

# CA Directory r12sp17+ and IBM WebSphere (WAS) 8.8.5

Scripted process to setup a Federated LDAP Userstore in WAS 8.8.5

Goal: Using “Custom” Label with CA Directory instead of Open format  
of pre-configured “Domino” Label

Alan Baugher, CA Sr. Principal Architect

April 2016

# Goals

- ❑ Any LDAPv3 directory will work with IBM WebSphere 8.8.x as a Federated Repository /Userstore per IBM documentation.
- ❑ IBM WAS provides a few pre-defined LDAP templates.
- ❑ The IBM Lotus Domino template allows “un-restricted” access to objectClasses & primary unique identifiers, to be used with CA Directory or OpenLDAP.
- ❑ However, as a goal, we would like to understand the management of the LDAP search criterial of the IBM WAS for Federated Repositories; and therefore will use the “Custom” option. This deck will use IBM command line processes to define variables for an LDAP store and the use the Jython scripting language to setup the Federated LDAP repository.



# Methodology

- ❑ Deploy IBM WAS 8.8.5 server.
  - Download from IBM and deploy on MS Windows OS or RHEL Linux
- ❑ Backup the IBM WAS 8.8.5 Cell that was created as part of the installation.
  - ❑ Save the cell as a compress file.
  - ❑ Save a copy of the wimconfig.xml file as a check point file.
- ❑ Download and install CA Directory r12.0sp17 or higher
  - ❑ Deploy the sample DSA of democorp [Included in CA Directory samples]
  - ❑ Update an exist user record as an administrator with a password & declare this uid as the service bind account.
  - ❑ Enable dynamic group functionality
  - ❑ Create a group OU and populate with groups and dynamic LDAP queries
- ❑ Download and Install Open Source WinMerge tool
  - ❑ Use as comparison tool for before / after state of updates to the wimconfig.xml file.
  - ❑ This process will validate what GUI checkboxes or updates occur to this file.
  - ❑ This process will validate any Jython / wsadmin CLI processes emulate the GUI updates to this file.
- ❑ Download and Install NotePad++ / TextPad
  - ❑ Use to edit the wimconfig.xml file
- ❑ Use “list” mode of the Jython script language to allow variable substitution
- ❑ Use IBM documentation for wsadmin/jython example
- ❑ Validation.
  - ❑ Bounce IBM WAS Service to clean cache entries
  - ❑ Login to IBM WAS UI
    - ❑ Setup initial Federated Repository using pre-defined template of “IBM Domino Server”
    - ❑ Validate Global Security / Federated Repositories Look Correct.
    - ❑ Exercise Use-Case with Users and Groups. Ensure all users are viewed. Validate all groups with static and dynamic members are displayed.
    - ❑ Save the wimconfig.xml file for “IBM Domain Server” state, then remove this configuration in the WAS UI.
    - ❑ Start effort to build a Custom template for CA Directory
  - ❑ Use WinMerge tool to compare before / after states with wimconfig.xml file.

# Background: IBM WAS Scripting Languages Supported

- JACL
  - TCL with Java
  - [Jacl](#) is a Tcl 8.x interpreter written in Java. You can script your Java applications in Tcl.
  - <http://wiki.tcl.tk/1215>
- JYTHON
  - Python with Java
  - **Jython** is an implementation of the [Python programming language](#) designed to run on the [Java](#) platform. Jython programs can import and use any Java class.
  - <https://en.wikipedia.org/wiki/Jython>
  - <http://www.wasscripting.com/index.html>
    - <http://www.amazon.com/WebSphere-Application-Server-Administration-Jython/dp/0137009526>
- IBM Websphere uses both for scripting with CLI command tool, **wsadmin**
  - [https://www.ibm.com/support/knowledgecenter/SSAW57\\_8.5.5/com.ibm.websphere.nd.doc/ae/rxml\\_atidmgrrepositoryconfig.html](https://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/rxml_atidmgrrepositoryconfig.html)
  - [https://www.ibm.com/support/knowledgecenter/was\\_beta/com.ibm.websphere.base.doc/ae/rxml\\_commandline.html](https://www.ibm.com/support/knowledgecenter/was_beta/com.ibm.websphere.base.doc/ae/rxml_commandline.html)
  - Per IBM Support Ticket, this is a preferred model for IBM to support and address any issues.

# Background: References

- Using wsadmin for administering a WebSphere environment - David Hare
  - [www-01.ibm.com/support/docview.wss?uid=swg27011283&aid=1&usg=AFQjCNFI9\\_ub12unJuxo4Y1mzQt7EVJbjA](http://www-01.ibm.com/support/docview.wss?uid=swg27011283&aid=1&usg=AFQjCNFI9_ub12unJuxo4Y1mzQt7EVJbjA)
- <WAS\_HOME>/bin/wsadmin.bat
  - Supports both Jacl and Jython scripting languages.
  - wsadmin –f <script> / wsadmin –c <command> / wsadmin –help
    - wsadmin provides five command objects:
      - **AdminControl** - for operational commands.
      - **AdminConfig** - for configurational commands
      - **AdminApp** - for administering applications.
      - **AdminTask** - for administrative commands.
  - Note: If the Global security is enabled...you will be asked for user name and password or you can specify it inline using –user and –password.
  - Note:
    - The remote method invocation (RMI), also known as the ORB bootstrap, port is designed to improve performance and communication with the server. The RMI connection is JSR 160 RMI compliant. The default setting of the RMI port is 2809
    - The SOAP connector port is more firewall compatible. The default setting of the SOAP port is 8880

[https://www.ibm.com/support/knowledgecenter/was\\_beta/com.ibm.websphere.wdt.doc/topics/tsoapv6.htm](https://www.ibm.com/support/knowledgecenter/was_beta/com.ibm.websphere.wdt.doc/topics/tsoapv6.htm)

<https://webspheredevelopmentnotes.wordpress.com/2012/12/25/wsadmin-tutorial-part1/>

# Background: Wsadmin - WAS Command Line Interface

```
wsadmin>print Help.help()
```

```
Wsadmin>print AdminTask.help('-commands')
```

```
\AppServer\bin>wsadmin.bat -username wsadmin -password Password01 -lang jython
```

```
WASX7209I: Connected to process "server1" on node baual01w7Node01 using SOAP connector; The type of process  
is: UnManagedProcess
```

```
WASX7031I: For help, enter: "print Help.help()"
```

```
wsadmin>
```

Ref:

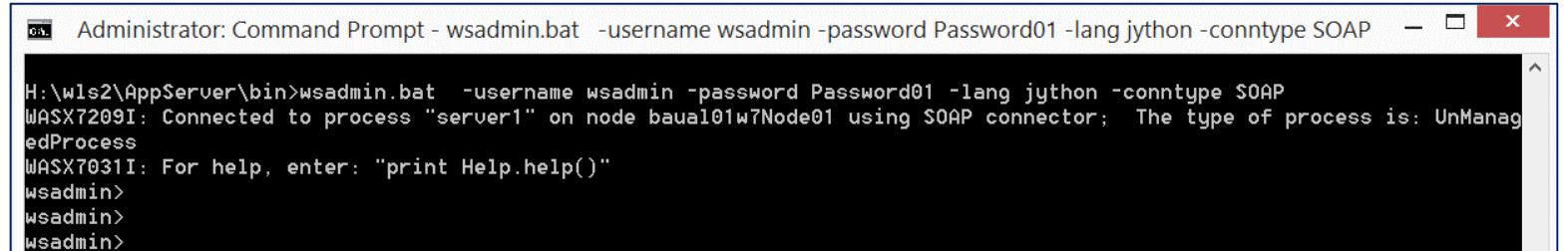
[https://www.ibm.com/support/knowledgecenter/SSAW57\\_8.5.5/com.ibm.websphere.nd.doc/ae/welc\\_howdoi\\_tscr.html](https://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/welc_howdoi_tscr.html)

# Background: Execute Jython Script

## Interactively

```
bin>wsadmin.bat -username wsadmin -password Password01 -lang jython -conntype SOAP
```

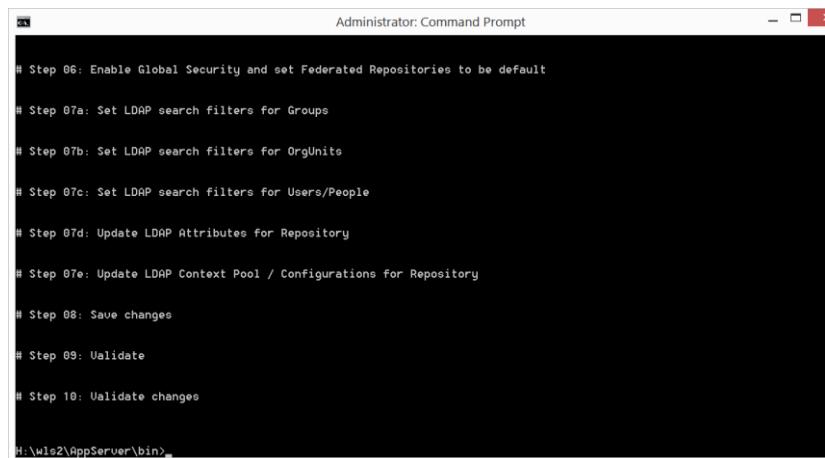
- Copy –n- paste file here
- Monitor for any error message



The screenshot shows an Administrator Command Prompt window titled "Administrator: Command Prompt - wsadmin.bat -username wsadmin -password Password01 -lang jython -conntype SOAP". The command entered is "H:\wls2\AppServer\bin>wsadmin.bat -username wsadmin -password Password01 -lang jython -conntype SOAP". The output shows the connection to "server1" on node "baual01w7Node01" using the SOAP connector, and it indicates that the process type is "UnManagedProcess". It also provides help information: "WASX7031I: For help, enter: "print Help.help()"".

## Input File

```
bin>wsadmin.bat -username wsadmin -password Password01 -lang jython -conntype SOAP -f "filename.py"
```



The screenshot shows an Administrator Command Prompt window titled "Administrator: Command Prompt". The command entered is "H:\wls2\AppServer\bin>wsadmin.bat -username wsadmin -password Password01 -lang jython -conntype SOAP -f "filename.py"". The output displays a series of comments starting with "# Step 06: Enable Global Security and set Federated Repositories to be default" through "# Step 10: Validate changes".

