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 Jthyon / 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/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

- <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://websphereapplicationservernotes.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>

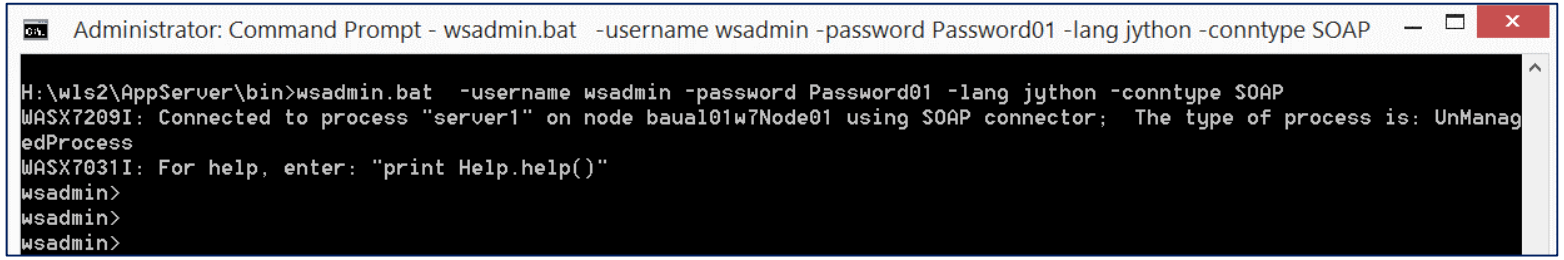
Ref: https://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/welc_howdoi_tscr.html

Background: Execute Jython Script

Interactively

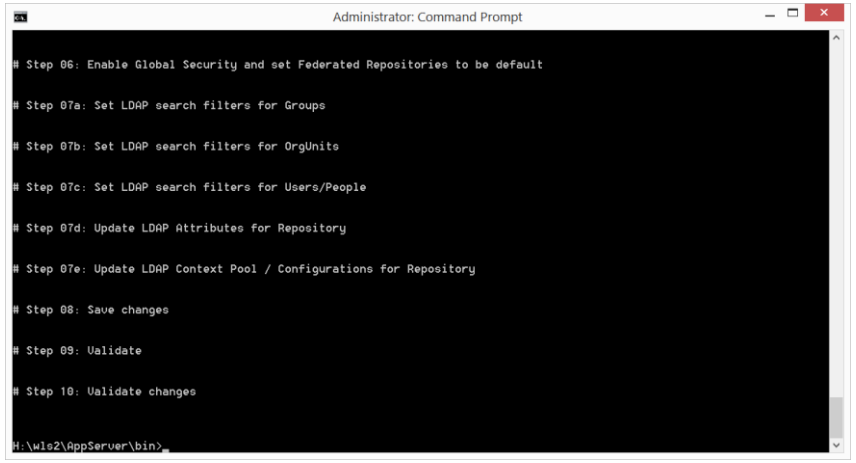
bin>wsadmin.bat -username wsadmin -password Password01 -lang jython -conntype SOAP

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



Input File

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



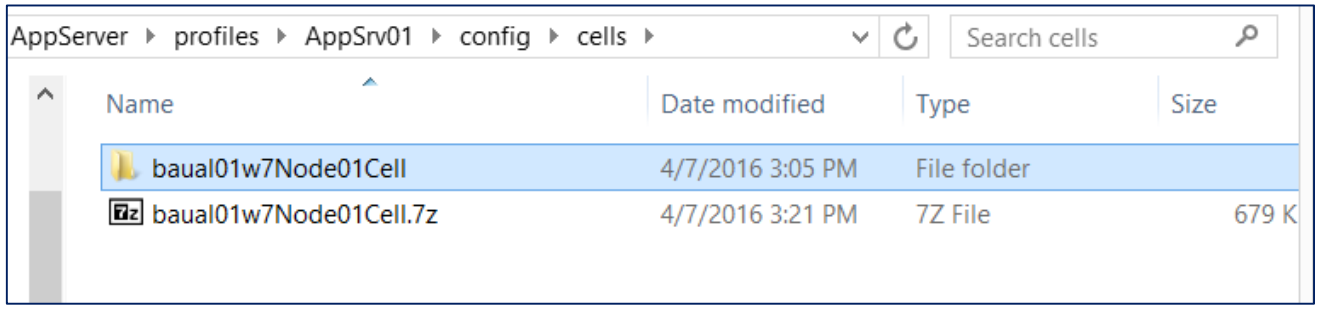
Background: WAS CLI Debug

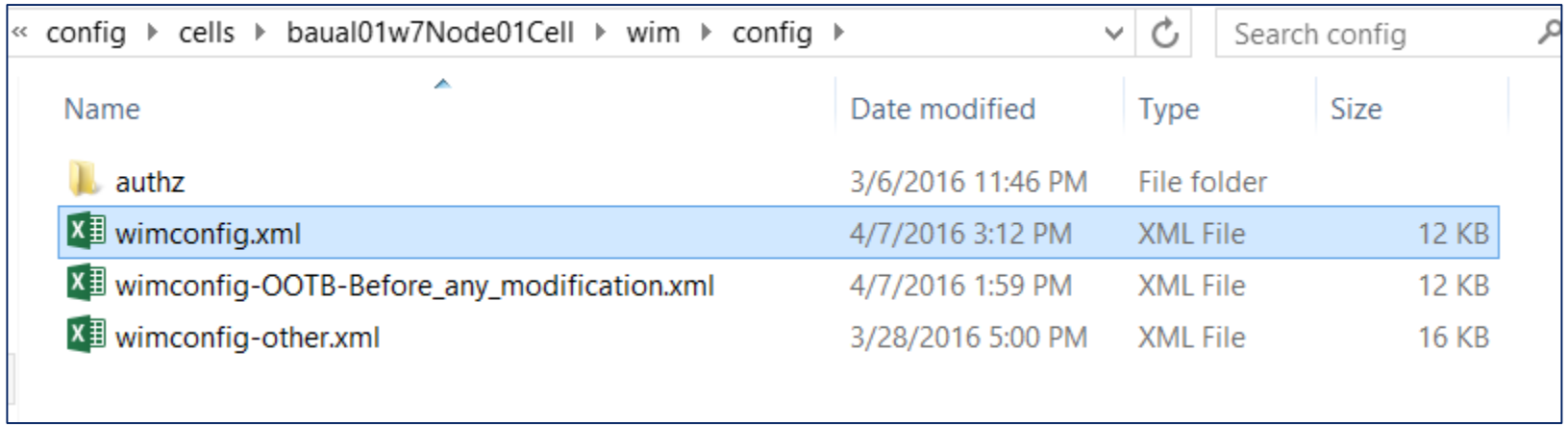
1. Enable wsadmin tracing by editing the wsadmin.properties file
    1. <WAS_HOME>/profiles/<PROFILE_NAME>/properties/wsadmin.properties
2. Enable “Admin=all” tracing on each server process involved.
    1. Uncomment the following line by removing the #:
    2. #com.ibm.ws.scripting.traceString=com.ibm.*=all=enabled
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.traceoutractive” mode to generate a single working command:

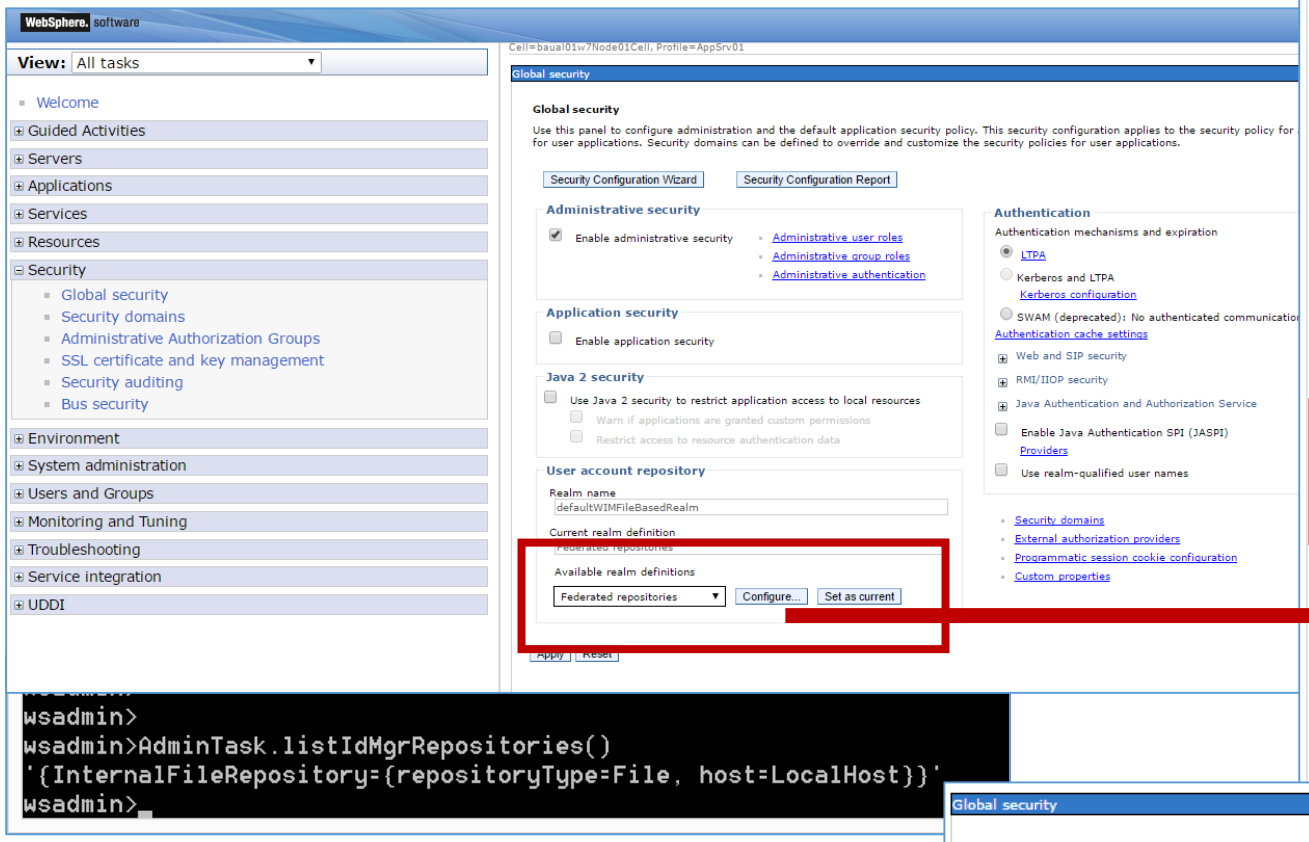
Steps to Enable Custom Label for CA Directory

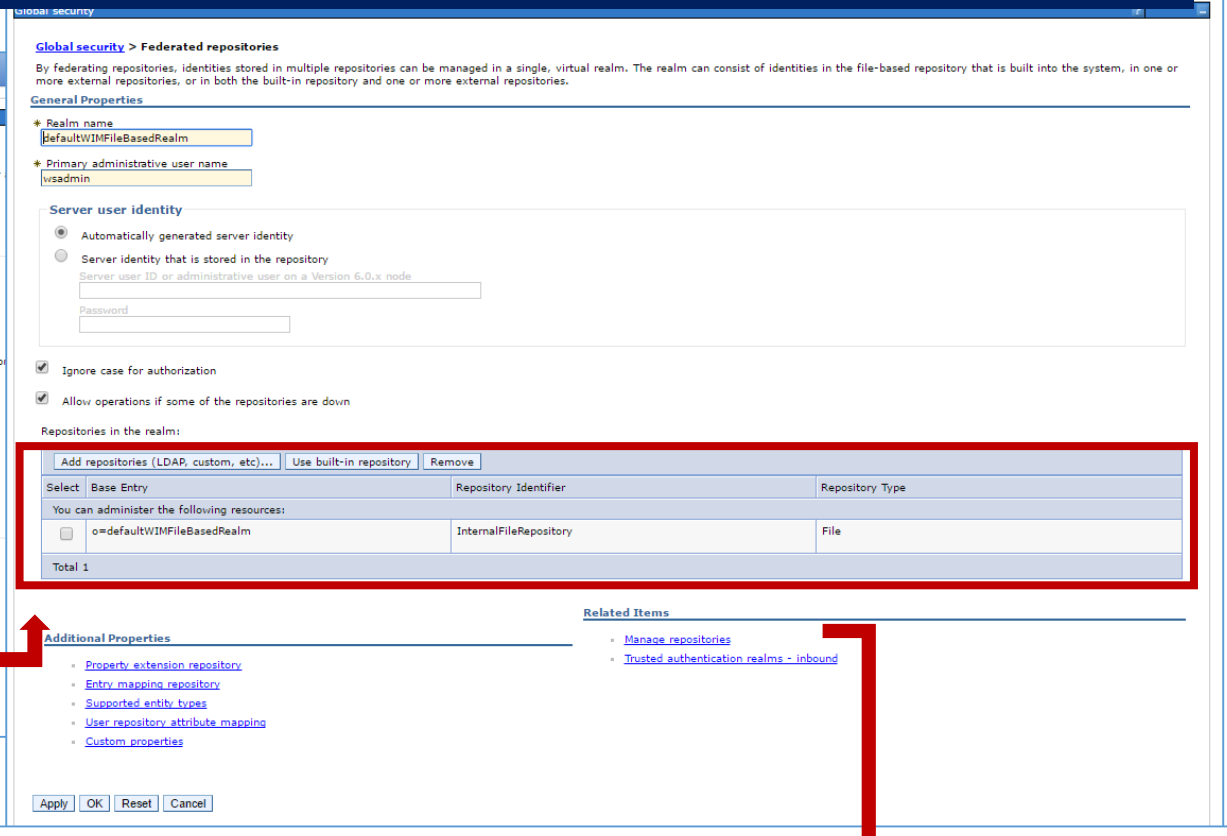
Step 01: Backup WAS Cell Before Starting

