Adding a new user to LDAP but it is not visible in BPM.
  Check the user's DN with filter
- LDAP group name longer than 255 char will result a sql error.
- WAS ldapsearch utility
  http://www-01.ibm.com/support/docview.wss?uid=swg21113384

BPM mustgather

Trace Strings.

=info:com.ibm.ws.security.=all:com.ibm.websphere.security.*=all:com.ibm.websphere.wim.*=all:com.ibm.wsspi.wim.*=all:com.ibm.ws.wim.*=all:WLE.wle_security=finest

Config tree

The profile config directory that stores the profile configuration in XML files
In an ND environment , config directories from both DMGR and Federated Nodes.

Contents of the xref tables
The user and group information is stored in the database tables.
The XREF tables replicate user and group information from LDAP as well.

References

- http://pic.dhe.ibm.com/infocenter/dmndhelp/v8r0mx/topic/com.ibm.wbpm.admin.doc/topics/deploying_introduction.html
- http://www-01.ibm.com/support/docview.wss?uid=swg21439593
- http://www-01.ibm.com/support/docview.wss?uid=swg21113384
- http://www-01.ibm.com/support/docview.wss?uid=swg21619620

Summary

- Different repositories supported by BPM
- Understanding the configuration files & DB tables used by BPM helps narrowing down the issues.
- Using of LDAP Filters is key to organize BPM users / groups and improving performance.
- Key items to be looked at when switching LDAP
- Common known problems and solutions described to resolve such occurrences

Additional WebSphere Product Resources

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at:
  http://www.ibm.com/software/websphere/support/supp_tech.html
- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at:
  http://www.ibm.com/developerworks/websphere/community/
- Join the Global WebSphere Community:
  http://www.websphereusergroup.org
- Access key product show-me demos and tutorials by visiting IBM® Education Assistant:
  http://www.ibm.com/software/info/education/assistant
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically:
  http://www.ibm.com/software/websphere/support/d2w.html
- Sign up to receive weekly technical My Notifications emails:
  http://www.ibm.com/software/support/einfo.html

Connect with us!

1. **Get notified on upcoming webcasts**
   Send an e-mail to wsehelp@us.ibm.com with subject line “wste subscribe” to get a list of mailing lists and to subscribe
2. **Tell us what you want to learn**
   Send us suggestions for future topics or improvements about our webcasts to wsehelp@us.ibm.com
3. **Be connected!**
   Connect with us on Facebook
   Connect with us on Twitter

Questions and Answers