# Background: WAS CLI Debug

1. Enable wsadmin tracing by editing the wsadmin.properties file
  1. <WAS\_HOME>/profiles/<PROFILE\_NAME>/properties/wsadmin.properties
2. Enable “Admin=all” tracing on each server process involved.
  1. Uncomment the following line by removing the #:
  2. #com.ibm.ws.scripting.traceString=com.ibm.\*=all=enabled
3. Run the script / commands with tracing enabled and review the server side trace.log and wsadmin.traceout
4. Open up the wsadmin.traceout file at:  
<WAS\_HOME>/profiles/<PROFILE\_NAME>/logs/wsadmin.traceout  
“mode to generate a single working command:

# Steps to Enable Custom Label for CA Directory

# Step 01: Backup WAS Cell Before Starting

AppServer > profiles > AppSrv01 > config > cells >			
Name	Date modified	Type	Size
baual01w7Node01Cell	4/7/2016 3:05 PM	File folder	
baual01w7Node01Cell.7z	4/7/2016 3:21 PM	7Z File	679 K

<< config > cells > baual01w7Node01Cell > wim > config >			
Name	Date modified	Type	Size
authz	3/6/2016 11:46 PM	File folder	
wimconfig.xml	4/7/2016 3:12 PM	XML File	12 KB
wimconfig-OOTB-Before_any_modification.xml	4/7/2016 1:59 PM	XML File	12 KB
wimconfig-other.xml	3/28/2016 5:00 PM	XML File	16 KB

# Step 02: Review WAS Federated Repositories: Before State

The screenshot displays the WebSphere Global security configuration interface. The main window shows the 'Global security' panel with various security settings like administrative security, authentication mechanisms, and Java 2 security. A red box highlights the 'Available realm definitions' section under 'Federated repositories', which lists 'defaultWIMFileBasedRealm'. Below this, a red arrow points to a terminal window showing the command `AdminTask.listIdMgrRepositories()`. Another red arrow points from the same section to a second 'Manage repositories' window, which also lists 'InternalFileRepository'.

**Global security > Federated repositories**

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm can consist of identities in the file-based repository that is built into the system, in one or more external repositories, or in both the built-in repository and one or more external repositories.

**General Properties**

\* Realm name: defaultWIMFileBasedRealm

\* Primary administrative user name: wsadmin

**Server user identity**

Automatically generated server identity

Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node

Ignore case for authorization

Allow operations if some of the repositories are down

**Repositories in the realm:**

Select	Base Entry	Repository Identifier	Repository Type
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File

Total 1

**Additional Properties**

- Manage repositories
- Trusted authentication realms - inbound

**Global security**

**Global security > Federated repositories > Manage repositories**

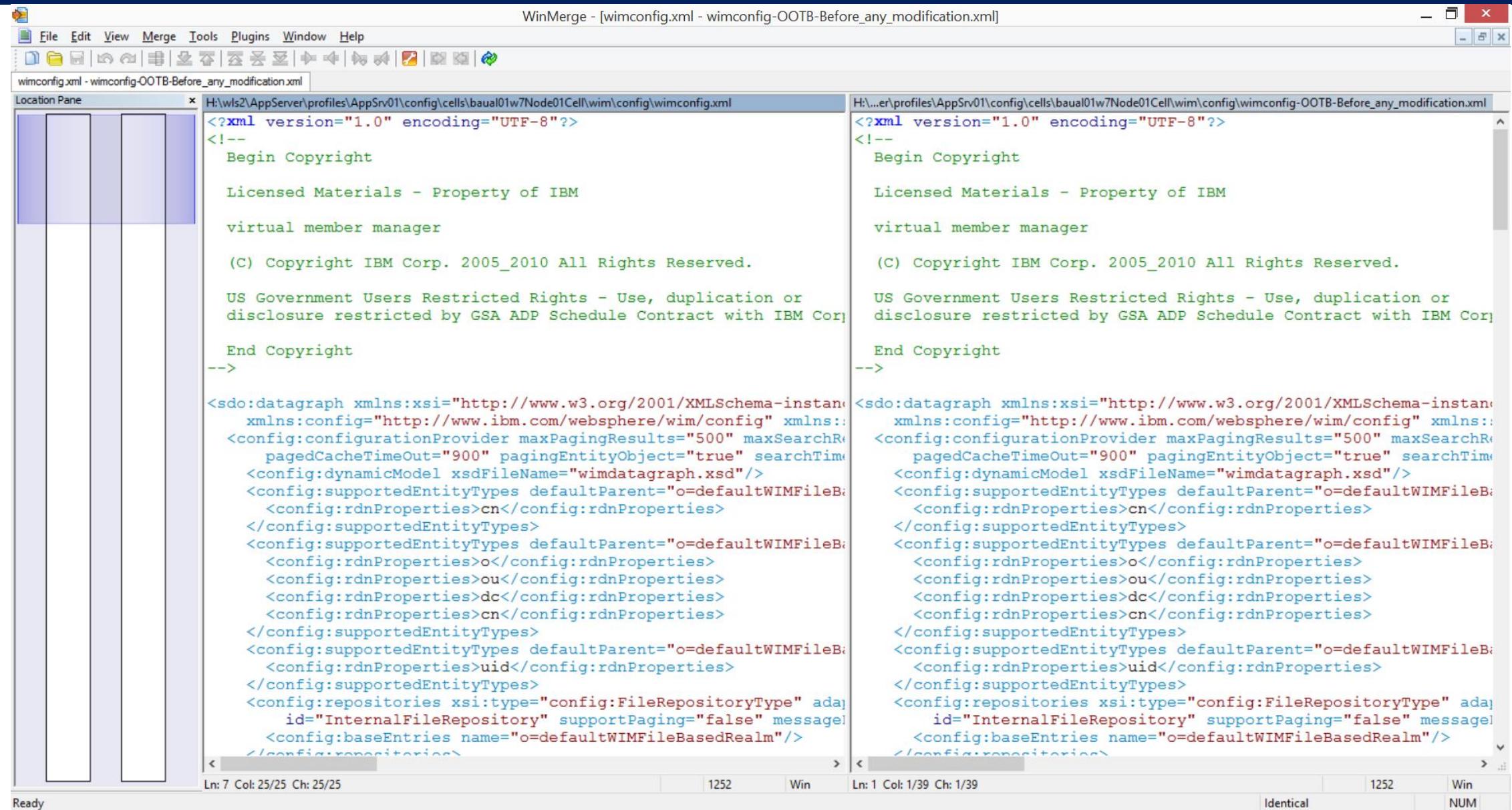
Repositories that are configured in the system are listed in the following table. You can add or delete external repositories.

**Add** **Delete**

Select	Repository Identifier	Repository Type
<input type="checkbox"/>	InternalFileRepository	File

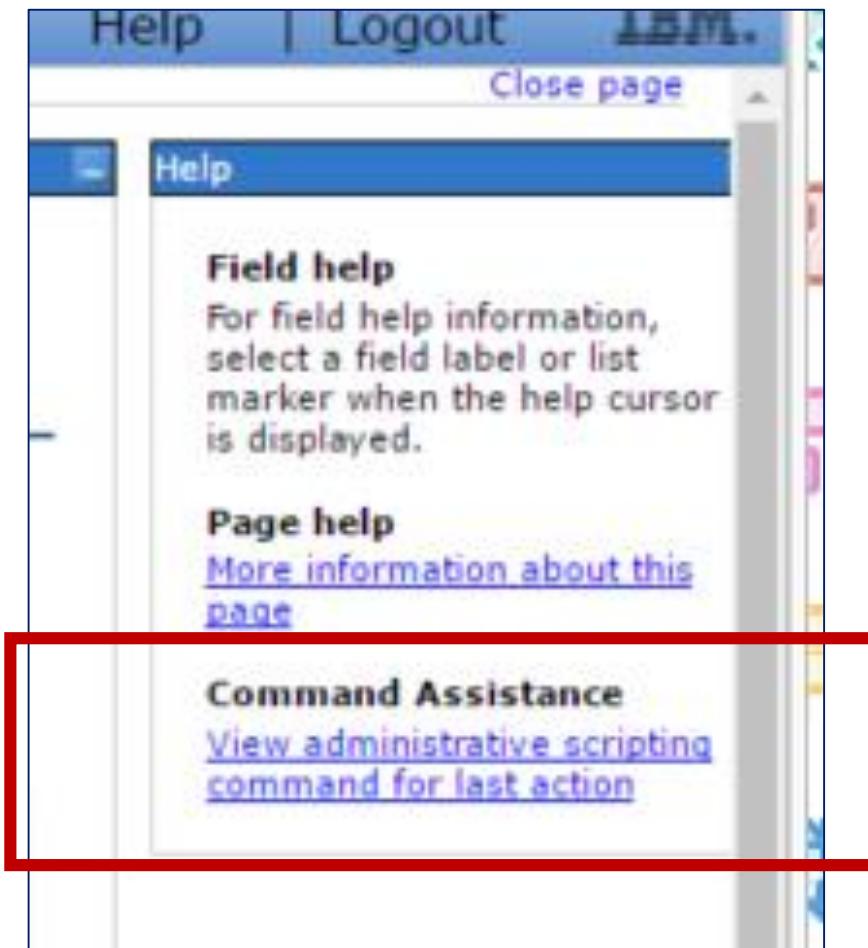
Total 1

Step 03: Make backup copy of wimconfig.xml and open within WinMerge Tool



## Step 04: Perform configuration steps in UI.

Use WAS Help Guide on Admin Scripting to display last command used in UI



The screenshot shows a Google Chrome browser window titled 'Administrative Scripting Commands - Google Chrome'. The URL is https://localhost:9043/ibm/console/com.ibm.ws.console.core.commandassistance.forwardCn. The page lists various wsadmin scripting commands:

- AdminTask.listIdMgrRepositories()
- AdminTask.getIdMgrRepository(['-id CA\_Directory'])
- AdminTask.listIdMgrLDAPServers(['-id CA\_Directory'])
- AdminTask.getIdMgrLDAPServer(['-id CA\_Directory -host 192.168.92.139'])
- AdminTask.listIdMgrLDAPAttrs(['-id CA\_Directory'])
- AdminTask.listIdMgrLDAPBackupServers(['-id CA\_Directory -primary\_host 192.168.92.139'])
- AdminTask.listIdMgrSupportedLDAPServerTypes()
- AdminTask.listIdMgrCustomProperties(['-id CA\_Directory'])
- AdminTask.getActiveSecuritySettings()

Total 9

## Step05: Define variables to be used in an IBM WAS wsadmin Jython script

```
# Configure CA Directory r12.x with IBM WAS 8.8.5 LDAP Federation Repository
# Set Variables for CUSTOM LDAP for IBM WAS 8.8.5
# Need quotes around variables
_ID_LABEL_ = 'CA_Directory'
_ADMIN_ID_ = 'wsadmin'
_ADMIN_PASSWORD_ = 'Password01'
_BIND_DN_ = 'cn=diradmin,ou=serviceaccount,ou=cam,o=ca'
_BIND_PASSWORD_ = 'Password01'
_BASE_OU_ = 'ou=cam,o=ca'
_PEOPLE_OU_ = 'ou=people,ou=cam,o=ca'
_PEOPLE_OBJECTCLASS_ = 'inetOrgPerson'
_GROUP_OU_ = 'ou=groups,ou=cam,o=ca'
_HOSTNAME_ = '192.168.92.139'
_PORT_ = '41389'
```

# Step 06a: Develop Jython Script to Add CA Directory as Custom WAS Federated Repository

```
# Configure CA Directory r12.x with IBM WAS 8.8.5
_ID_LABEL_ = 'CA_Directory'
_ADMIN_ID_ = 'wsadmin'
_ADMIN_PASSWORD_ = 'Password01'
_BIND_DN_ = 'cn=diradmin,ou=serviceaccount,ou=cam,o=ca'
_BIND_PASSWORD_ = 'Password01'
_BASE_OU_ = 'ou=cam,o=ca'
_PEOPLE_OU_ = 'ou=people,ou=cam,o=ca'
_PEOPLE_OBJECTCLASS_ = 'inetOrgPerson'
_GROUP_OU_ = 'ou=groups,ou=cam,o=ca'
_HOSTNAME_ = '192.168.92.139'
_PORT_ = '41389'

print'# Step 01a: Check WIM admin/password are correct = \
+AdminTask.WIMCheckPassword(['-username', _ADMIN_ID_, '-password',
,_ADMIN_PASSWORD_])

print'# Step 01b: See if Global Security is Enabled = \
+AdminTask.isGlobalSecurityEnabled()

print'# Step 01c: Validate current configurations'
AdminTask.listIdMgrRepositories()

print'# Step 02: Ensure Admin User still uses file based to avoid locking our selves
out.'
AdminTask.configureAdminWIMUserRegistry(['-
realmName','defaultWIMFileBasedRealm','verifyRegistry','false'])

print'# Step 03a: Remove LDAP Server Place Holder'
AdminTask.deleteIdMgrRealmBaseEntry(['-name','defaultWIMFileBasedRealm','-
baseEntry',_BASE_OU_])
AdminConfig.save()
AdminTask.deleteIdMgrRepository(['-id',_ID_LABEL_])

print'# Step 03b: Add LDAP Server Place Holder'
AdminTask.createIdMgrLDAPRepository(['-default','true','-id', _ID_LABEL_,'-
adapterClassName','com.ibm.ws.wim.adapter.Idap.LdapAdapter','-
ldapServerType','CUSTOM','sslConfiguration','','certificateMapMode','exactdn','-
supportChangeLog','none','certificateFilter','','loginProperties','uid'])

print'# Step 03c: Update LDAP Server authentication bind / hostname'
AdminTask.addIdMgrLDAPServer(['-id',_ID_LABEL_,'-host',_HOSTNAME_,'-
port',_PORT_,'-bindDN',_BIND_DN_,'-bindPassword',_BIND_PASSWORD_,'-
referral','ignore','sslEnabled','false','ldapServerType','CUSTOM','sslConfiguration','','-
certificateMapMode','exactdn','certificateFilter'])

print'# Step 03d: Clear out any default Login Properties'
AdminTask.updateIdMgrLDAPRepository(['-id',_ID_LABEL_,'-loginProperties','[""]'])
```

```
print'# Step 03e: Update Repository'
AdminTask.updateIdMgrLDAPRepository(['-id',_ID_LABEL_,'-
adapterClassName','com.ibm.ws.wim.adapter.Idap.LdapAdapter','-
ldapServerType','CUSTOM','sslConfiguration','','certificateMapMode','exactdn','-
certificateFilter','','supportChangeLog','none','loginProperties','uid'])

print'# Step 04a: Add the Base Entries [NOTE: Base OU MUST be UNIQUE in the
Realm]'
AdminTask.addIdMgrRepositoryBaseEntry(['-id',_ID_LABEL_,'-name',_BASE_OU_,'-
nameInRepository',_BASE_OU_])

print'# Step 04b: Update default WIM'
AdminTask.addIdMgrRealmBaseEntry(['-name','defaultWIMFileBasedRealm','-
baseEntry',_BASE_OU_])

print'# Step 05: Validate the Admin Name ( wasadmin in file-based registry )'
AdminTask.validateAdminName(['-registryType','WIMUserRegistry','-
adminUser',_ADMIN_ID_])

print'# Step 06: Enable Global Security and set Federated Repositories to be
default'
AdminTask.setAdminActiveSecuritySettings(['-
activeUserRegistry','WIMUserRegistry','enableGlobalSecurity','true'])

print'# Step 07a: Set LDAP search filters for Groups'
AdminTask.addIdMgrLDAPEntityType(['-id',_ID_LABEL_,'-name','Group','-
objectClasses','groupOfNames','searchBases',_GROUP_OU_])
AdminTask.addIdMgrLDAPGroupDynamicMemberAttr(['-id',_ID_LABEL_,'-name',
'member','objectClass','dxDynamicGroupOfNames'])
AdminTask.addIdMgrLDAPGroupMemberAttr(['-id',_ID_LABEL_,'-name',
'member','dummyMember','uid=dummy','objectClass','groupOfNames'])
AdminTask.setIdMgrLDAPGroupConfig(['-id',_ID_LABEL_,'-name','member','-
scope','direct','updateGroupMembership','true'])

print'# Step 07b: Set LDAP search filters for OrgUnits'
AdminTask.addIdMgrLDAPEntityType(['-id',_ID_LABEL_,'-name','OrgContainer','-
objectClasses','organization','searchBases',_BASE_OU_])
AdminTask.addIdMgrLDAPEntityTypeRDNAttr(['-id',_ID_LABEL_,'-
entityTypeName','OrgContainer','name','objectClass','organization'])
AdminTask.addIdMgrLDAPEntityTypeRDNAttr(['-id',_ID_LABEL_,'-
entityTypeName','OrgContainer','name','ou','objectClass','organizationalUnit'])
AdminTask.addIdMgrLDAPEntityTypeRDNAttr(['-id',_ID_LABEL_,'-
entityTypeName','OrgContainer','name','dc','objectClass','domain'])
#AdminTask.addIdMgrLDAPEntityTypeRDNAttr(['-id',_ID_LABEL_,'-
entityTypeName','OrgContainer','name','cn','objectClass','container'])
AdminTask.updateIdMgrLDAPEntityType(['-id',_ID_LABEL_,'-
name','OrgContainer','objectClasses','organizationalUnit'])
AdminTask.updateIdMgrLDAPEntityType(['-id',_ID_LABEL_,'-
name','OrgContainer','objectClasses','domain'])
#AdminTask.updateIdMgrLDAPEntityType(['-id',_ID_LABEL_,'-
name','OrgContainer','objectClasses','container'])
config.html
```

```
print'# Step 07c: Set LDAP search filters for Users/People'
AdminTask.addIdMgrLDAPEntityType(['-id',_ID_LABEL_,'-name','PersonAccount','-
objectClasses','PEOPLE_OBJECTCLASS','searchBases',_PEOPLE_OU_])

print'# Step 07d: Update LDAP Attributes for Repository'
AdminTask.addIdMgrLDAPAttr(['-id',_ID_LABEL_,'-name','userPassword','-
propertyName','password','entityTypes','PersonAccount'])

print'# Step 07e: Update LDAP Context Pool / Configurations for Repository'
AdminTask.setIdMgrLDAPContextPool(['-id',_ID_LABEL_,'enabled','true','initPoolSize','1','-
maxPoolSize','0','poolTimeOut','0','poolWaitTime','3000','prefPoolSize','3'])
AdminTask.setIdMgrLDAPAttrCache(['-id',_ID_LABEL_,'attributeSizeLimit','2000','-
cacheSize','4000','cacheTimeOut','1200','enabled','true'])
#AdminTask.setIdMgrLDAPAttrCache(['-id',_ID_LABEL_,'attributeSizeLimit','2000','-
cacheSize','4000','cacheTimeOut','1200','enabled','true','cacheDistPolicy','none','-
cachesDiskOffLoad','false'])
AdminTask.setIdMgrLDAPSearchResultCache(['-id',_ID_LABEL_,'cacheSize','2000','-
cacheTimeOut','600','enabled','true','searchResultSizeLimit','1000'])

print'# Step 08: Update default Realm to Login if userstore is down'
# Fed Repository CheckBox "Allow operations if some of the repositories are down"
AdminTask.updateIdMgrRealm(['-name defaultWIMFileBasedRealm -allowOperationIfReposDown true'])

print'# Step 09: Save changes'
AdminConfig.save()

print'# Step 10: Clear WSA Auth Cache - All'
AdminTask.clearIdMgrRepositoryCache()

print'# Step 11: Validate Person / Group objects defined'
AdminTask.getIdMgrLDAPEntityType(['-id',_ID_LABEL_,'-name','PersonAccount'])
AdminTask.getIdMgrLDAPEntityType(['-id',_ID_LABEL_,'-name','Group'])

print'# Step 12: Validate changes'
AdminTask.listIdMgrRepositories()

# Note: Restart WAS Service to validate all changes
# Example: net stop "IBMWAS85Service - baual01w7Node01"
```