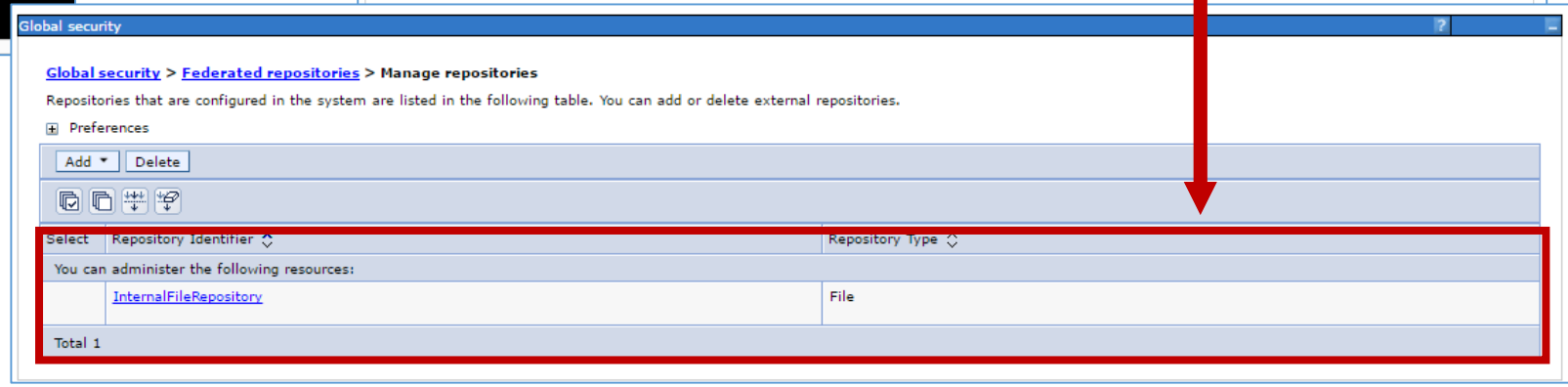




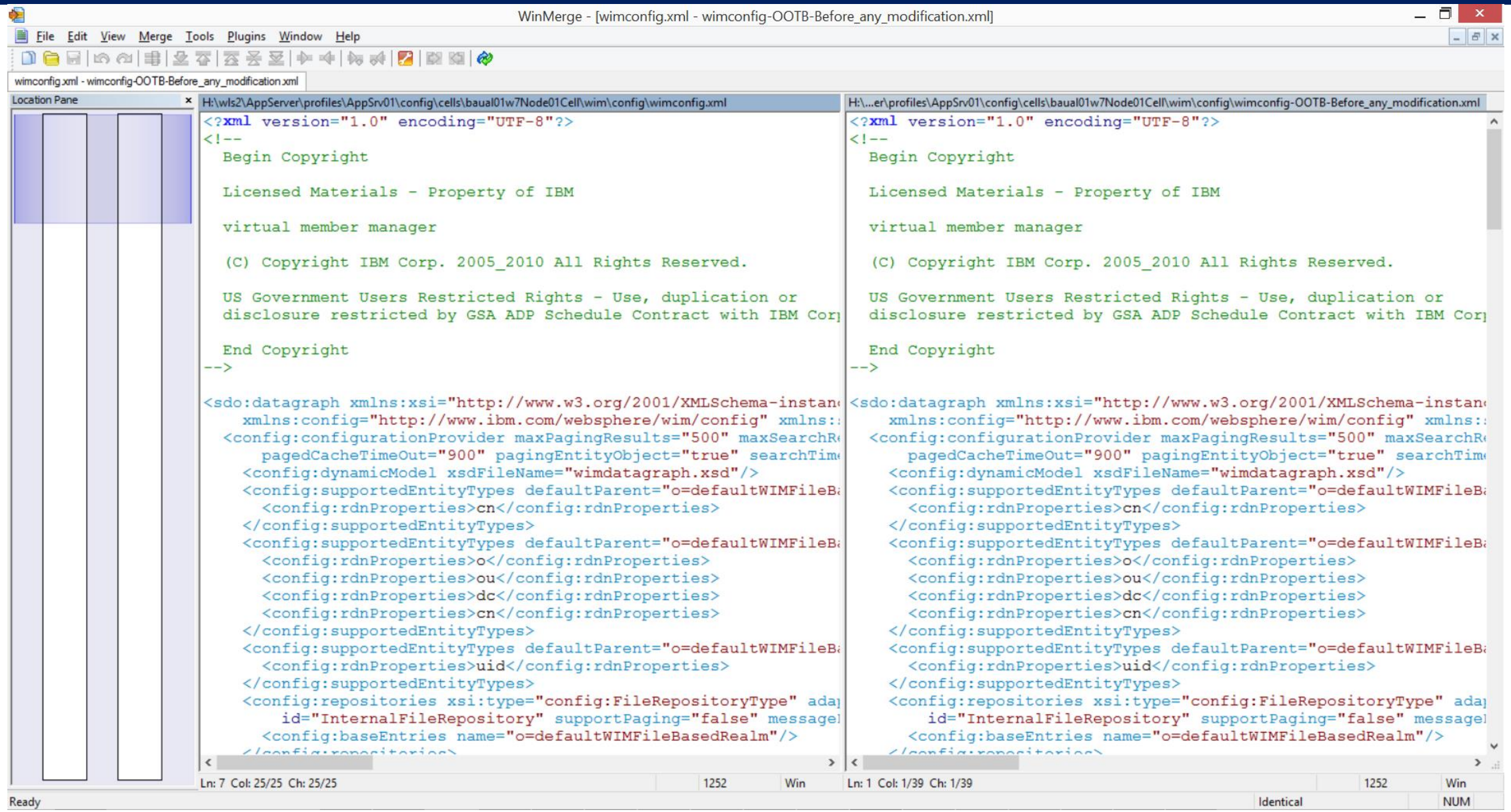
Step 02: Review WAS Federated Repositories: Before State



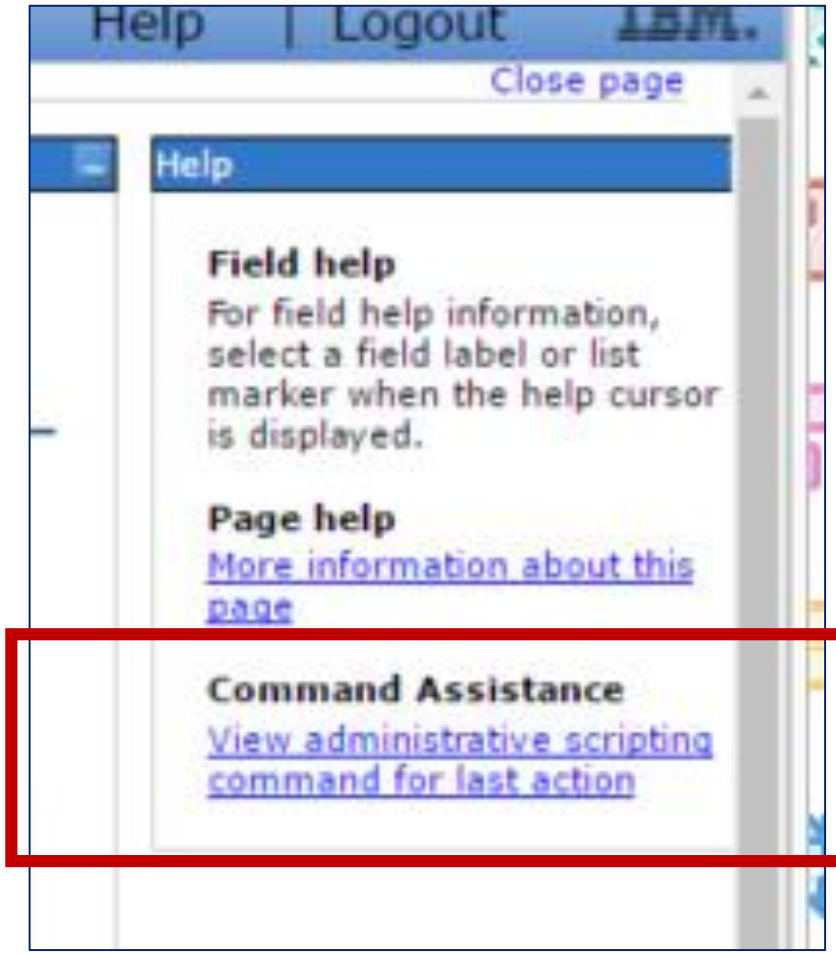


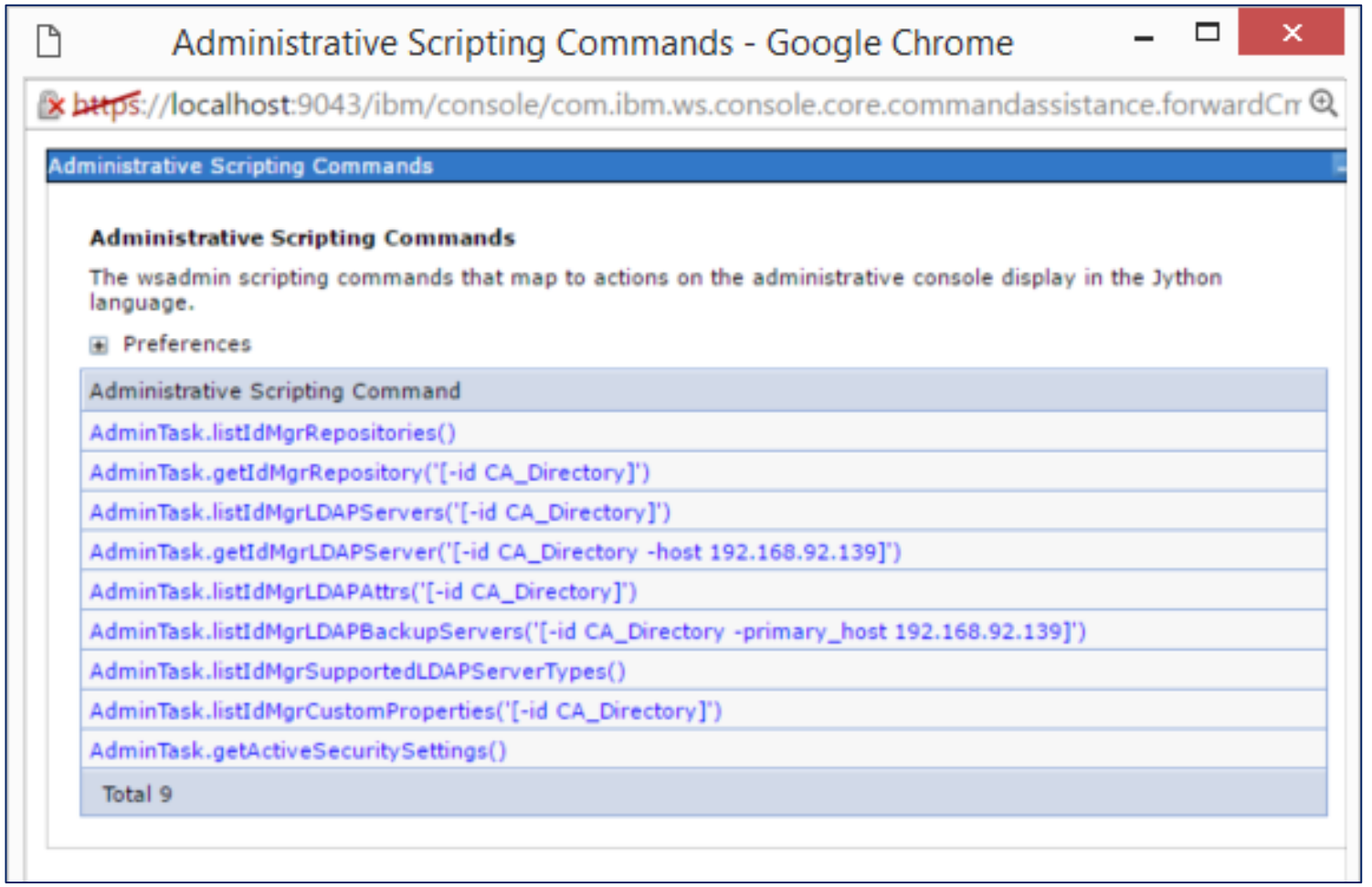


Step 03: Make backup copy of wimconfig.xml and open within WinMerge Tool



Step 04: Perform configuration steps in UI.
Use WAS Help Guide on Admin Scripting to display last command used in UI





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.ldap.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_,'-
referal','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.ldap.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','o','-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: UnManag
edProcess
WASX7031I: For help, enter: "print Help.help()"
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
wsadmin>
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\Admini
strator\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.i
bm.websphere.wim.exception.WIMConfigurationException: CWWIM5025E  Base entry ou=cam,o=ca is not found in the defaultWIMF
ileBasedRealm realm.
```

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

WinMerge - [wimconfig.xml - wimconfig-OOTB-Before_any_modification.xml]

Location Pane

H:\wls2\AppServer\profiles\AppSrv01\config\cells\baual01w7Node01Cell\wim\config\wimconfig.xml

```
    <config:repositories xsi:type="config:FileRepositoryType" ada
        id="InternalFileRepository" supportPaging="false" message
      <config:baseEntries name="o=defaultWIMFileBasedRealm"/>
    </config:repositories>
    <config:repositories xsi:type="config:LdapRepositoryType" ada
        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" referal="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:searchBa
      </config:ldapEntityTypes>
      <config:ldapEntityTypes name="OrgContainer">
        <config:rdnAttributes name="o" objectClass="organization",
        <config:rdnAttributes name="ou" objectClass="organizationa
        <config:rdnAttributes name="dc" objectClass="domain"/>
        <config:objectClasses>organization</config:objectClasses>
        <config:objectClasses>organizationalUnit</config:objectCla
        <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:searchBa
      </config:ldapEntityTypes>
      <config:groupConfiguration updateGroupMembership="false">
```

H:\...er\profiles\AppSrv01\config\cells\baual01w7Node01Cell\wim\config\wimconfig-OOTB-Before_any_modification.xml

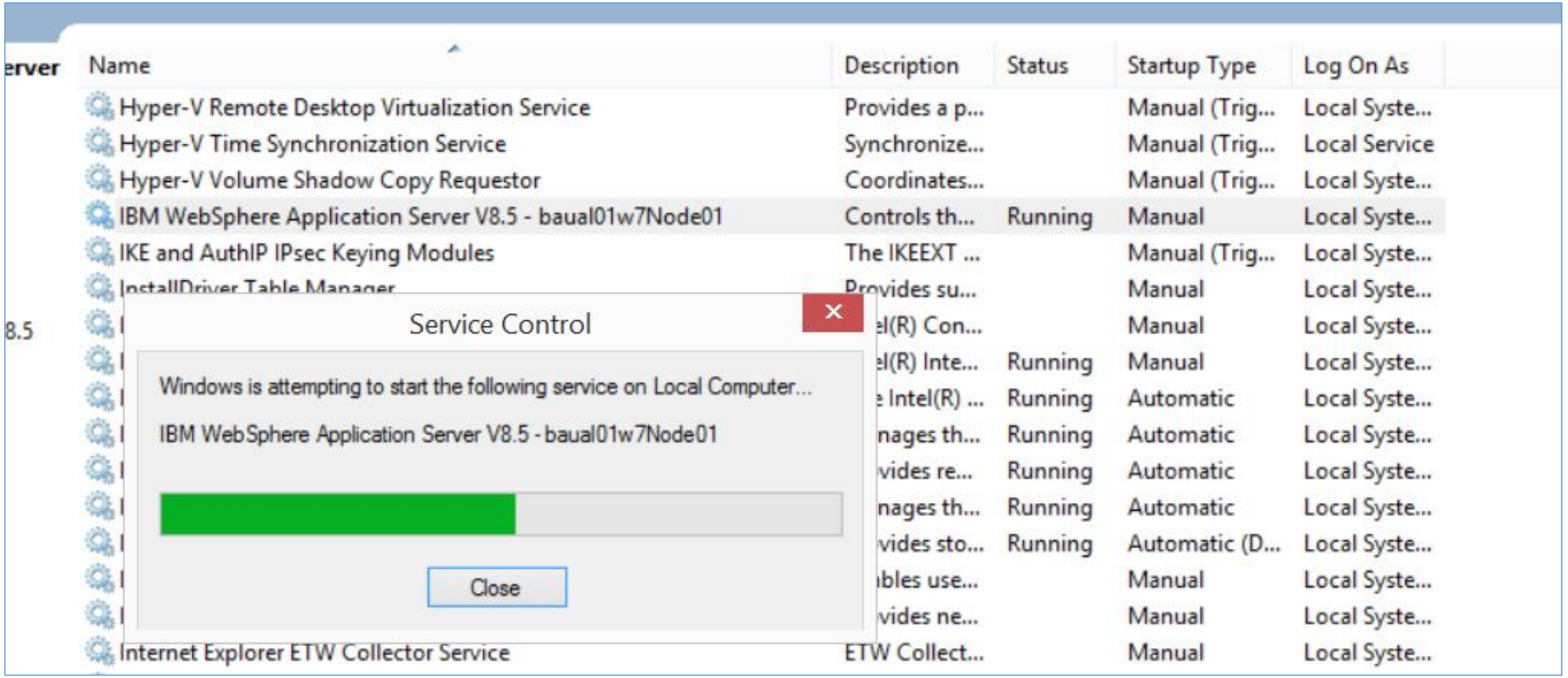
```
    <config:repositories xsi:type="config:FileRepositoryType" ada
        id="InternalFileRepository" supportPaging="false" message
      <config:baseEntries name="o=defaultWIMFileBasedRealm"/>
    </config:repositories>
```

Ln: 48 Col: 1/92 Ch: 1/92 | 1252 | Win

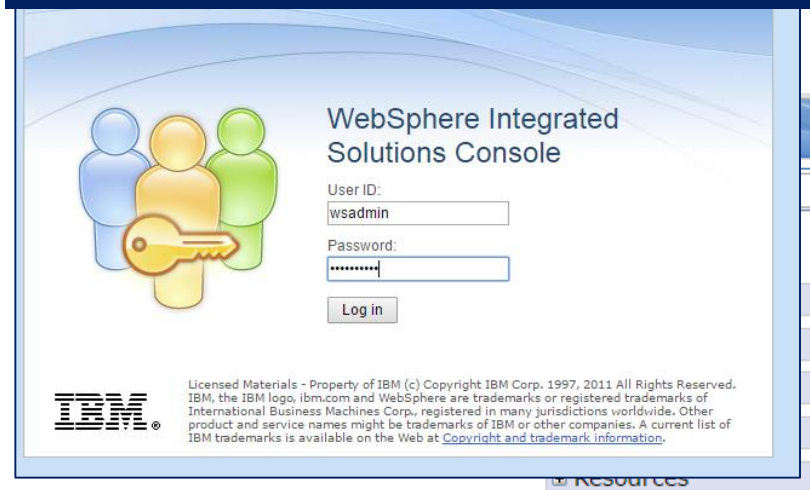
Line: 37-38 | 1252 | Win

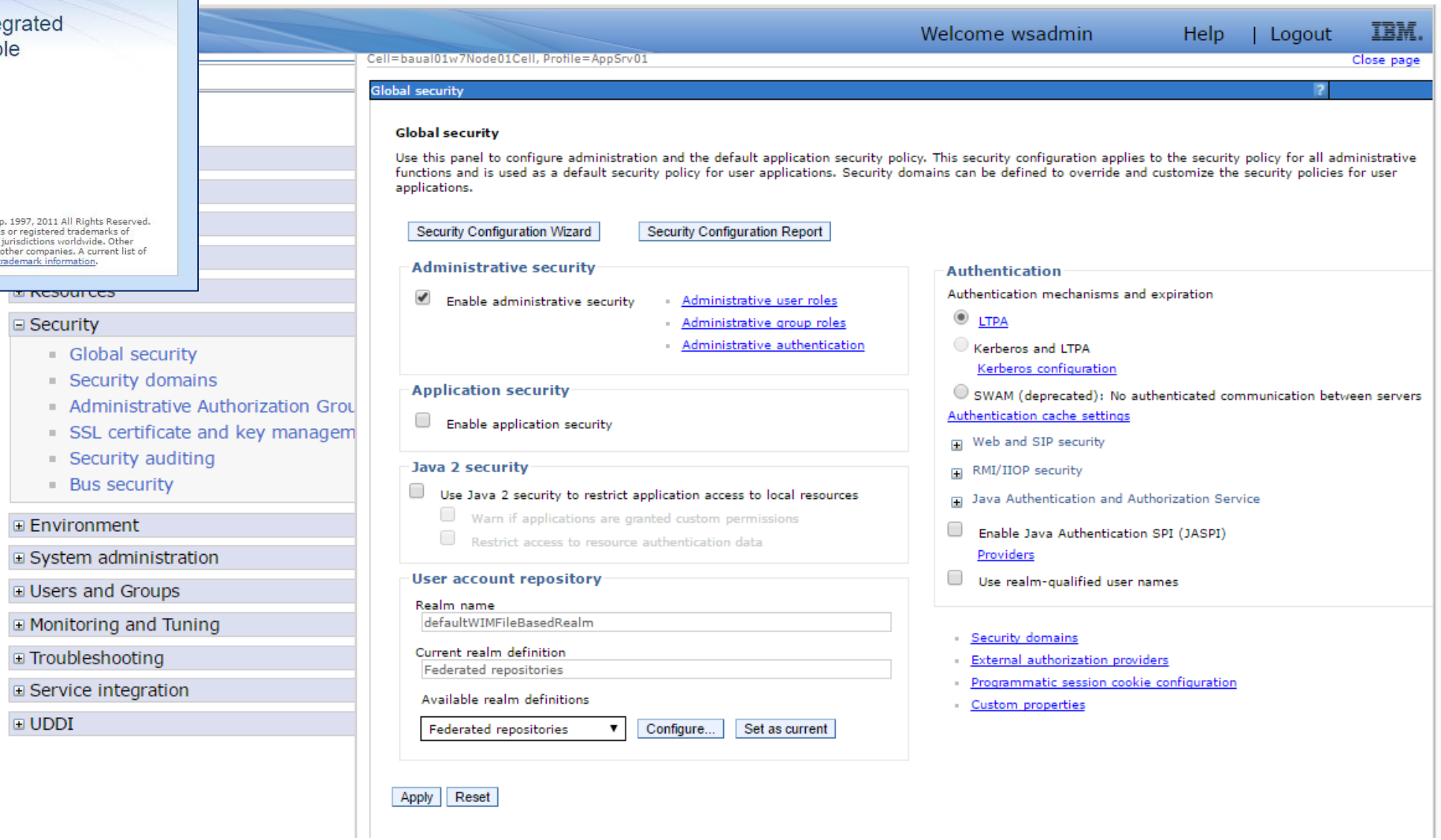
Ready | 3 Differences Found | NUM

Step 06d: Bounce NT Services to clear WAS cache

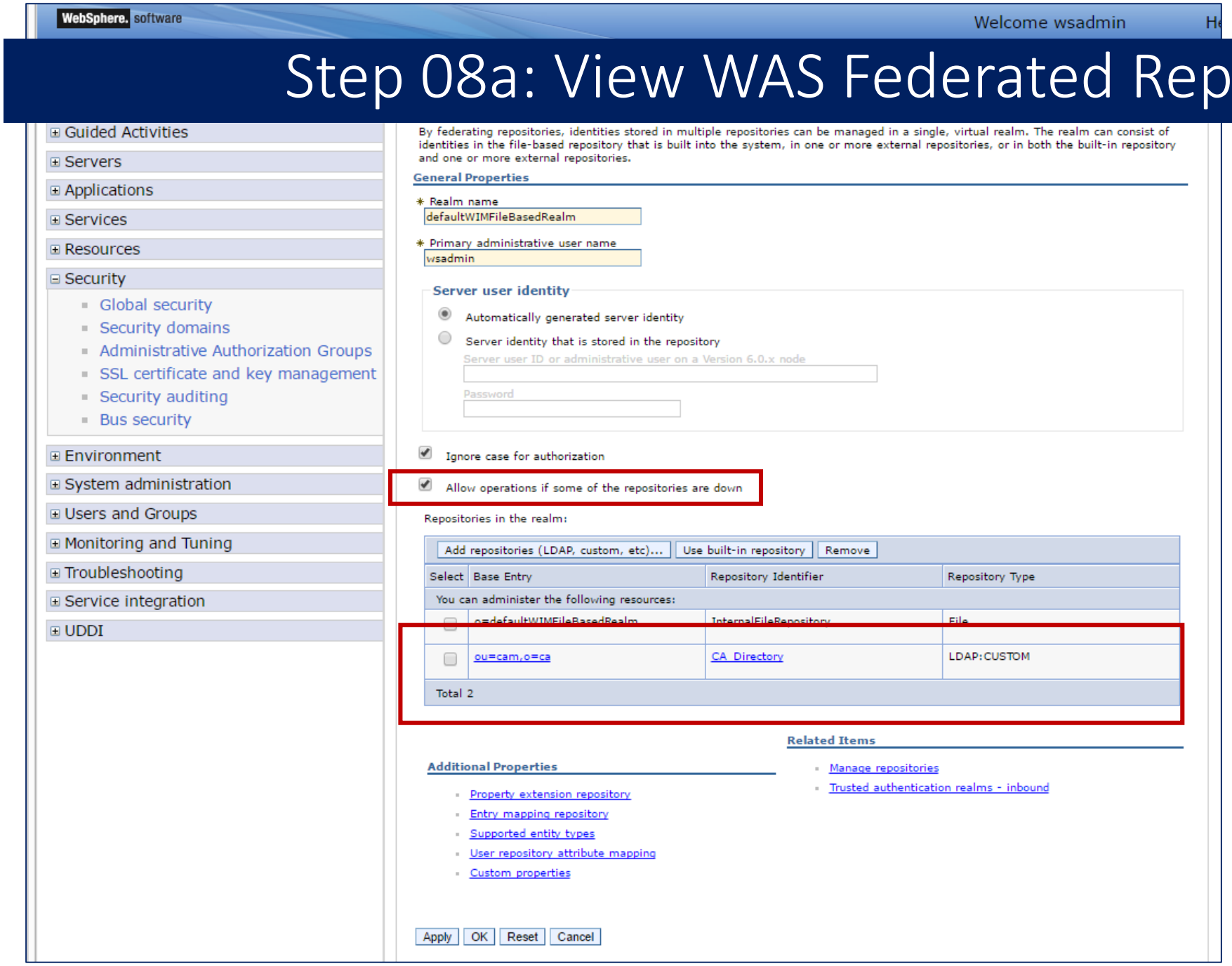


Step 07: WAS Federated Repositories: After State





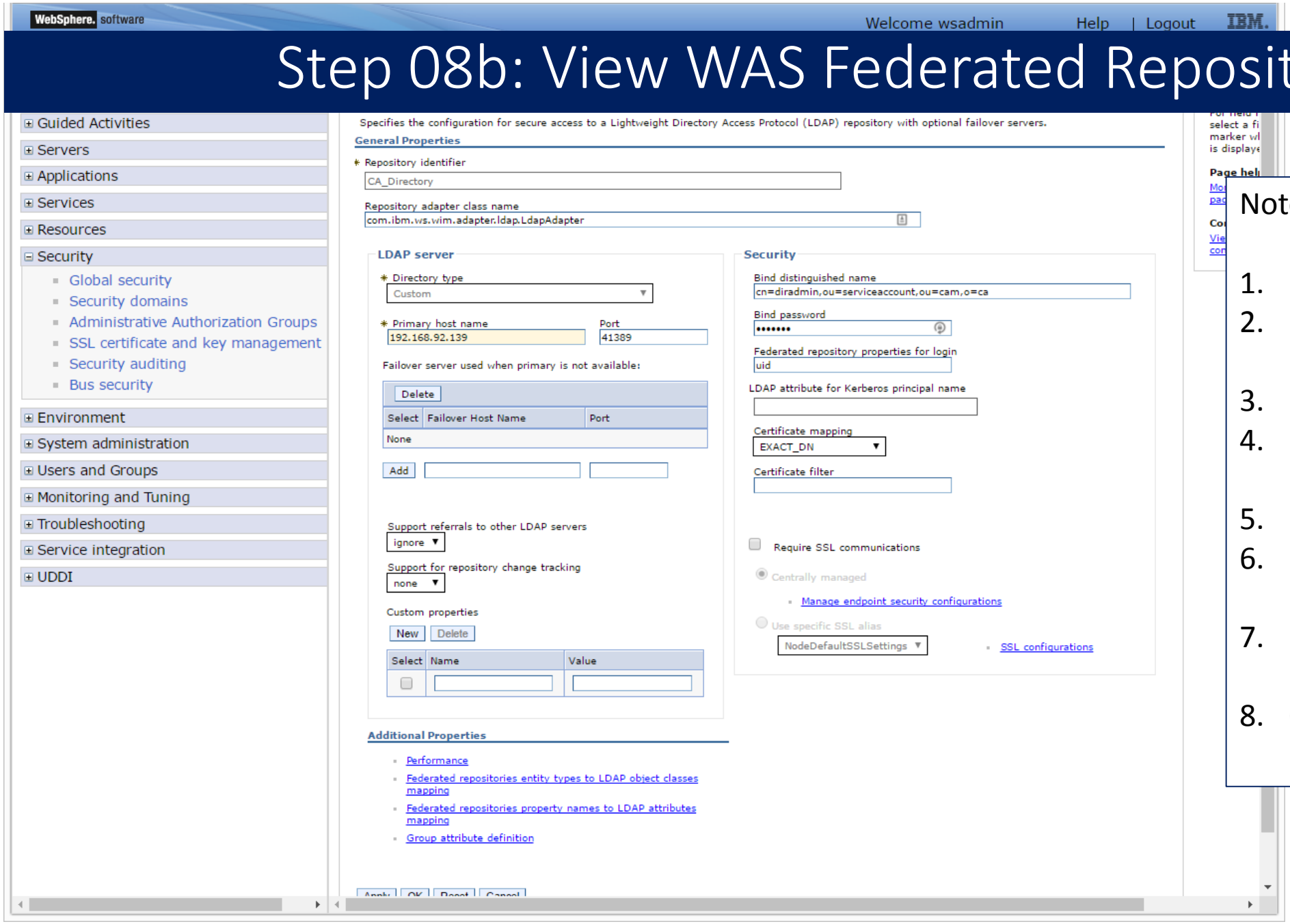
Step 08a: View WAS Federated Repositories



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

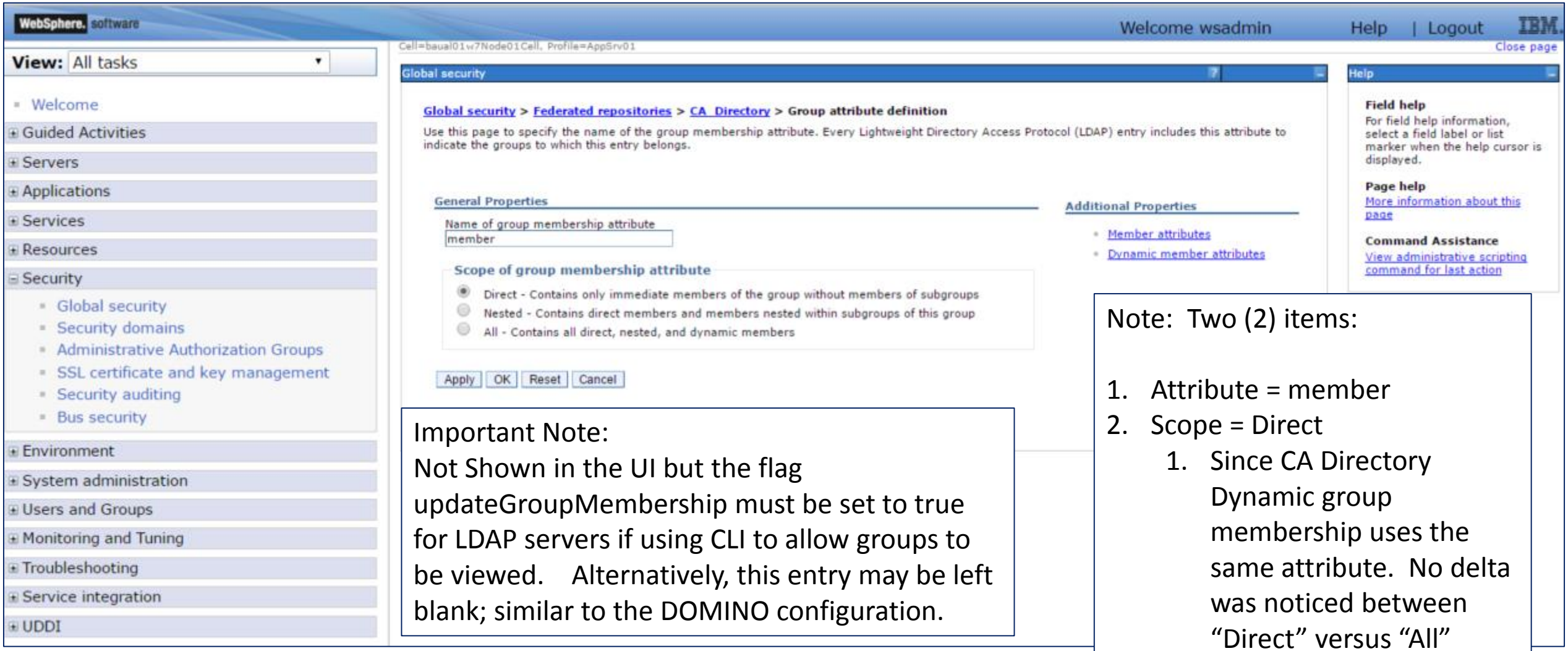
Step 08b: View WAS Federated Repositories



Note: Eight (8) items:

1. Label = CA_Directory
2. Using standard OOTB IBM ldap 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