## Step 06b: Import Jython Script

```
Administrator: Command Prompt - wsadmin.bat -username wsadmin -password Password01 -lang jython -conntype SOAP
H:\wls2\AppServer\bin>wsadmin.bat -username wsadmin -password Password01 -lang jython -conntype SOAP
WASX7209I: Connected to process "server1" on node baual01w7Node01 using SOAP connector; The type of process is: UnManagedProcess
WASX7031I: For help, enter: "print Help.help()"
wsadmin>
```

**Interactively – Copy-n-Paste the script**  
Exception / Warning messages will not stop the script from completion

```
Administrator: Command Prompt
H:\wls2\AppServer\bin>wsadmin.bat -username wsadmin -password Password01 -lang jython -conntype SOAP -f C:\Users\Administrator\Desktop\clients\nfcu\CLI_wsadmin_new_LDAP\Steps_to_add_custom_LDAP_v14.py.txt
```

**Input File Method**  
Note: Comment out section 3a to avoid exception messages (see below)

To-Do: Add in try/except functionality to continue after exception occurs

```
# Step 03a: Remove LDAP Server Place Holder
WASX7017E: Exception received while running file "C:\Users\Administrator\Desktop\clients\nfcu\CLI_wsadmin_new_LDAP\Steps_to_add_custom_LDAP_v12.py.txt"; exception information: com.ibm.websphere.wim.exception.WIMConfigurationException: com.ibm.websphere.wim.exception.WIMConfigurationException: CWIWIM5025E Base entry ou=cam,o=ca is not found in the defaultWIMFfileBasedRealm realm.
```

## Step 06c: Compare wimconfig.xml after incremental updates to reach final state

Location Pane

```

H:\wls2\AppServer\profiles\AppSrv01\config\cells\baual01w7Node01Cell\wim\config\wimconfig.xml
<config:repositories xsi:type="config:FileRepositoryType" adaj
    id="InternalFileRepository" supportPaging="false" message
    <config:baseEntries name="o=defaultWIMFileBasedRealm"/>
</config:repositories>
<config:repositories xsi:type="config:LdapRepositoryType" adaj
    id="CA_Directory" isExtIdUnique="true" supportAsyncMode=":
    supportPaging="false" supportSorting="false" supportTrans
    certificateFilter="" certificateMapMode="exactdn" ldapSer
    translateRDN="false">
    <config:baseEntries name="ou=cam,o=ca" nameInRepository="ou
    <config:loginProperties>uid</config:loginProperties>
    <config:ldapServerConfiguration primaryServerQueryTimeInter
        sslConfiguration="">
        <config:ldapServers authentication="simple" bindDN="cn=di
            bindPassword="{xor}Dz4sLCgwLTtvbg==" connectionPool=":
            derefAliases="always" referral="ignore" sslEnabled="fa
            <config:connections host="192.168.92.139" port="41389"/>
        </config:ldapServers>
    </config:ldapServerConfiguration>
    <config:ldapEntityTypes name="Group">
        <config:objectClasses>groupOfNames</config:objectClasses>
        <config:searchBases>ou=groups,ou=cam,o=ca</config:searchB
    </config:ldapEntityTypes>
    <config:ldapEntityTypes name="OrgContainer">
        <config:rdnAttributes name="o" objectClass="organization".
        <config:rdnAttributes name="ou" objectClass="organization"
        <config:rdnAttributes name="dc" objectClass="domain"/>
        <config:objectClasses>organization</config:objectClasses>
        <config:objectClasses>organizationalUnit</config:objectCl
        <config:objectClasses>domain</config:objectClasses>
        <config:searchBases>ou=cam,o=ca</config:searchBases>
    </config:ldapEntityTypes>
    <config:ldapEntityTypes name="PersonAccount">
        <config:objectClasses>inetOrgPerson</config:objectClasses>
        <config:searchBases>ou=people,ou=cam,o=ca</config:searchB
    </config:ldapEntityTypes>
    <config:groupConfiguration updateGroupMembership="false">

```

H:\...er\profiles\AppSrv01\config\cells\baual01w7Node01Cell\wim\config\wimconfig-OOTB-Before\_any\_modification.xml

```

<config:repositories xsi:type="config:FileRepositoryType" adaj
    id="InternalFileRepository" supportPaging="false" message
    <config:baseEntries name="o=defaultWIMFileBasedRealm"/>
</config:repositories>

```

Ready

Ln: 48 Col: 1/92 Ch: 1/92      1252      Win      Line: 37-38      1252      Win

3 Differences Found      NUM

## Step 06d: Bounce NT Services to clear WAS cache

Server	Name	Description	Status	Startup Type	Log On As
	Hyper-V Remote Desktop Virtualization Service	Provides a p...	Manual (Trig...	Local Syste...	
	Hyper-V Time Synchronization Service	Synchronize...	Manual (Trig...	Local Service	
	Hyper-V Volume Shadow Copy Requestor	Coordinates...	Manual (Trig...	Local Syste...	
	IBM WebSphere Application Server V8.5 - baual01w7Node01	Controls th...	Running	Manual	Local Syste...
	IKE and AuthIP IPsec Keying Modules	The IKEEXT ...		Manual (Trig...	Local Syste...
	InstallDriver Table Manager	Provides su...		Manual	Local Syste...
8.5	Service Control	<span style="color: red;">X</span>			
		Windows is attempting to start the following service on Local Computer...			
	IBM WebSphere Application Server V8.5 - baual01w7Node01	el(R) Con...	Running	Manual	Local Syste...
		el(R) Inte...	Running	Automatic	Local Syste...
		e Intel(R) ...	Running	Automatic	Local Syste...
		nages th...	Running	Automatic	Local Syste...
		vides re...	Running	Automatic	Local Syste...
		nages th...	Running	Automatic	Local Syste...
		vides sto...	Running	Automatic (D...	Local Syste...
		ibles use...		Manual	Local Syste...
		vides ne...		Manual	Local Syste...
	Internet Explorer ETW Collector Service	ETW Collect...		Manual	Local Syste...

# Step 07: WAS Federated Repositories: After State

The image shows two screenshots of the WebSphere Integrated Solutions Console. The left screenshot displays the login interface with fields for User ID (wsadmin) and Password, and a Log in button. The right screenshot shows the 'Global security' configuration page under the 'Administrative security' tab. It includes sections for 'Administrative security' (with checked boxes for 'Enable administrative security' and 'Administrative user roles', and uncheckable options for 'Administrative group roles' and 'Administrative authentication'), 'Application security' (unchecked), 'Java 2 security' (unchecked), and 'User account repository' (set to 'Federated repositories'). The right side of the page also lists 'Authentication' mechanisms (LTPA, Kerberos and LTPA, SWAM), 'Web and SIP security', 'RMI/IOP security', 'Java Authentication and Authorization Service', and 'Custom properties'. Navigation links like 'Security Configuration Wizard' and 'Security Configuration Report' are also visible.

WebSphere Integrated Solutions Console

User ID: wsadmin  
Password:   
Log in

Licensed Materials - Property of IBM (c) Copyright IBM Corp. 1997, 2011 All Rights Reserved.  
IBM, the IBM logo, ibm.com and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at [Copyright and trademark information](#).

Cell=baau01w7Node01Cell, Profile=AppSrv01

Welcome wsadmin Help | Logout IBM. Close page

Global security

Global security

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.

Security Configuration Wizard    Security Configuration Report

Administrative security

Enable administrative security    [Administrative user roles](#)  
 [Administrative group roles](#)  
 [Administrative authentication](#)

Application security

Enable application security

Java 2 security

Use Java 2 security to restrict application access to local resources  
 Warn if applications are granted custom permissions  
 Restrict access to resource authentication data

User account repository

Realm name: defaultWIMFileBasedRealm  
Current realm definition: Federated repositories  
Available realm definitions: Federated repositories ▾ [Configure...](#) [Set as current](#)

Authentication

Authentication mechanisms and expiration

LTPA  
 Kerberos and LTPA  
[Kerberos configuration](#)  
 SWAM (deprecated): No authenticated communication between servers  
[Authentication cache settings](#)

Web and SIP security  
 RMI/IOP security  
 Java Authentication and Authorization Service  
 Enable Java Authentication SPI (JASPI) Providers  
 Use realm-qualified user names

[Security domains](#)  
[External authorization providers](#)  
[Programmatic session cookie configuration](#)  
[Custom properties](#)

Apply    Reset

# Step 08a: View WAS Federated Repositories

Guided Activities

Servers

Applications

Services

Resources

Security

- Global security
- Security domains
- Administrative Authorization Groups
- SSL certificate and key management
- Security auditing
- Bus security

Environment

System administration

Users and Groups

Monitoring and Tuning

Troubleshooting

Service integration

UDDI

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm can consist of identities in the file-based repository that is built into the system, in one or more external repositories, or in both the built-in repository and one or more external repositories.

**General Properties**

\* Realm name  
defaultWIMFileBasedRealm

\* Primary administrative user name  
wsadmin

**Server user identity**

Automatically generated server identity

Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node

Password

Ignore case for authorization

Allow operations if some of the repositories are down

**Repositories in the realm:**

Add repositories (LDAP, custom, etc)... Use built-in repository Remove

Select	Base Entry	Repository Identifier	Repository Type
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File
<input type="checkbox"/>	ou=cam,o=ca	CA_Directory	LDAP: CUSTOM

Total 2

**Related Items**

Additional Properties

- Property extension repository
- Entry mapping repository
- Supported entity types
- User repository attribute mapping
- Custom properties

Manage repositories

Trusted authentication realms - inbound

Apply OK Reset Cancel

Note: Two (2) items:

1. CA Directory is listed as a Federated Repository and Type=CUSTOM
2. Check Box for “Allow operations if some of the repositories are down, enabled=true

# Step 08b: View WAS Federated Repositories

Specifies the configuration for secure access to a Lightweight Directory Access Protocol (LDAP) repository with optional failover servers.