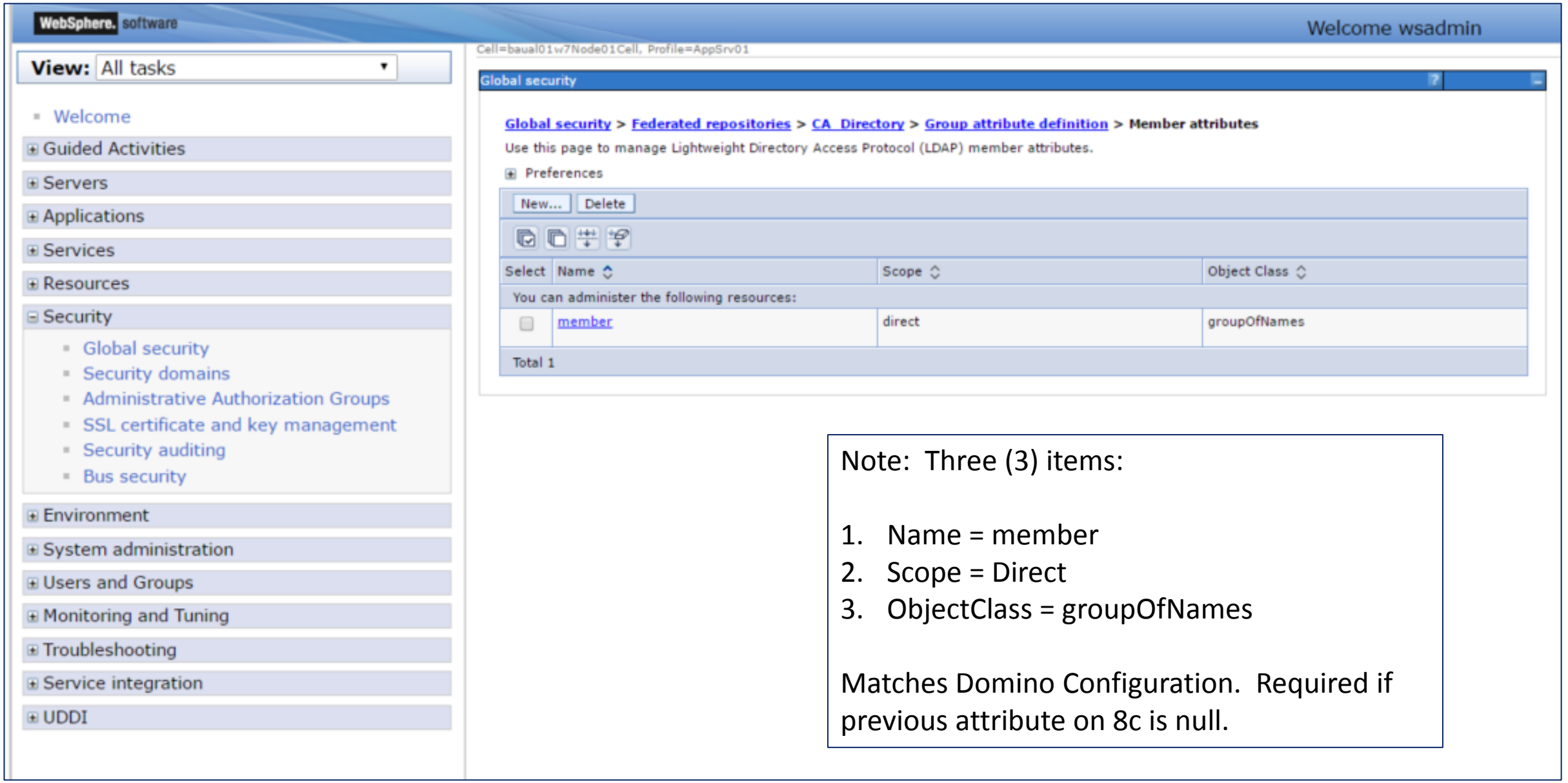


Important Note:
Not Shown in the UI but the flag updateGroupMembership must be set to true for LDAP servers if using CLI to allow groups to be viewed. Alternatively, this entry may be left blank; similar to the DOMINO configuration.

Note: Two (2) items:

1. Attribute = member
2. Scope = Direct
    1. Since CA Directory Dynamic group membership uses the same attribute. No delta was noticed between “Direct” versus “All”

Step 08d: View WAS Federated Repositories

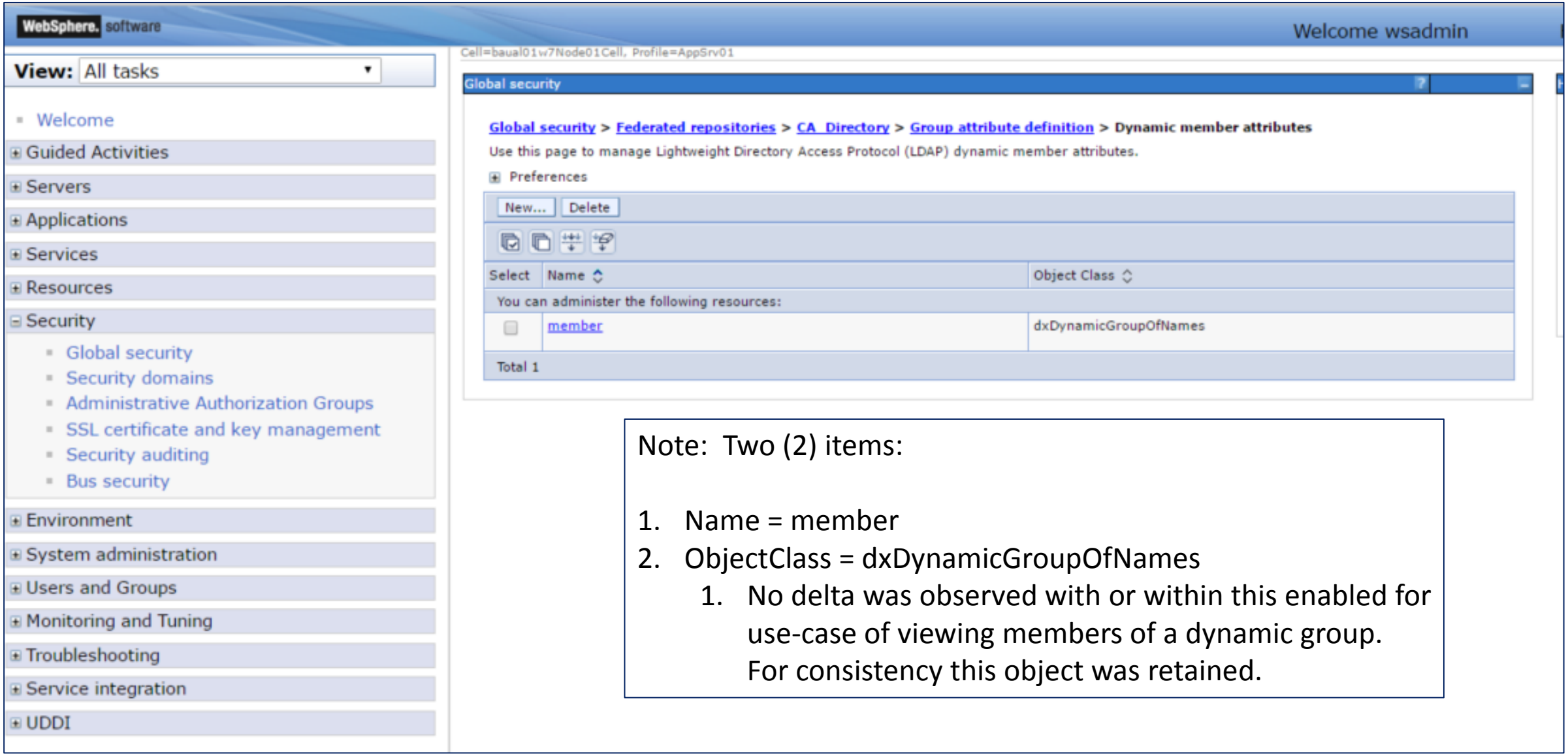


Note: Three (3) items:

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

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

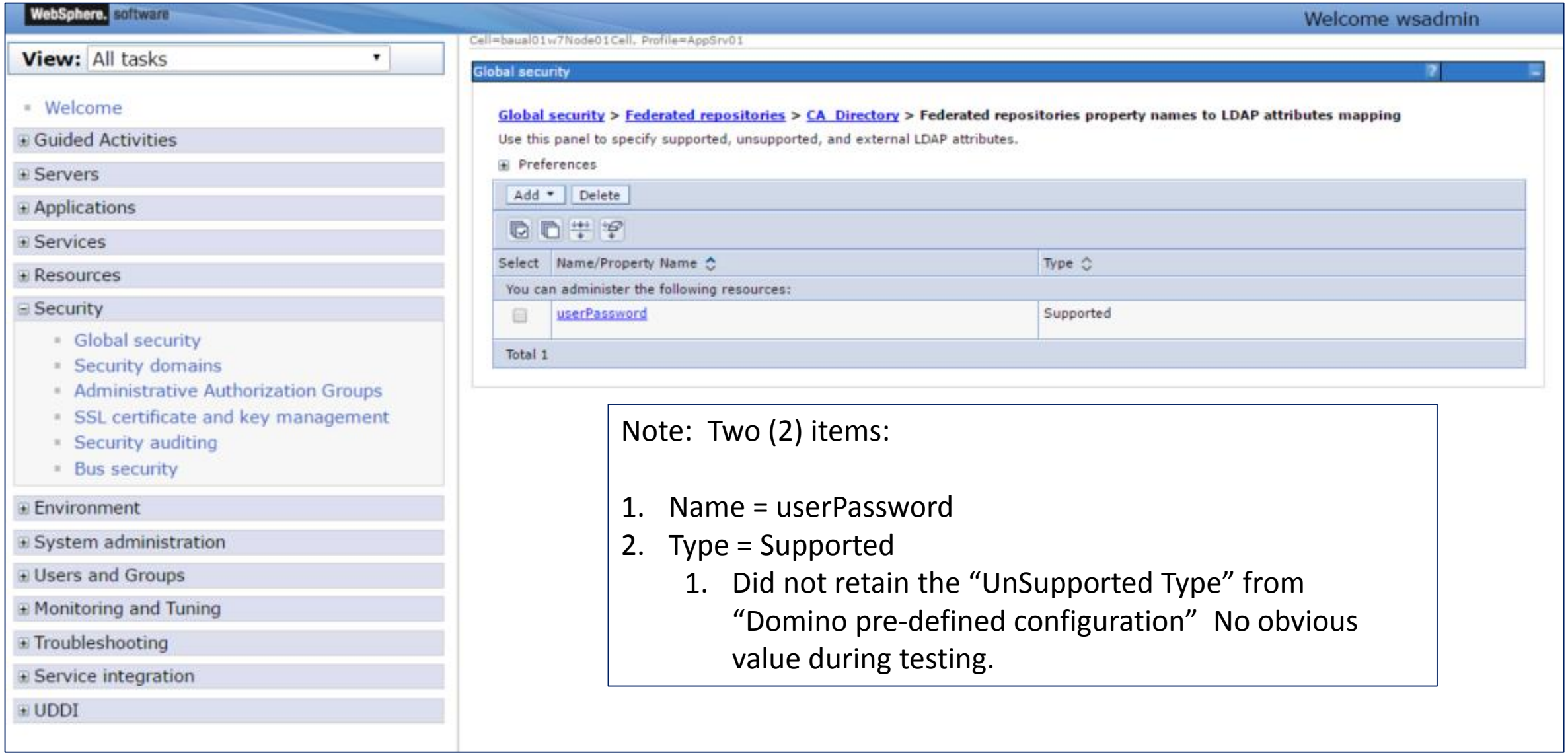
Step 08e: View WAS Federated Repositories



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.

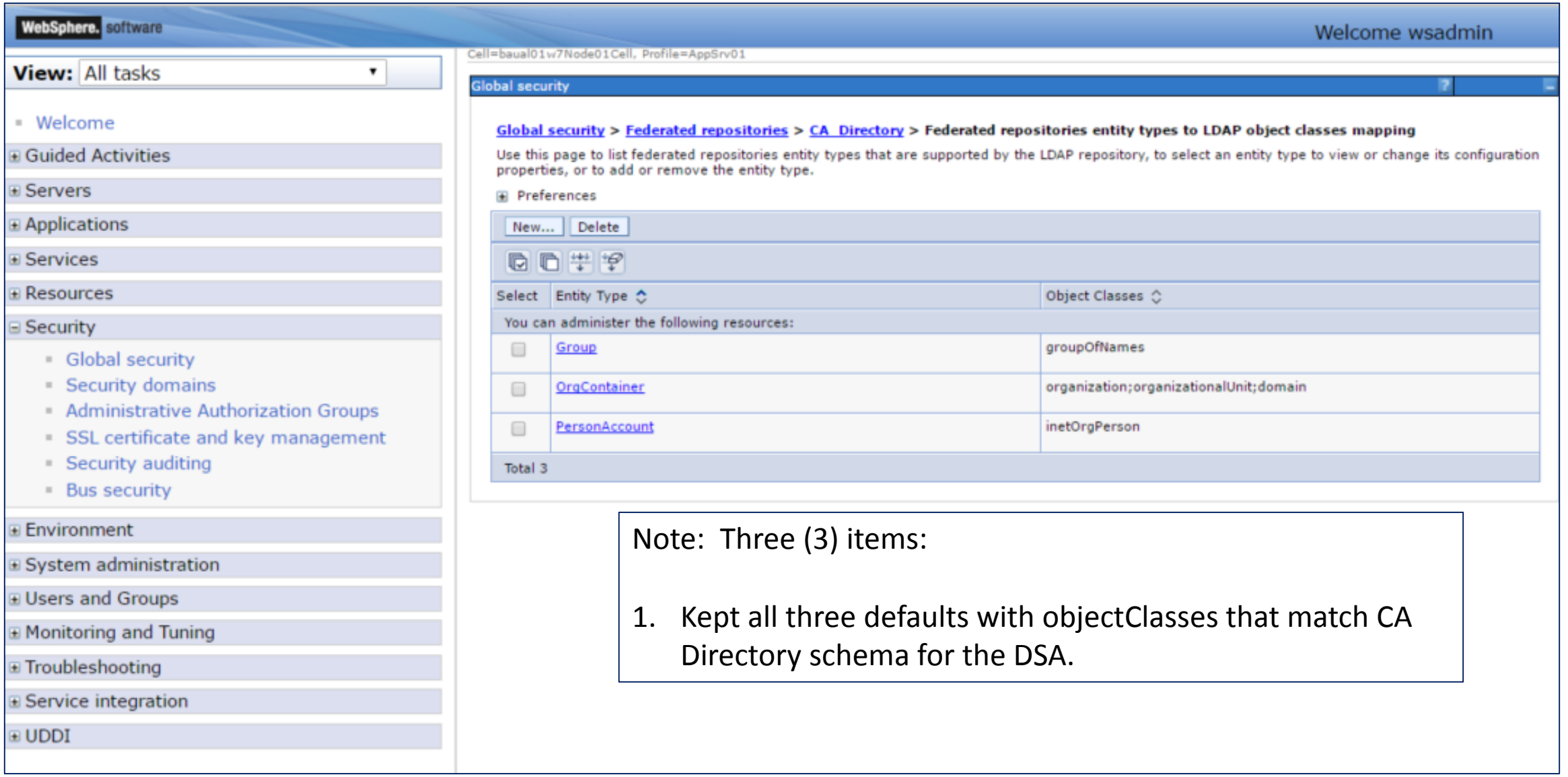
Step 08f: View WAS Federated Repositories



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.

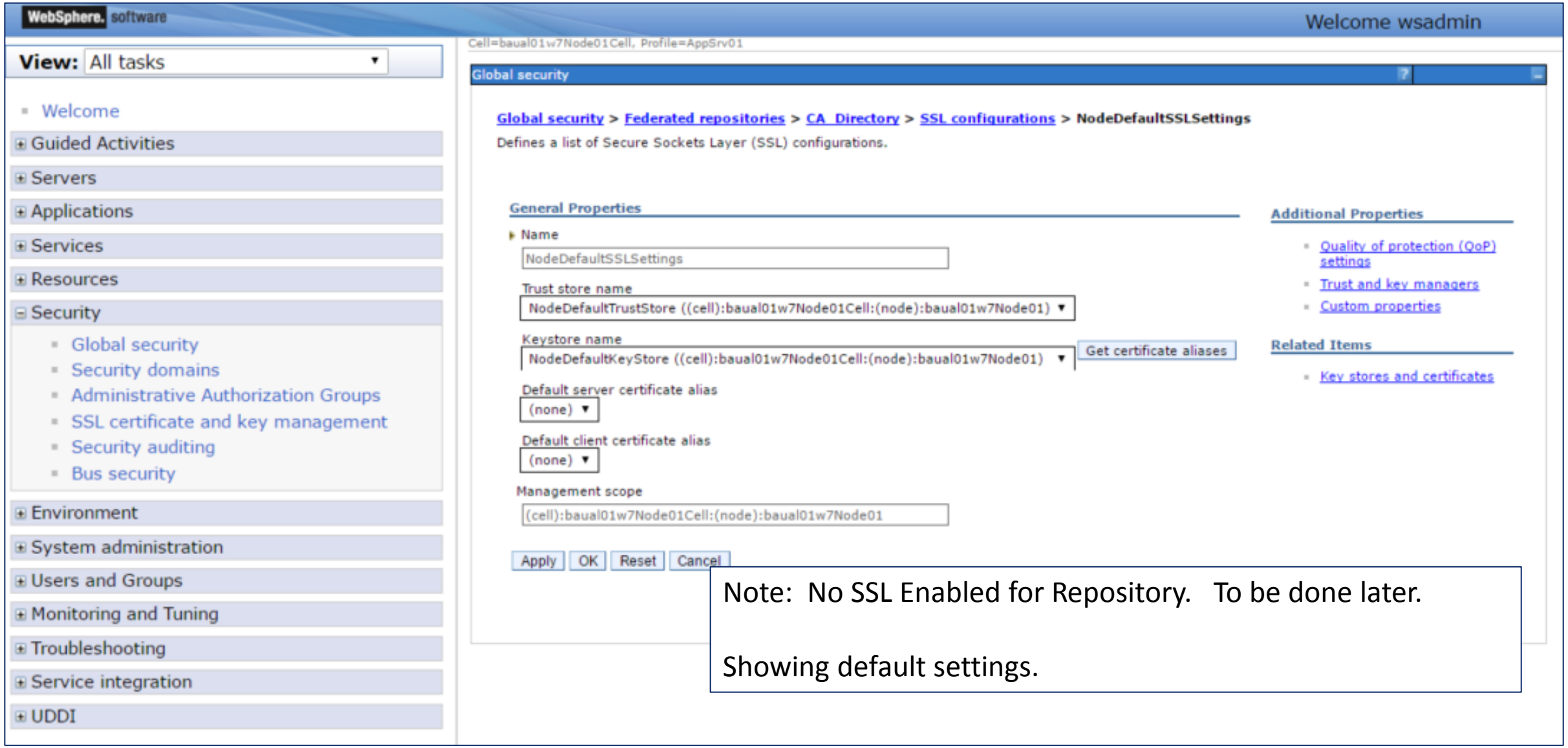
Step 08g: View WAS Federated Repositories