**General Properties**

\* Repository identifier: CA\_Directory

Repository adapter class name: com.ibm.ws.wim.adapter.Idap.LdapAdapter

**LDAP server**

- \* Directory type: Custom
- \* Primary host name: 192.168.92.139 Port: 41389
- Failover server used when primary is not available:
  - Delete
  - Select: Failover Host Name: Port: None
  - Add: [ ] [ ]
- Support referrals to other LDAP servers: ignore
- Support for repository change tracking: none
- Custom properties:
  - New
  - Delete
  - Select

Name	Value
[ ]	[ ]

**Additional Properties**

- Performance
- Federated repositories entity types to LDAP object classes mapping
- Federated repositories property names to LDAP attributes mapping
- Group attribute definition

Buttons: Apply | OK | Reset | Cancel

For field 1  
select a fi  
marker w/  
is displayed

Page helpe  
Mo  
pad  
Co  
View  
con

Note: Eight (8) items:

1. Label = CA\_Directory
2. Using standard OOTB IBM Ildap adapter. Do not change.
3. Directory Type = Custom
4. Hostname = CA Directory hostname/IP
5. Port = CA Directory DSA Port
6. Bind DN = CA Directory DSA Bind DN with Password
7. Login Attribute = uid
  1. May be changed
8. Certificate Mapping = EXACT\_DN

# Step 08c: View WAS Federated Repositories

WebSphere software

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
- Security
  - Global security
  - Security domains
  - Administrative Authorization Groups
  - SSL certificate and key management
  - Security auditing
  - Bus security
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Cell=bauai01vr7Node01Cell, Profile=AppSrv01

## Global security

Global security > Federated repositories > CA Directory > Group attribute definition

Use this page to specify the name of the group membership attribute. Every Lightweight Directory Access Protocol (LDAP) entry includes this attribute to indicate the groups to which this entry belongs.

**General Properties**

Name of group membership attribute  
member

**Scope of group membership attribute**

Direct - Contains only immediate members of the group without members of subgroups  
 Nested - Contains direct members and members nested within subgroups of this group  
 All - Contains all direct, nested, and dynamic members

Apply OK Reset Cancel

**Important Note:**  
Not Shown in the UI but the flag updateGroupMembership must be set to true for LDAP servers if using CLI to allow groups to be viewed. Alternatively, this entry may be left blank; similar to the DOMINO configuration.

Welcome wsadmin

Help | Logout

IBM. Close page

Help

Field help  
For field help information, select a field label or list marker when the help cursor is displayed.

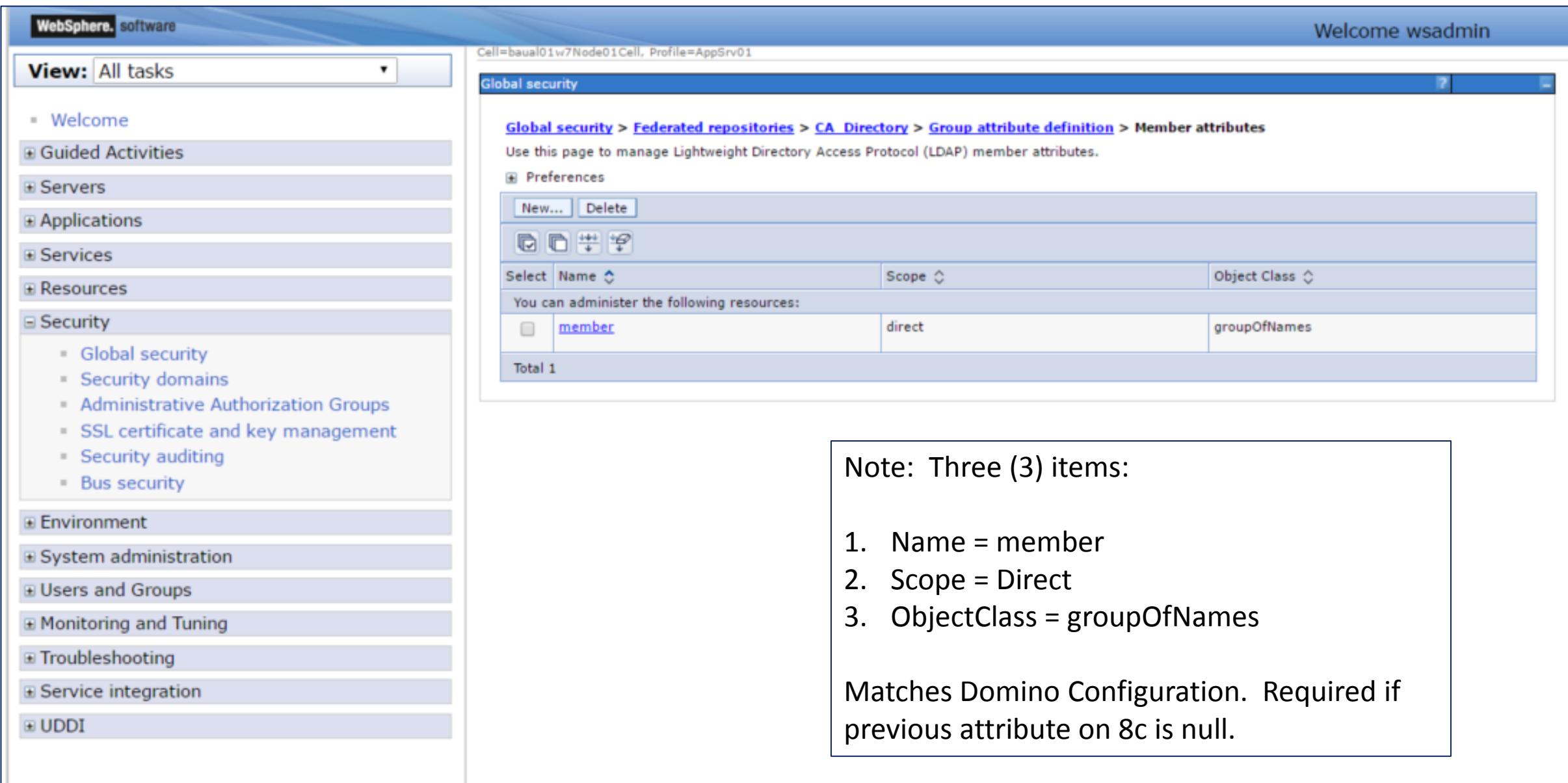
Page help  
More information about this page

Command Assistance  
View administrative scripting command for last action

Note: Two (2) items:

- Attribute = member
- Scope = Direct
  - Since CA Directory Dynamic group membership uses the same attribute. No delta was noticed between "Direct" versus "All"

# Step 08d: View WAS Federated Repositories



The screenshot shows the WebSphere Application Server Administration Console interface. The left sidebar menu is visible, showing various management categories like Guided Activities, Servers, Applications, Services, Resources, Security, Environment, System administration, Users and Groups, Monitoring and Tuning, Troubleshooting, Service integration, and UDDI. The 'View' dropdown at the top is set to 'All tasks'. The main content area is titled 'Global security' and displays the path: Global security > Federated repositories > CA Directory > Group attribute definition > Member attributes. It states: 'Use this page to manage Lightweight Directory Access Protocol (LDAP) member attributes.' A table lists one resource: member (Name), direct (Scope), and groupOfNames (Object Class). A note box on the right side contains the following text:

Note: Three (3) items:

1. Name = member
2. Scope = Direct
3. ObjectClass = groupOfNames

Matches Domino Configuration. Required if previous attribute on 8c is null.

# Step 08e: View WAS Federated Repositories

The screenshot shows the WebSphere Application Server Administration Console interface. The left sidebar menu is visible with various navigation options like Welcome, Guided Activities, Servers, Applications, Services, Resources, Security, Environment, System administration, Users and Groups, Monitoring and Tuning, Troubleshooting, Service integration, and UDDI. The main content area is titled "Global security" and shows the path: Global security > Federated repositories > CA\_Directory > Group attribute definition > Dynamic member attributes. It provides a description: "Use this page to manage Lightweight Directory Access Protocol (LDAP) dynamic member attributes." Below this, there is a table with one item:

Select	Name	Object Class
<input type="checkbox"/>	<a href="#">member</a>	dxDynamicGroupOfNames

Total 1

Note: Two (2) items:

1. Name = member
2. ObjectClass = dxDynamicGroupOfNames
  1. No delta was observed with or within this enabled for use-case of viewing members of a dynamic group. For consistency this object was retained.

# Step 08f: View WAS Federated Repositories

WebSphere software Welcome wsadmin

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
- Security
  - Global security
  - Security domains
  - Administrative Authorization Groups
  - SSL certificate and key management
  - Security auditing
  - Bus security
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Cell=bau01w7Node01Cell, Profile=AppSrv01

Global security

Global security > Federated repositories > CA Directory > Federated repositories property names to LDAP attributes mapping

Use this panel to specify supported, unsupported, and external LDAP attributes.

Preferences

Add Delete

Select Name/Property Name Type

You can administer the following resources:

	Name/Property Name	Type
<input type="checkbox"/>	userPassword	Supported

Total 1

Note: Two (2) items:

1. Name = userPassword
2. Type = Supported
  1. Did not retain the “UnSupported Type” from “Domino pre-defined configuration” No obvious value during testing.

# Step 08g: View WAS Federated Repositories

The screenshot shows the WebSphere Application Server Administration Console interface. The left sidebar menu includes 'View: All tasks' and categories like 'Welcome', 'Guided Activities', 'Servers', 'Applications', 'Services', 'Resources', 'Security' (which is expanded to show 'Global security', 'Security domains', 'Administrative Authorization Groups', 'SSL certificate and key management', 'Security auditing', and 'Bus security'), 'Environment', 'System administration', 'Users and Groups', 'Monitoring and Tuning', 'Troubleshooting', 'Service integration', and 'UDDI'. The main content area is titled 'Global security' and shows the path 'Global security > Federated repositories > CA Directory > Federated repositories entity types to LDAP object classes mapping'. It displays a table of entity types and their corresponding LDAP object classes:

Select	Entity Type	Object Classes
<input type="checkbox"/>	<a href="#">Group</a>	groupOfNames
<input type="checkbox"/>	<a href="#">OrgContainer</a>	organization;organizationalUnit;domain
<input type="checkbox"/>	<a href="#">PersonAccount</a>	inetOrgPerson

Total 3

Note: Three (3) items:

1. Kept all three defaults with objectClasses that match CA Directory schema for the DSA.

# Step 08h: View WAS Federated Repositories

WebSphere software

Welcome wsadmin

Cell=baual01w7Node01Cell, Profile=AppSrv01

Global security

Global security > Federated repositories > CA Directory > SSL configurations > NodeDefaultSSLSettings

Defines a list of Secure Sockets Layer (SSL) configurations.