Note: Three (3) items:

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

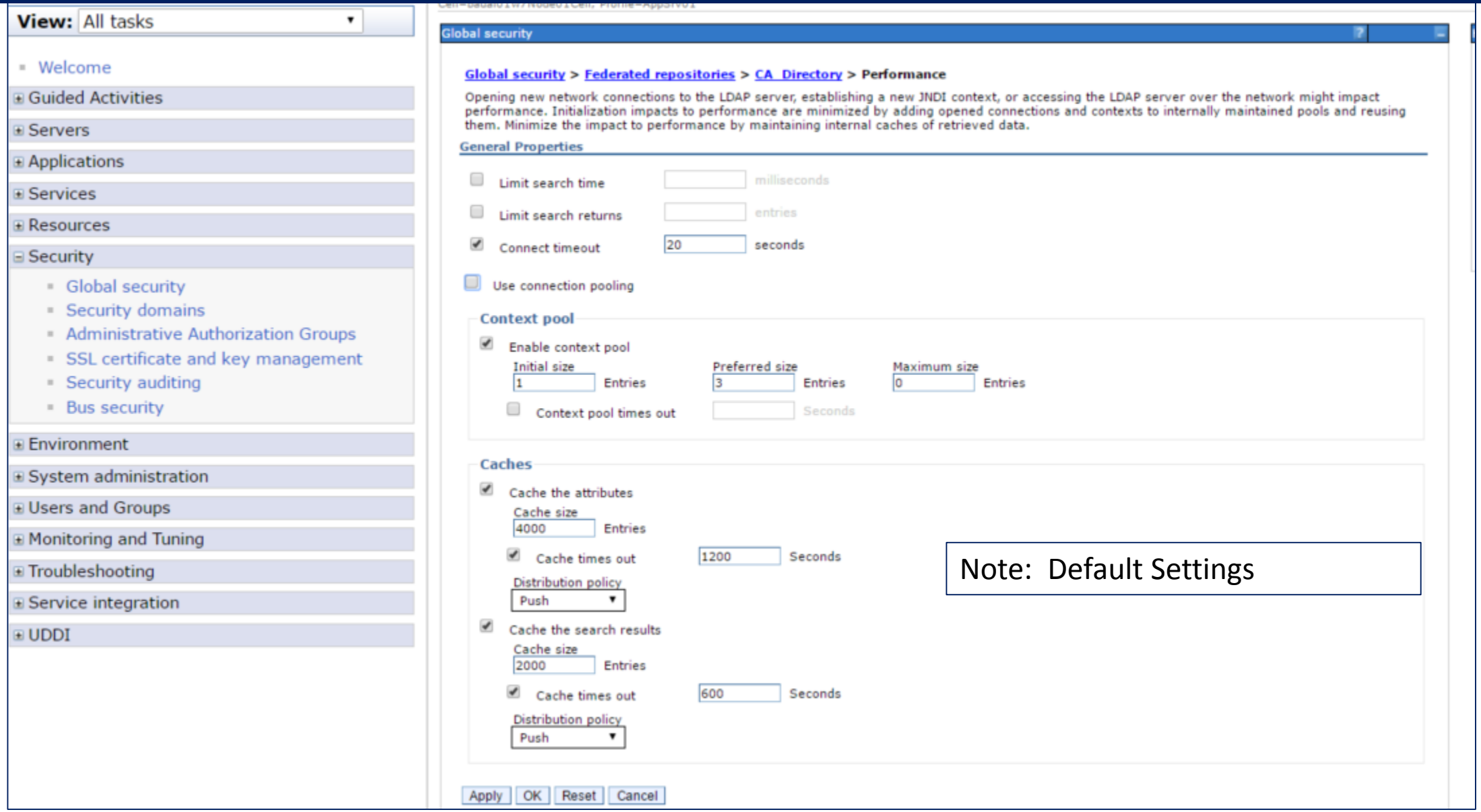
Step 08h: View WAS Federated Repositories



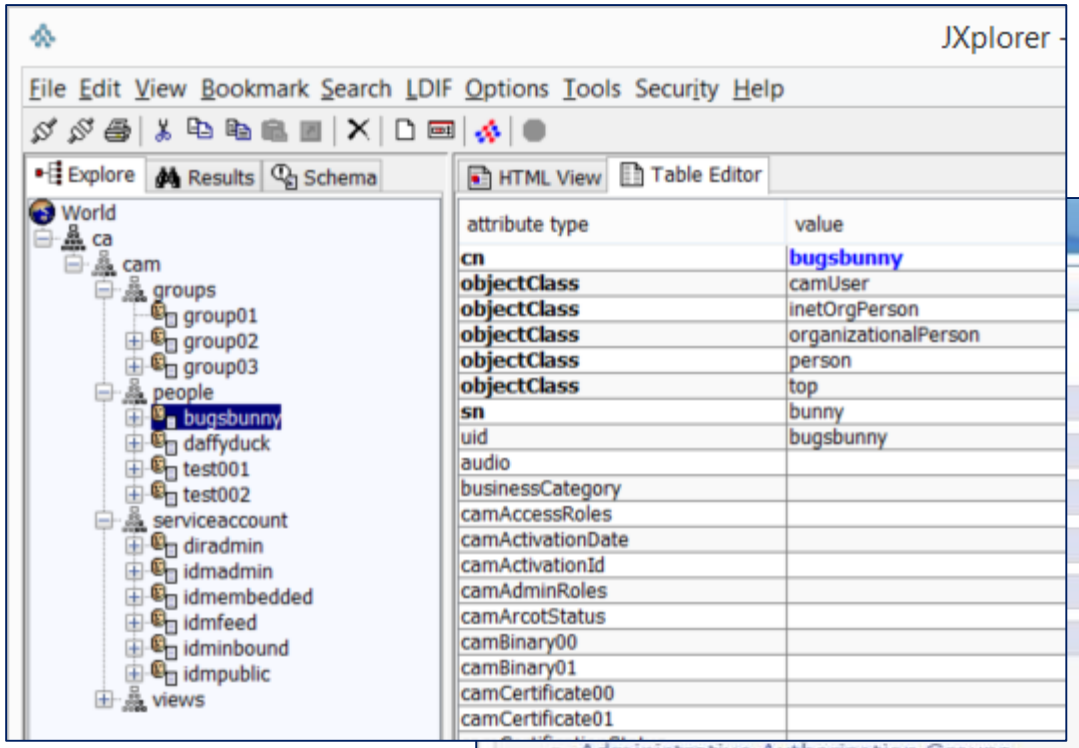
Note: No SSL Enabled for Repository. To be done later.

Showing default settings.

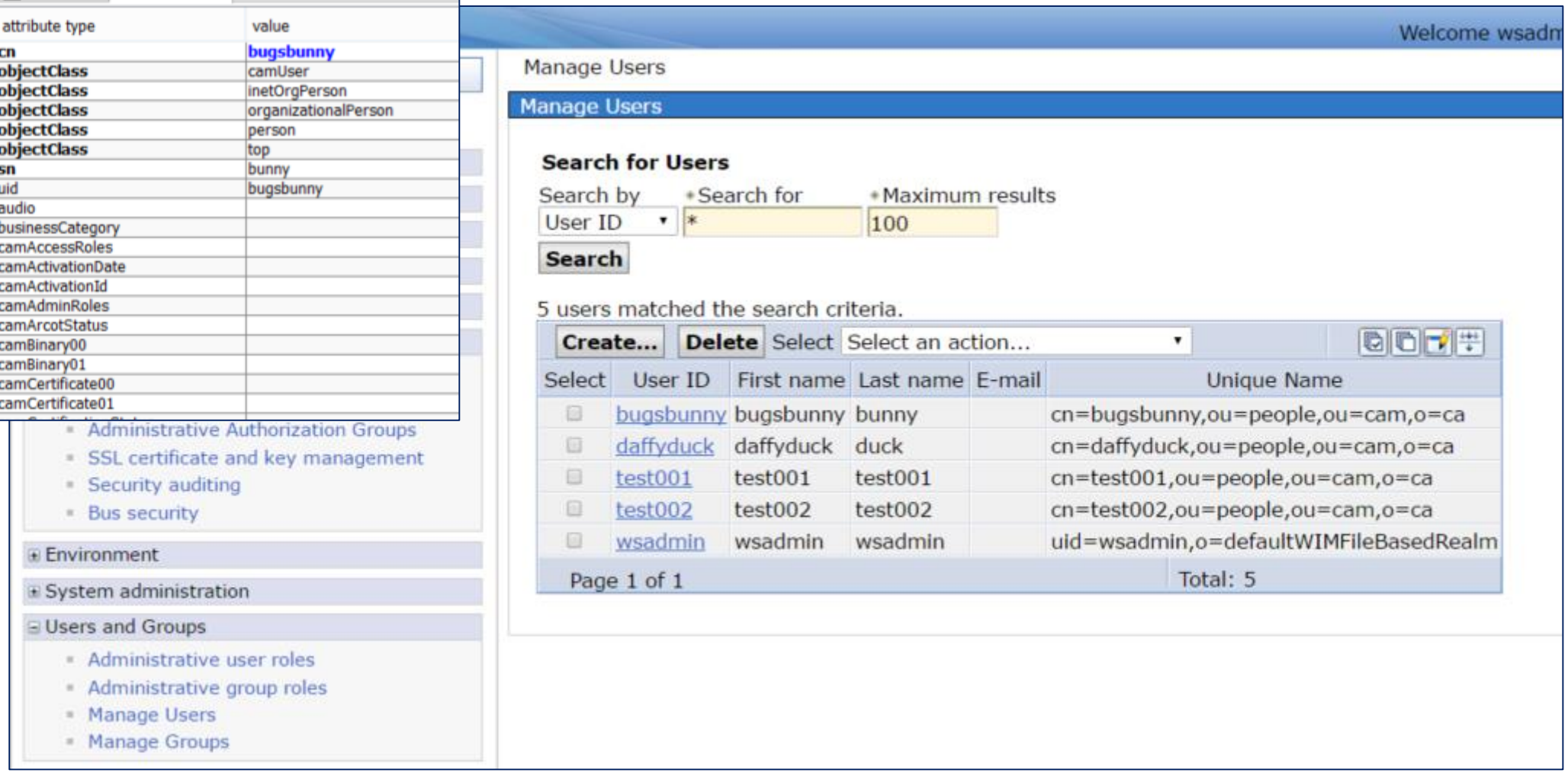
Step 08i: View WAS Federated Repositories



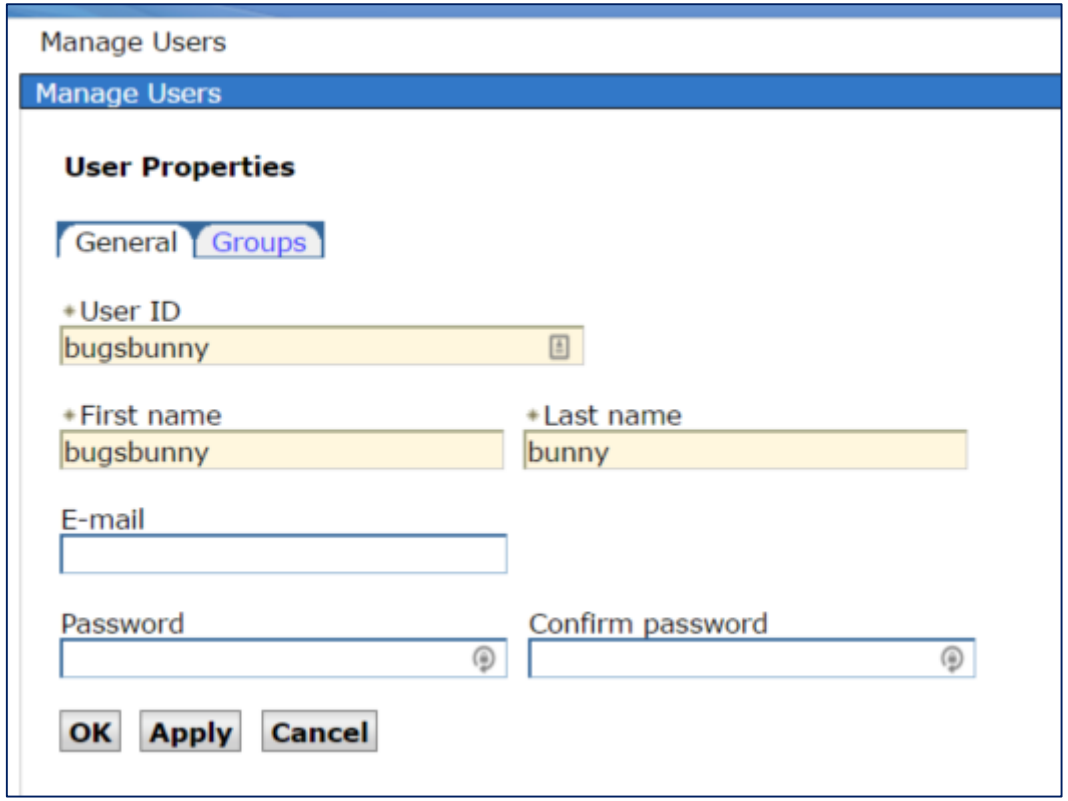
Step 09a: Validate Use-Case for Users Lookup

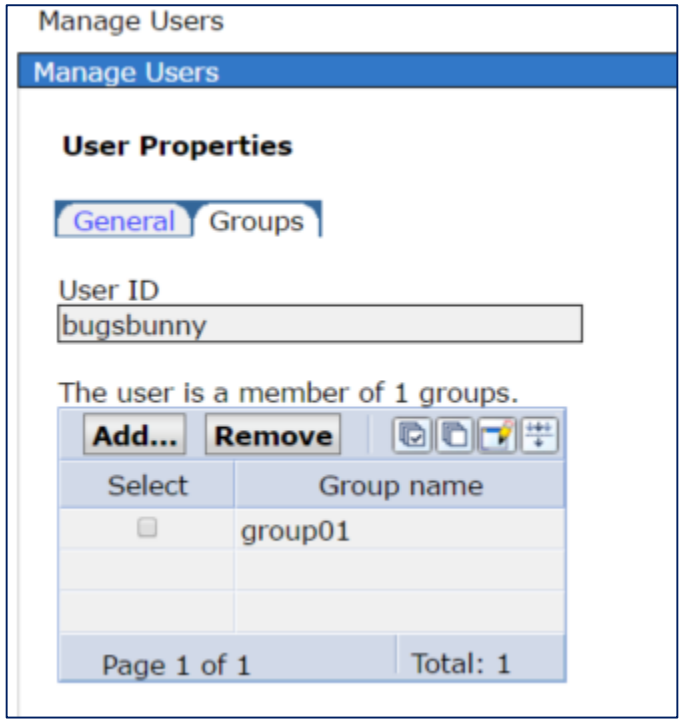


People Search OU limited to ou=people,ou=cam,o=ca
No service account will be displayed.

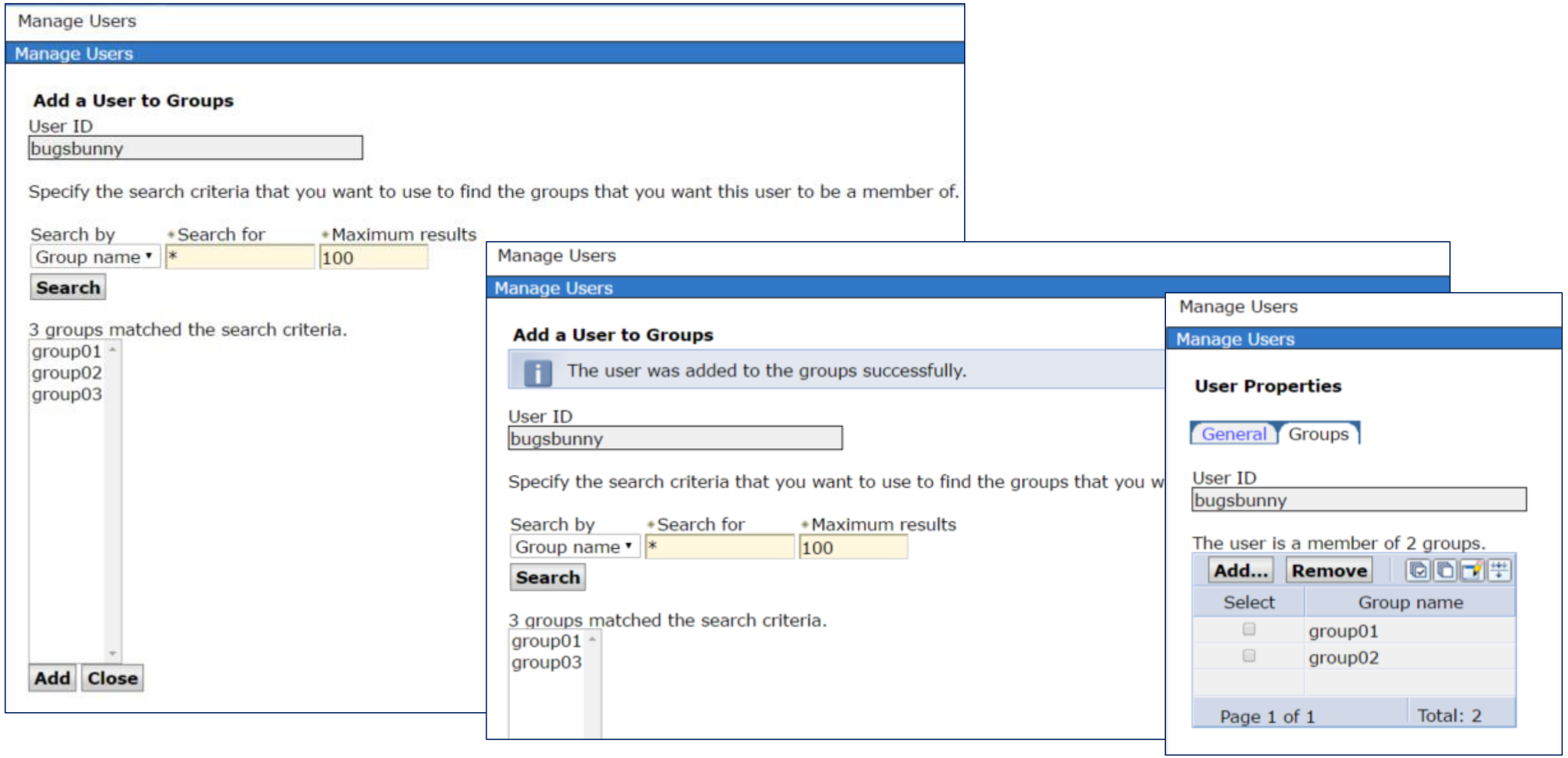


Step 09b: Validate Use-Case for Users Lookup

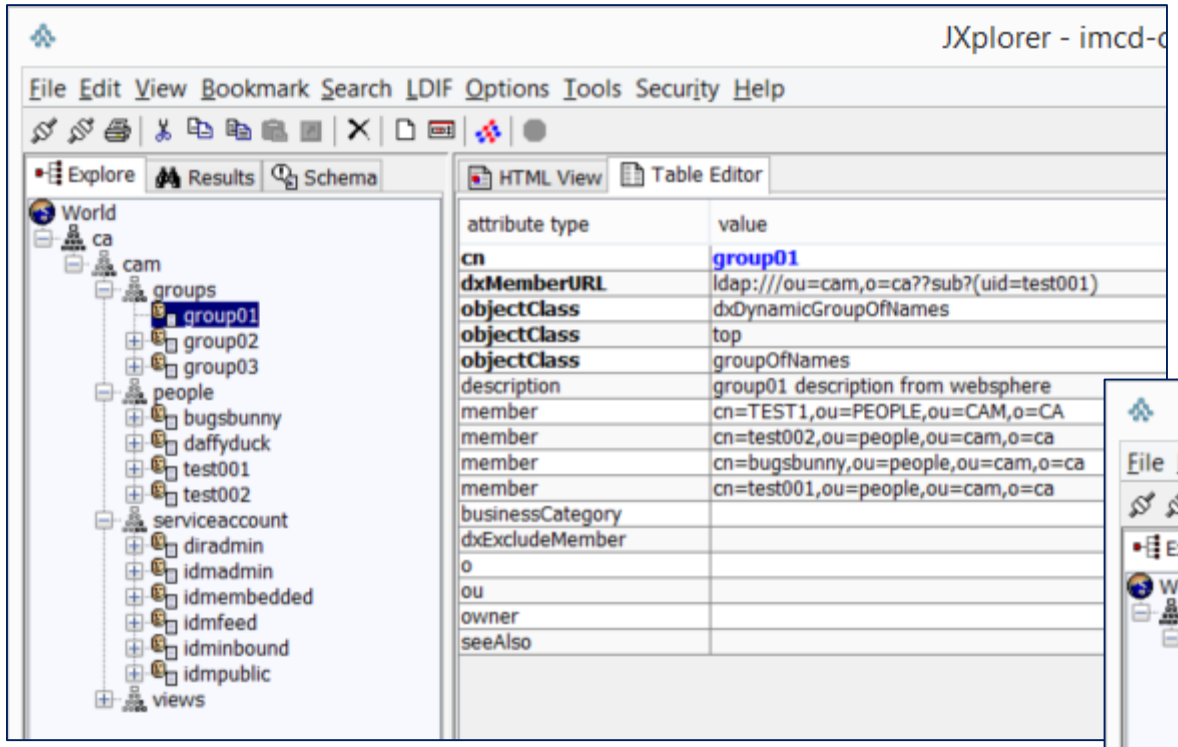


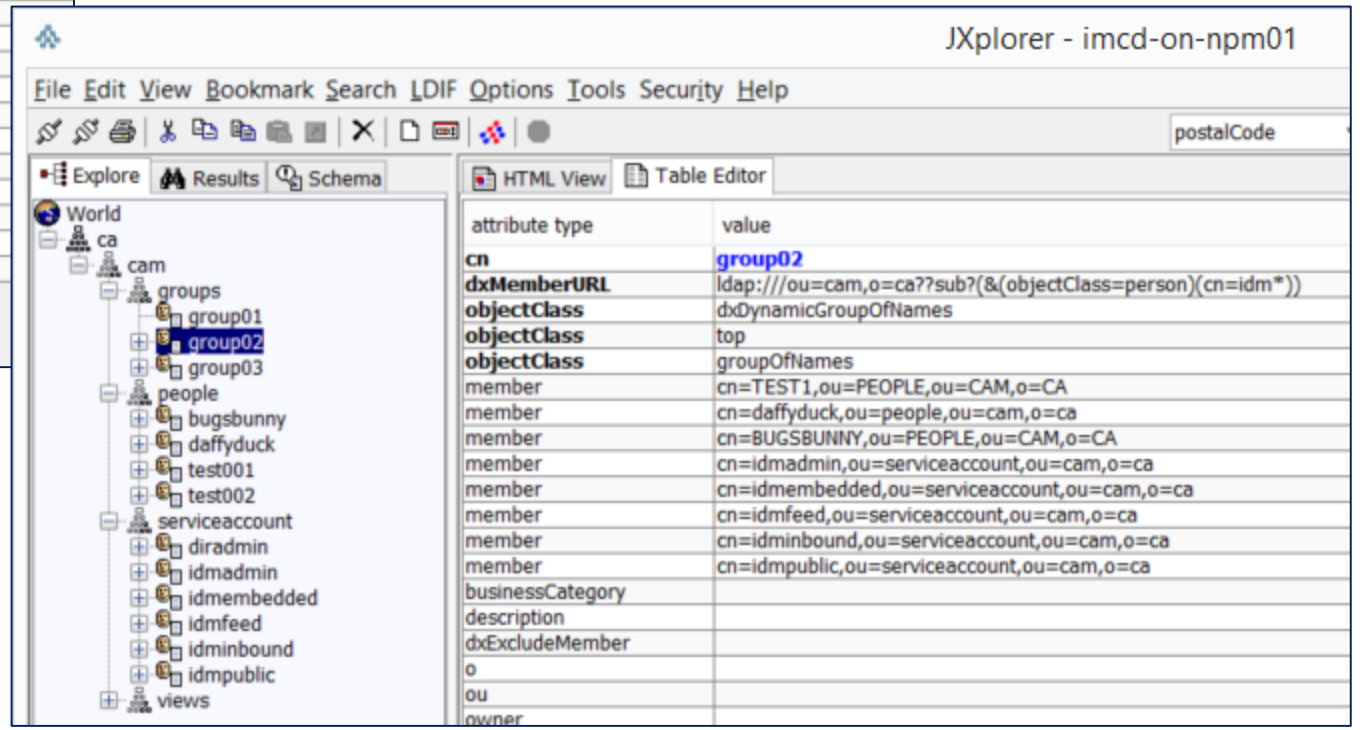


Step 09c: Validate Use-Case for Users Lookup

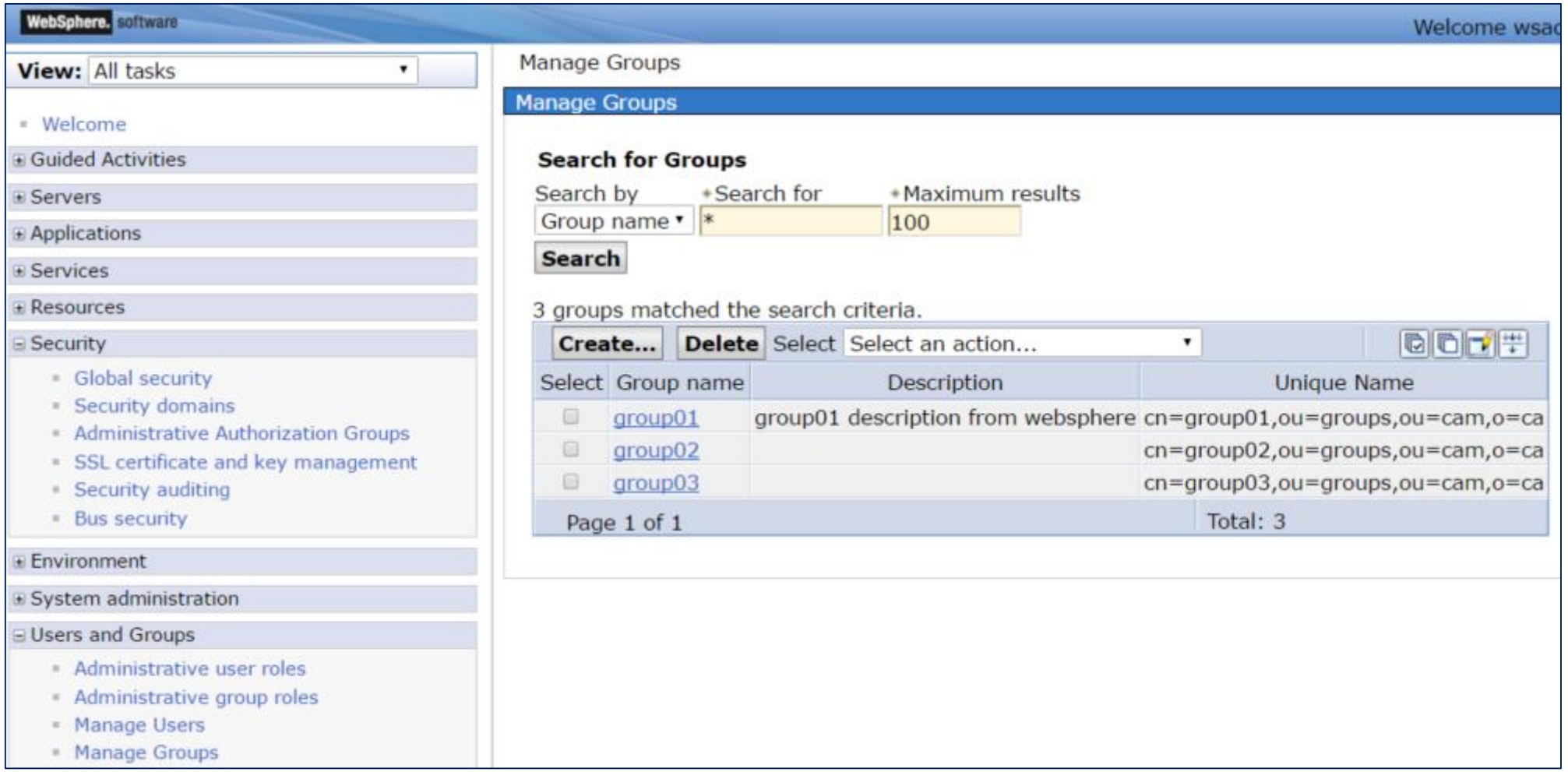


Step 10a: Validate Use-Case for Group Lookup

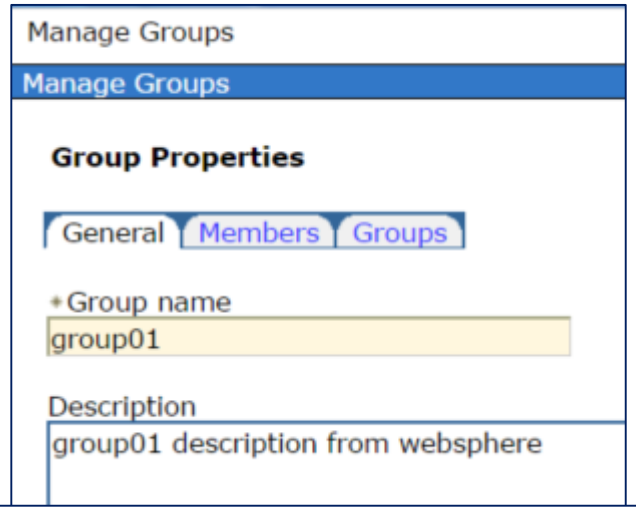


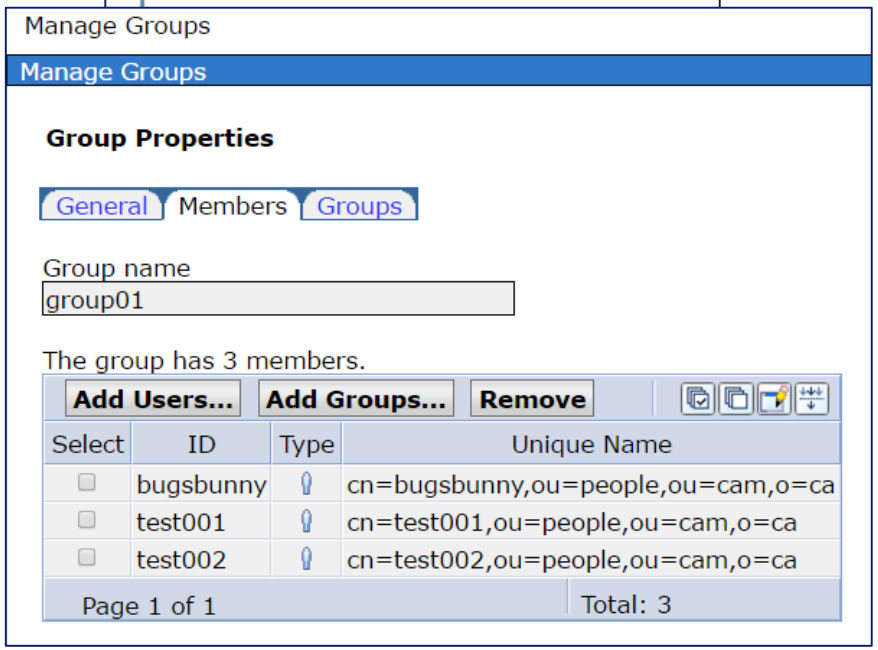


Step 10b: Validate Use-Case for Group Lookup