General Properties

Name: NodeDefaultSSLSettings

Trust store name: NodeDefaultTrustStore ((cell):baual01w7Node01Cell:(node):baual01w7Node01)

Keystore name: NodeDefaultKeyStore ((cell):baual01w7Node01Cell:(node):baual01w7Node01)

Default server certificate alias: (none)

Default client certificate alias: (none)

Management scope: (cell):baual01w7Node01Cell:(node):baual01w7Node01

Additional Properties

- Quality of protection (QoP) settings
- Trust and key managers
- Custom properties

Related Items

- Key stores and certificates

Apply OK Reset Cancel

Note: No SSL Enabled for Repository. To be done later.

Showing default settings.

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
- Security
  - Global security
  - Security domains
  - Administrative Authorization Groups
  - SSL certificate and key management
  - Security auditing
  - Bus security
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

# Step 08i: View WAS Federated Repositories

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
- Security
  - Global security
  - Security domains
  - Administrative Authorization Groups
  - SSL certificate and key management
  - Security auditing
  - Bus security
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Global security

Global security > Federated repositories > CA\_Directory > Performance

Opening new network connections to the LDAP server, establishing a new JNDI context, or accessing the LDAP server over the network might impact performance. Initialization impacts to performance are minimized by adding opened connections and contexts to internally maintained pools and reusing them. Minimize the impact to performance by maintaining internal caches of retrieved data.

General Properties

Limit search time  milliseconds

Limit search returns  entries

Connect timeout  20 seconds

Use connection pooling

Enable context pool

Initial size <input type="text"/> 1 Entries	Preferred size <input type="text"/> 3 Entries	Maximum size <input type="text"/> 0 Entries
<input type="checkbox"/> Context pool times out <input type="text"/> Seconds		

Caches

Cache the attributes

Cache size  
 4000 Entries

Cache times out  1200 Seconds

Distribution policy  
Push

Cache the search results

Cache size  
 2000 Entries

Cache times out  600 Seconds

Distribution policy  
Push

Note: Default Settings

Apply OK Reset Cancel

# Step 09a: Validate Use-Case for Users Lookup

JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

Explore Results Schema

World ca cam groups group01 group02 group03 people bugsbunny daffyduck test001 test002 serviceaccount diradmin idmadmin idmembedded idmfeed idminbound idmpublic views

attribute type	value
cn	bugsbunny
objectClass	camUser
objectClass	inetOrgPerson
objectClass	organizationalPerson
objectClass	person
objectClass	top
sn	bunny
uid	bugsbunny
audio	
businessCategory	
camAccessRoles	
camActivationDate	
camActivationId	
camAdminRoles	
camArcotStatus	
camBinary00	
camBinary01	
camCertificate00	
camCertificate01	

Administrative Authorization Groups  
SSL certificate and key management  
Security auditing  
Bus security

+ Environment  
+ System administration  
Users and Groups  
Administrative user roles  
Administrative group roles  
Manage Users  
Manage Groups

People Search OU limited to ou=people,ou=cam,o=ca  
No service account will be displayed.

Welcome wsadmin

Manage Users

Search for Users

Search by \* Search for \* Maximum results User ID 100

Search

5 users matched the search criteria.

Select	User ID	First name	Last name	E-mail	Unique Name
<input type="checkbox"/>	bugsbunny	bugsbunny	bunny		cn=bugsbunny,ou=people,ou=cam,o=ca
<input type="checkbox"/>	daffyduck	daffyduck	duck		cn=daffyduck,ou=people,ou=cam,o=ca
<input type="checkbox"/>	test001	test001	test001		cn=test001,ou=people,ou=cam,o=ca
<input type="checkbox"/>	test002	test002	test002		cn=test002,ou=people,ou=cam,o=ca
<input type="checkbox"/>	wsadmin	wsadmin	wsadmin		uid=wsadmin,o=defaultWIMFileBasedRealm

Page 1 of 1 Total: 5

# Step 09b: Validate Use-Case for Users Lookup

Manage Users

Manage Users

User Properties

General Groups

+ User ID  
bugsbunny

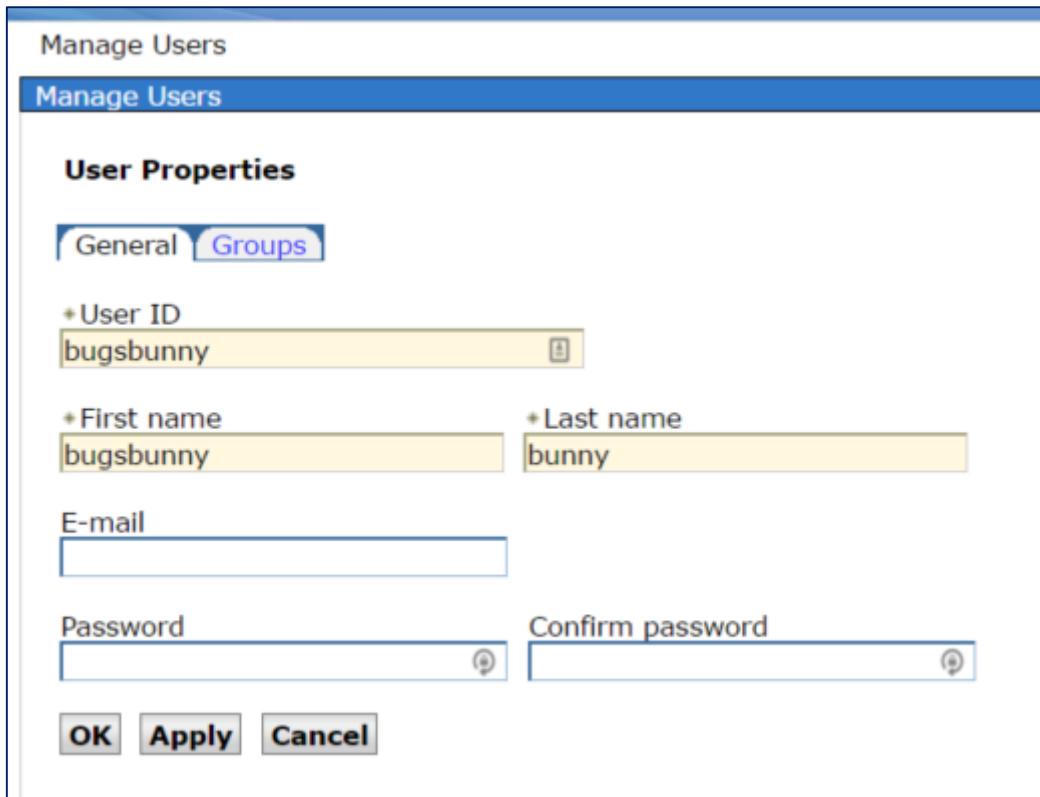
+ First name  
bugsbunny

+ Last name  
bunny

E-mail

Password  
 Confirm password

OK Apply Cancel



This screenshot shows the 'User Properties' dialog. It has tabs for 'General' and 'Groups'. The 'General' tab is active, displaying fields for User ID ('bugsbunny'), First name ('bugsbunny'), Last name ('bunny'), E-mail (empty), Password (empty), and Confirm password (empty). At the bottom are OK, Apply, and Cancel buttons.

Manage Users

Manage Users

User Properties

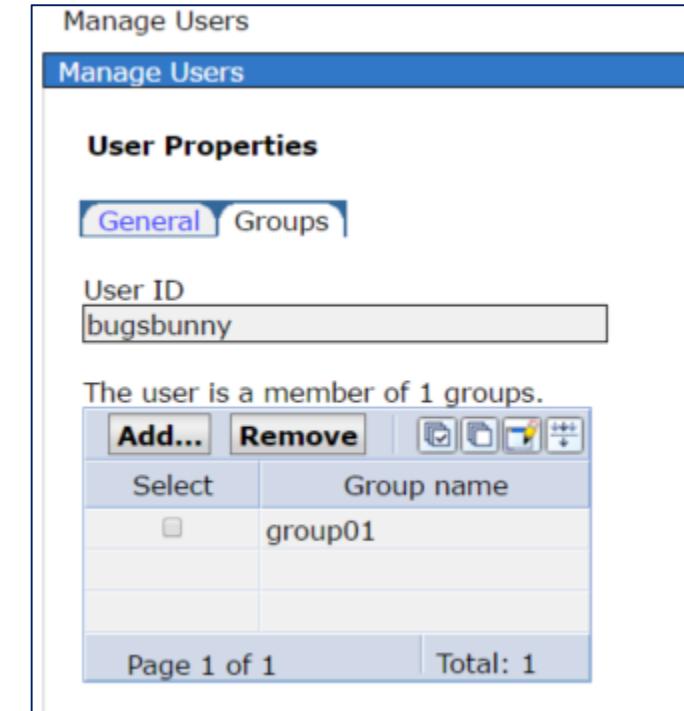
General Groups

User ID  
bugsbunny

The user is a member of 1 groups.

Select	Group name
<input type="checkbox"/>	group01

Page 1 of 1 Total: 1



This screenshot shows the 'User Properties' dialog with the 'Groups' tab selected. It displays the user ID ('bugsbunny') and a message stating 'The user is a member of 1 groups.' Below this is a table showing one group entry: 'group01'. At the bottom, it shows 'Page 1 of 1' and 'Total: 1'.

# Step 09c: Validate Use-Case for Users Lookup

Manage Users

Manage Users

**Add a User to Groups**

User ID  
bugsbunny

Specify the search criteria that you want to use to find the groups that you want this user to be a member of.

Search by \*Search for \*Maximum results

Group name \* 100

**Search**

3 groups matched the search criteria.

group01  
group02  
group03

**Add** **Close**

Manage Users

Manage Users

**Add a User to Groups**

The user was added to the groups successfully.

User ID  
bugsbunny

Specify the search criteria that you want to use to find the groups that you want this user to be a member of.

Search by \*Search for \*Maximum results

Group name \* 100

**Search**

3 groups matched the search criteria.

group01  
group03

**User Properties**

**General** **Groups**

User ID  
bugsbunny

The user is a member of 2 groups.