Step 10c: Validate Use-Case for Group Lookup



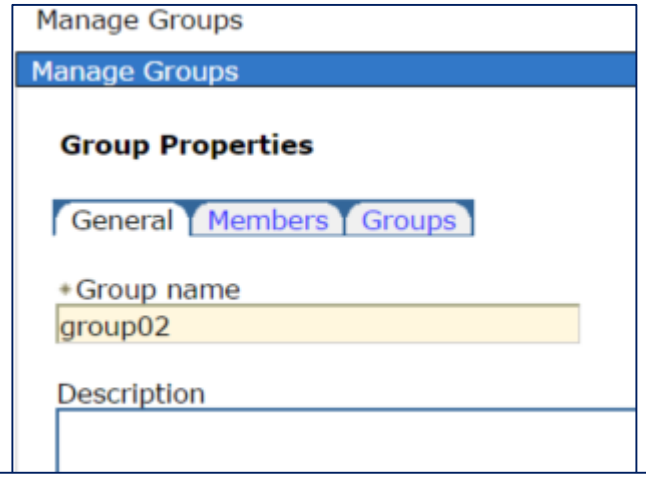


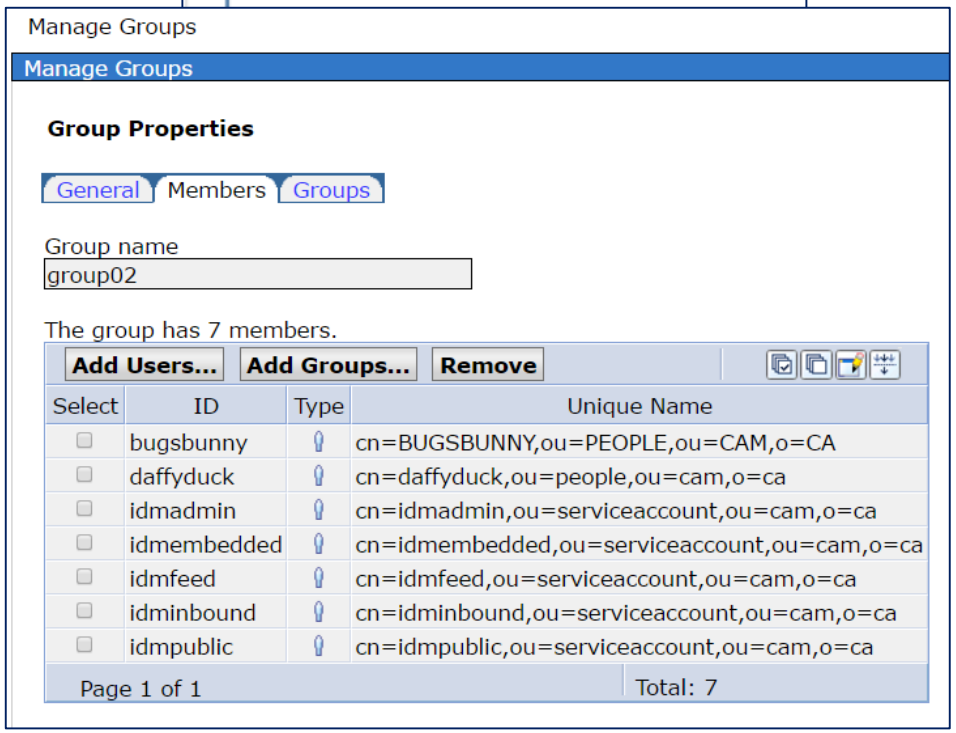
Note: Groups includes both STATIC and Dynamic Members

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

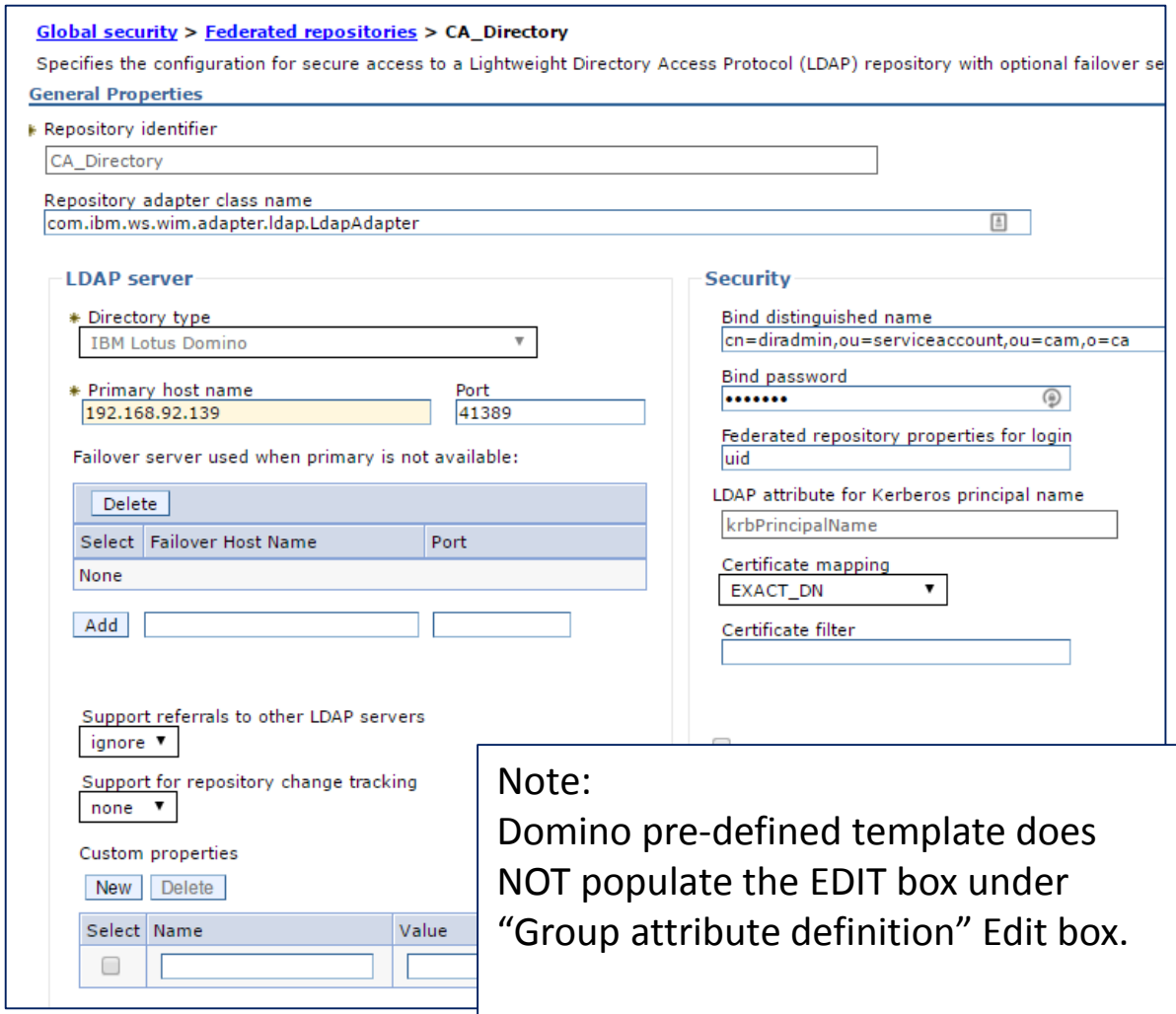
WAS does not require the static member to be in UPPER CASE to view or manage. Likely legacy behavior.

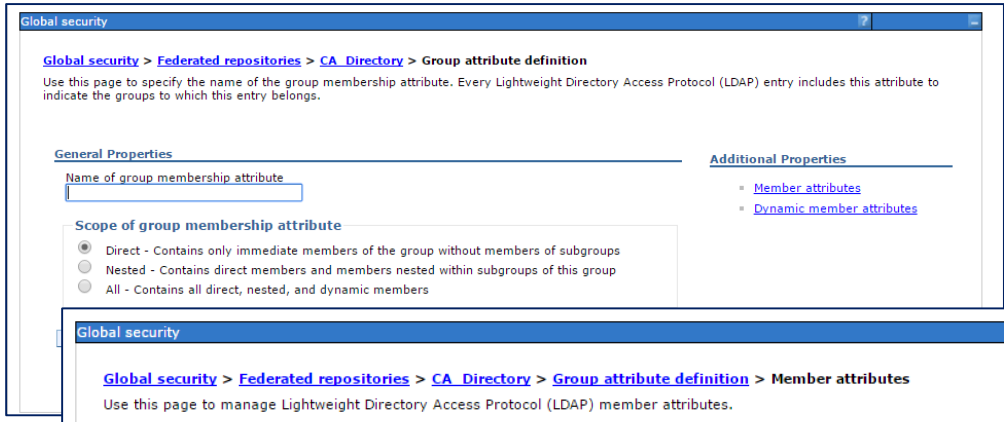
WAS does check if the Group member does exist. Any account that is listed as a member but with no UID, will not be displayed.

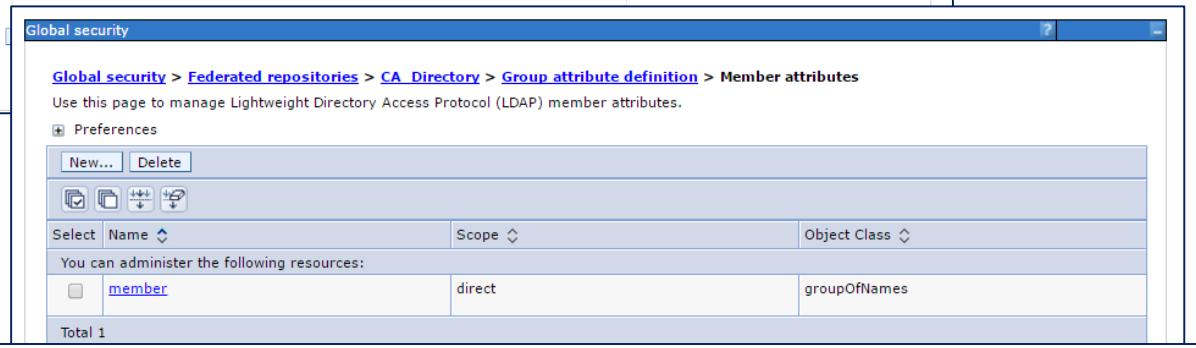


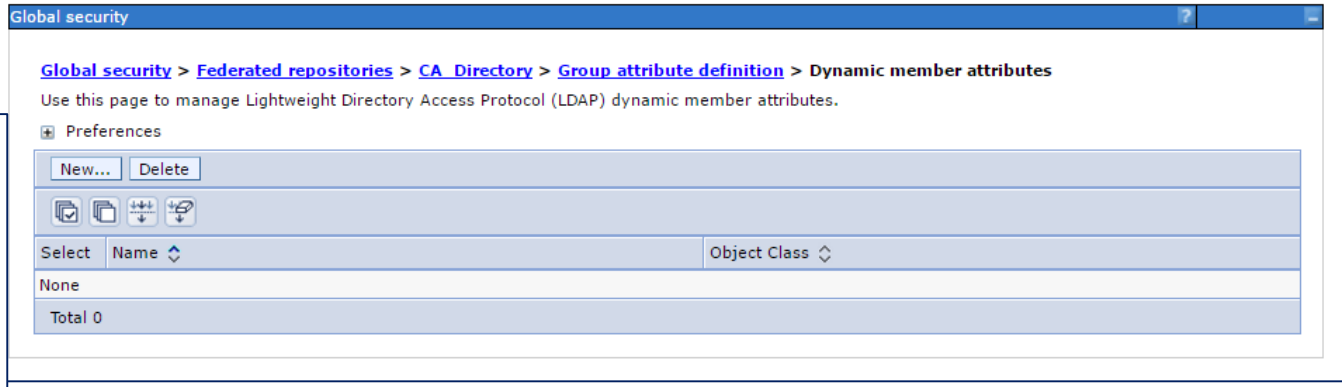


View Deltas – Between Working Domino vs Custom Type









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

View Deltas – Between Working Domino vs Custom Type

Search for Users

Search by: User ID | *Search for: * | *Maximum results: 100

Search

11 users matched the search criteria.

Create... | Delete | Select: Select an action...

Select	User ID	First name	Last name	E-mail	Unique Name