Select	Group name
<input type="checkbox"/>	group01
<input type="checkbox"/>	group02

Page 1 of 1 Total: 2

# Step 10a: Validate Use-Case for Group Lookup

The image displays two JXplorer interfaces, each showing the structure of an LDAP directory and a table editor for viewing attribute values.

**JXplorer - imcd-ca**

**World** tree:

- ca
  - cam
    - groups
      - group01
      - group02
      - group03
    - people
      - bugsbunny
      - daffyduck
    - test001
    - test002
  - serviceaccount
    - diradmin
    - idmadmin
    - idmembedded
    - idmfeed
    - idminbound
    - idmpublic
  - views

**Table Editor** (attribute type, value)

attribute type	value
cn	group01
dxMemberURL	ldap:///ou=cam,o=ca??sub?(uid=test001)
objectClass	dxDynamicGroupOfNames
objectClass	top
objectClass	groupOfNames
description	group01 description from websphere
member	cn=TEST1,ou=PEOPLE,ou=CAM,o=CA
member	cn=test002,ou=people,ou=cam,o=ca
member	cn=bugsbunny,ou=people,ou=cam,o=ca
member	cn=test001,ou=people,ou=cam,o=ca
businessCategory	
dxExcludeMember	
o	
ou	
owner	
seeAlso	

**JXplorer - imcd-on-npm01**

**World** tree:

  - ca
    - cam
      - groups
        - group01
        - group02
        - group03
      - people
        - bugsbunny
        - daffyduck
      - test001
      - test002
    - serviceaccount
      - diradmin
      - idmadmin
      - idmembedded
      - idmfeed
      - idminbound
      - idmpublic
    - views

**Table Editor** (attribute type, value)

attribute type	value
cn	group02
dxMemberURL	ldap:///ou=cam,o=ca??sub?(&(objectClass=person)(cn=idm*))
objectClass	dxDynamicGroupOfNames
objectClass	top
objectClass	groupOfNames
member	cn=TEST1,ou=PEOPLE,ou=CAM,o=CA
member	cn=daffyduck,ou=people,ou=cam,o=ca
member	cn=BUGSBUNNY,ou=PEOPLE,ou=CAM,o=CA
member	cn=idmadmin,ou=serviceaccount,ou=cam,o=ca
member	cn=idmembedded,ou=serviceaccount,ou=cam,o=ca
member	cn=idmfeed,ou=serviceaccount,ou=cam,o=ca
member	cn=idminbound,ou=serviceaccount,ou=cam,o=ca
member	cn=idmpublic,ou=serviceaccount,ou=cam,o=ca
businessCategory	
description	
dxExcludeMember	
o	
ou	
owner	

# Step 10b: Validate Use-Case for Group Lookup

WebSphere software

Welcome wsad

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
- Security
  - Global security
  - Security domains
  - Administrative Authorization Groups
  - SSL certificate and key management
  - Security auditing
  - Bus security
- Environment
- System administration
- Users and Groups
  - Administrative user roles
  - Administrative group roles
  - Manage Users
  - Manage Groups

Manage Groups

Manage Groups

Search for Groups

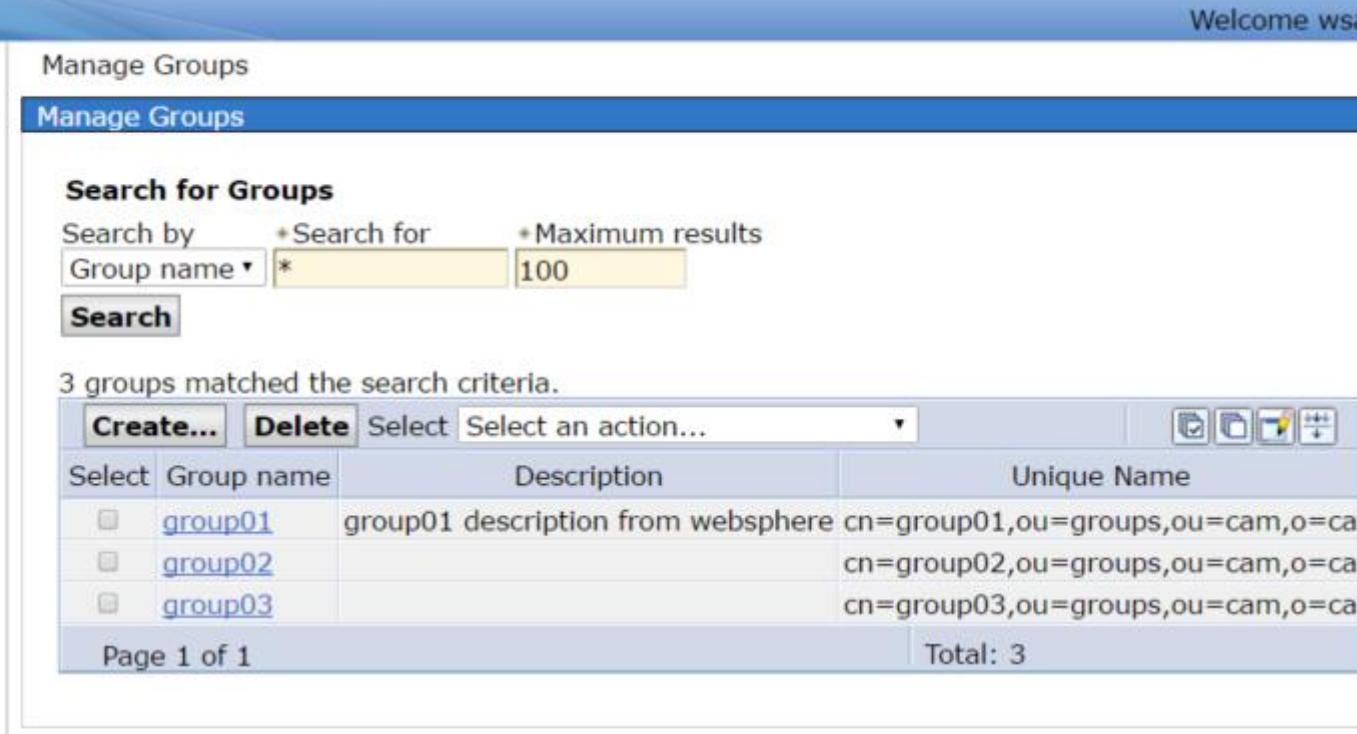
Search by \* Search for \* Maximum results  
Group name \* 100

Search

3 groups matched the search criteria.

Select	Group name	Description	Unique Name
<input type="checkbox"/>	group01	group01 description from websphere cn=group01,ou=groups,ou=cam,o=ca	cn=group01,ou=groups,ou=cam,o=ca
<input type="checkbox"/>	group02		cn=group02,ou=groups,ou=cam,o=ca
<input type="checkbox"/>	group03		cn=group03,ou=groups,ou=cam,o=ca

Page 1 of 1 Total: 3



# Step 10c: Validate Use-Case for Group Lookup

Manage Groups

Manage Groups

**Group Properties**

General Members Groups

\* Group name  
group01

Description  
group01 description from websphere

Manage Groups

Manage Groups

**Group Properties**

General Members Groups

Group name  
group01

The group has 3 members.

Add Users... Add Groups... Remove

Select	ID	Type	Unique Name
<input type="checkbox"/>	bugs bunny		cn=bugs bunny,ou=people,ou=cam,o=ca
<input type="checkbox"/>	test001		cn=test001,ou=people,ou=cam,o=ca
<input type="checkbox"/>	test002		cn=test002,ou=people,ou=cam,o=ca

Page 1 of 1 Total: 3

Note: Groups includes both STATIC and Dynamic Members

When WAS adds a STATIC member to a GROUP, the objects are replaced with UPPER CASE syntax.

WAS does not require the static member to be in UPPER CASE to view or manage.  
Likely legacy behavior.

WAS does check if the Group member does exist. Any account that is listed as a member but with no UID, will not be displayed.

Manage Groups

Manage Groups

**Group Properties**

General Members Groups

\* Group name  
group02

Description

Manage Groups

Manage Groups

**Group Properties**

General Members Groups

Group name  
group02

The group has 7 members.

Add Users... Add Groups... Remove

Select	ID	Type	Unique Name
<input type="checkbox"/>	bugs bunny		cn=BUGSBUNNY,ou=PEOPLE,ou=CAM,o=CA
<input type="checkbox"/>	daffy duck		cn=daffy duck,ou=people,ou=cam,o=ca
<input type="checkbox"/>	idm admin		cn=idm admin,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	idm embedded		cn=idm embedded,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	idm feed		cn=idm feed,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	idm in bound		cn=idm in bound,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	idm public		cn=idm public,ou=serviceaccount,ou=cam,o=ca

Page 1 of 1 Total: 7

# View Deltas – Between Working Domino vs Custom Type

[Global security > Federated repositories > CA\\_Directory](#)  
Specifies the configuration for secure access to a Lightweight Directory Access Protocol (LDAP) repository with optional failover support.

**General Properties**

**Repository identifier**  
CA\_Directory

**Repository adapter class name**  
com.ibm.ws.wim.adapter.ldap.LdapAdapter

**LDAP server**

\* **Directory type**: IBM Lotus Domino

\* **Primary host name**: 192.168.92.139    **Port**: 41389

**Failover server used when primary is not available:**

**Select** Failover Host Name    Port

**None**

**Add**

**Support referrals to other LDAP servers**: ignore

**Support for repository change tracking**: none

**Custom properties**

New    Delete

Select	Name	Value
<input type="checkbox"/>		

## Note:

Domino pre-defined template does NOT populate the EDIT box under “Group attribute definition” Edit box.

However, it does populate the “Group attribute definition/Member attribute” section with name/scope/objectClass

[Global security > Federated repositories > CA\\_Directory > Group attribute definition](#)  
Use this page to specify the name of the group membership attribute. Every Lightweight Directory Access Protocol (LDAP) entry includes this attribute to indicate the groups to which this entry belongs.

**General Properties**

Name of group membership attribute:

**Additional Properties**

- = Member attributes
- = Dynamic member attributes

**Scope of group membership attribute**

- Direct - Contains only immediate members of the group without members of subgroups
- Nested - Contains direct members and members nested within subgroups of this group
- All - Contains all direct, nested, and dynamic members

[Global security > Federated repositories > CA\\_Directory > Group attribute definition > Member attributes](#)  
Use this page to manage Lightweight Directory Access Protocol (LDAP) member attributes.

**Preferences**

New...    Delete

Select	Name	Scope	Object Class
<input type="checkbox"/>	member	direct	groupOfNames

Total 1

[Global security > Federated repositories > CA\\_Directory > Group attribute definition > Dynamic member attributes](#)  
Use this page to manage Lightweight Directory Access Protocol (LDAP) dynamic member attributes.

**Preferences**

New...    Delete

Select	Name	Object Class
	None	

Total 0

# View Deltas – Between Working Domino vs Custom Type

**Search for Users**

Search by \*Search for \*Maximum results  
User ID \* 100

**Search**

11 users matched the search criteria.

Select	User ID	First name	Last name	E-mail	Unique Name
<input type="checkbox"/>	<a href="#">bugs bunny</a>	bugs bunny	bunny		cn=bugs bunny,ou=people,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">daffy duck</a>	daffy duck	duck		cn=daffy duck,ou=people,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">dir admin</a>	dir admin	dir admin		cn=dir admin,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">idm admin</a>	idm admin	idm admin		cn=idm admin,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">idm embedded</a>	idm embedded	idm embedded		cn=idm embedded,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">idm feed</a>	idm feed	idm feed		cn=idm feed,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">idm in bound</a>	idm in bound	idm in bound		cn=idm in bound,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">idm public</a>	idm public	idm public		cn=idm public,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">test 001</a>	test 001	test 001		cn=test 001,ou=people,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">test 002</a>	test 002	test 002		cn=test 002,ou=people,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">ws admin</a>	ws admin	ws admin		uid=ws admin,o=defaultWIMFileBasedRealm

Page 1 of 1 Total: 11

## Note:

Domino pre-defined template uses the base OU to search for users & groups. Even the service accounts are on display.

This template will also display the CA Directory static and dynamic group memberships; with no dynamic configuration set.

**Manage Groups**

**Group Properties**

**General** Members Groups

Group name  
group01

The group has 3 members.

Select	ID	Type	Unique Name
<input type="checkbox"/>	<a href="#">bugs bunny</a>		cn=bugs bunny,ou=people,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">test 001</a>		cn=test 001,ou=people,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">test 002</a>		cn=test 002,ou=people,ou=cam,o=ca

Page 1 of 1 Total: 3

**Manage Groups**

**Group Properties**

**General** Members Groups

Group name  
group02

The group has 7 members.

Select	ID	Type	Unique Name
<input type="checkbox"/>	<a href="#">BUGSBUNNY</a>		cn=BUGSBUNNY,ou=PEOPLE,ou=CAM,o=CA
<input type="checkbox"/>	<a href="#">daffy duck</a>		cn=daffy duck,ou=people,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">idm admin</a>		cn=idm admin,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">idm embedded</a>		cn=idm embedded,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">idm feed</a>		cn=idm feed,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">idm in bound</a>		cn=idm in bound,ou=serviceaccount,ou=cam,o=ca
<input type="checkbox"/>	<a href="#">idm public</a>		cn=idm public,ou=serviceaccount,ou=cam,o=ca

Page 1 of 1 Total: 7

**CUSTOM TYPE**

```

<ies name="o=defaultW
ies>
<es xsi:type="config:>
ry" isExtIdUnique="true" supportAsynMode="false" supportExternalName="false" supportSorting="false" supportTransactions="false" supportChar
ter="" certificateMapMode="exactdn" ldapServerType="CUSTOM"
false">
ies name="ou=cam,o=ca" nameInRepository="ou=cam,o=ca"/>
properties>uid</config:loginProperties>
erConfiguration primaryServerQueryTimeInterval="15" returnToPrimarySe
tion="">
rvers authentication="simple" bindDN="cn=diradmin,ou=serviceaccount,oi
rd="{xor}Dz4sLCgwLTtvbg==" connectionPool="false" connectTimeout="20"
es="always" referral="ignore" sslEnabled="false">
ections host="192.168.92.139" port="41389"/>
ervers>
verConfiguration>
tyTypes name="Group">
Classes>groupOfNames</config:objectClasses>
Bases>ou=groups,ou=cam,o=ca</config:searchBases>
ityTypes>
tyTypes name="OrgContainer">
ributes name="o" objectClass="organization"/>
ributes name="ou" objectClass="organizationalUnit"/>
ributes name="dc" objectClass="domain"/>
Classes>organization</config:objectClasse
Classes>organizationalUnit</config:object
Classes>domain</config:objectClasses>
Bases>ou=cam,o=ca</config:searchBases>
ityTypes>
tyTypes name="PersonAccount">
Classes>inetOrgPerson</config:objectCl
Bases>ou=people,ou=cam,o=ca</config:searchBases>
ityTypes>
figuration updateGroupMembership="true">
<+tributes dummyMember="uid=dummy" name="member" objectClass="groupOf
<

```

**DOMINO TYPE**

```

<ies name="o=defaultWIM
ies>
<es xsi:type="config:Ld
ry" isExtIdUnique="true" supportAsynMode="false" supportExternalName="false" supportSorting="false" supportTransactions="false" supportChar
ter="" certificateMapMode="exactdn" ldapServerType="DOMINO"
false">
ies name="ou=cam,o=ca" nameInRepository="ou=cam,o=ca"/>
properties>uid</config:loginProperties>
erConfiguration primaryServerQueryTimeInterval="15" returnToPrimarySe
tion="">
rvers authentication="simple" bindDN="cn=diradmin,ou=serviceaccount,oi
rd="{xor}Dz4sLCgwLTtvbg==" connectionPool="false" connectTimeout="20"
es="always" referral="ignore" sslEnabled="false">
ections host="192.168.92.139" port="41389"/>
ervers>
verConfiguration>
tyTypes name="Group">
Classes>groupOfNames</config:objectClasses>
ityTypes>
tyTypes name="OrgContainer">
ributes name="o" objectClass="organization"/>
ributes name="ou" objectClass="organizationalUnit"/>
ributes name="dc" objectClass="domain"/>
Classes>organization</config:objectClasse
Classes>organizationalUnit</config:object
Classes>domain</config:objectClasses>
Classes>container</config:objectClasses>
ityTypes>
tyTypes name="PersonAccount">
Classes>inetOrgPerson</config:objectCl
ityTypes>
figuration>
<+tributes dummyMember="uid=dummy" name="member" objectClass="groupOf
<

```

**Filter Groups to Group OU**

**Filter OrgUnits to Base OU**

**Filter Users to People OU**

**Label**

**Delta Unable to add CN for OrgUnits via CLI  
- No impact to use-case testing**

**CUSTOM TYPE**

```

<config:rdnAttributes>organization"/>
<config:rdnAttributes>"organizationalUnit"/>
<config:rdnAttributes>"domain"/>

<config:objectClasses>organization</config:objectClasses>
<config:objectClasses>organizationalUnit</config:objectClasses>
<config:objectClasses>domain</config:objectClasses>
<config:searchBases>ou=cam,o=ca</config:searchBases>
</config:ldapEntityTypes>

```

Attribute required if membershipAttribute is defined; otherwise no Groups will display for either configuration.

```

</config:ldapEntityTypes>
<config:groupConfiguration updateGroupMembership="true">
  <config:memberAttributes dummyMember="uid=dummy" name="member" objectClass="dynamicMember" scope="direct"/>
  <config:dynamicMemberAttributes name="member" objectClass="dxDynamicMember" scope="dynamic"/>
  <config:membershipAttribute name="member" scope="direct"/>
</config:groupConfiguration>

```

dynamicMemberAttribute for dynamic groups defined;  
but not required for use-cases with CA Directory

```

</config:attributeConfiguration>
<config:contextPool enabled="true" initPoolSize="1" maxPoolSize="0" poolWaitTime="3000" prefPoolSize="3"/>
<config:cacheConfiguration cachesDiskOffLoad="false">
  <config:attributesCache attributeSizeLimit="2000" cacheSize="4000" cacheTimeOut="600" enabled="true" cacheDistPolicy="push"/>
  <config:searchResultsCache cacheSize="2000" cacheTimeOut="600" enabled="true" searchResultSizeLimit="1000" cacheDistPolicy="push"/>
</config:cacheConfiguration>

```

**DOMINO TYPE**

```

<config:rdnAttributes>organization"/>
<config:rdnAttributes>"organizationalUnit"/>
<config:rdnAttributes>"domain"/>
<config:rdnAttributes name="cn" objectClass="container"/>
<config:objectClasses>organization</config:objectClasses>
<config:objectClasses>organizationalUnit</config:objectClasses>
<config:objectClasses>domain</config:objectClasses>
<config:objectClasses>container</config:objectClasses>
</config:ldapEntityTypes>

```

membershipAttribute name=member may be removed completely; no impact to use-cases with CA Directory

```

</config:ldapEntityTypes>
<config:groupConfiguration>
  <config:memberAttributes dummyMember="uid=dummy" name="member" objectClass="dynamicMember" scope="dynamic"/>
</config:groupConfiguration>
<config:entityTypes>PersonAccount</config:entityTypes>
</config:attributes>
<config:attributes name="krbPrincipalName" propertyName="kerberosId">
  <config:entityTypes>PersonAccount</config:entityTypes>
</config:attributes>
<config:propertiesNotSupported name="homeAddress"/>
<config:propertiesNotSupported name="businessAddress"/>

```

Attribute(s) not in schema nor required to be managed

```

</config:attributeConfiguration>
<config:contextPool enabled="true" initPoolSize="1" maxPoolSize="0" poolWaitTime="3000" prefPoolSize="3"/>
<config:cacheConfiguration cachesDiskOffLoad="false">
  <config:attributesCache attributeSizeLimit="2000" cacheSize="4000" cacheTimeOut="600" enabled="true" cacheDistPolicy="push"/>
  <config:searchResultsCache cacheSize="2000" cacheTimeOut="600" enabled="true" searchResultSizeLimit="1000"/>
</config:cacheConfiguration>

```