☐	bugsbunny	bugsbunny	bunny		cn=bugsbunny,ou=people,ou=cam,o=ca
☐	daffyduck	daffyduck	duck		cn=daffyduck,ou=people,ou=cam,o=ca
☐	diradmin	diradmin	diradmin		cn=diradmin,ou=serviceaccount,ou=cam,o=ca
☐	idmadmin	idmadmin	idmadmin		cn=idmadmin,ou=serviceaccount,ou=cam,o=ca
☐	idmembedded	idmembedded	idmembedded		cn=idmembedded,ou=serviceaccount,ou=cam,o=ca
☐	idmfeed	idmfeed	idmfeed		cn=idmfeed,ou=serviceaccount,ou=cam,o=ca
☐	idminbound	idminbound	idminbound		cn=idminbound,ou=serviceaccount,ou=cam,o=ca
☐	idmpublic	idmpublic	idmpublic		cn=idmpublic,ou=serviceaccount,ou=cam,o=ca
☐	test001	test001	test001		cn=test001,ou=people,ou=cam,o=ca
☐	test002	test002	test002		cn=test002,ou=people,ou=cam,o=ca
☐	wsadmin	wsadmin	wsadmin		uid=wsadmin,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.

Add Users... | Add Groups... | Remove

Select	ID	Type	Unique Name
☐	bugsbunny		cn=bugsbunny,ou=people,ou=cam,o=ca
☐	test001		cn=test001,ou=people,ou=cam,o=ca
☐	test002		cn=test002,ou=people,ou=cam,o=ca

Page 1 of 1 — Total: 3

Manage Groups

Group Properties

General | Members | Groups

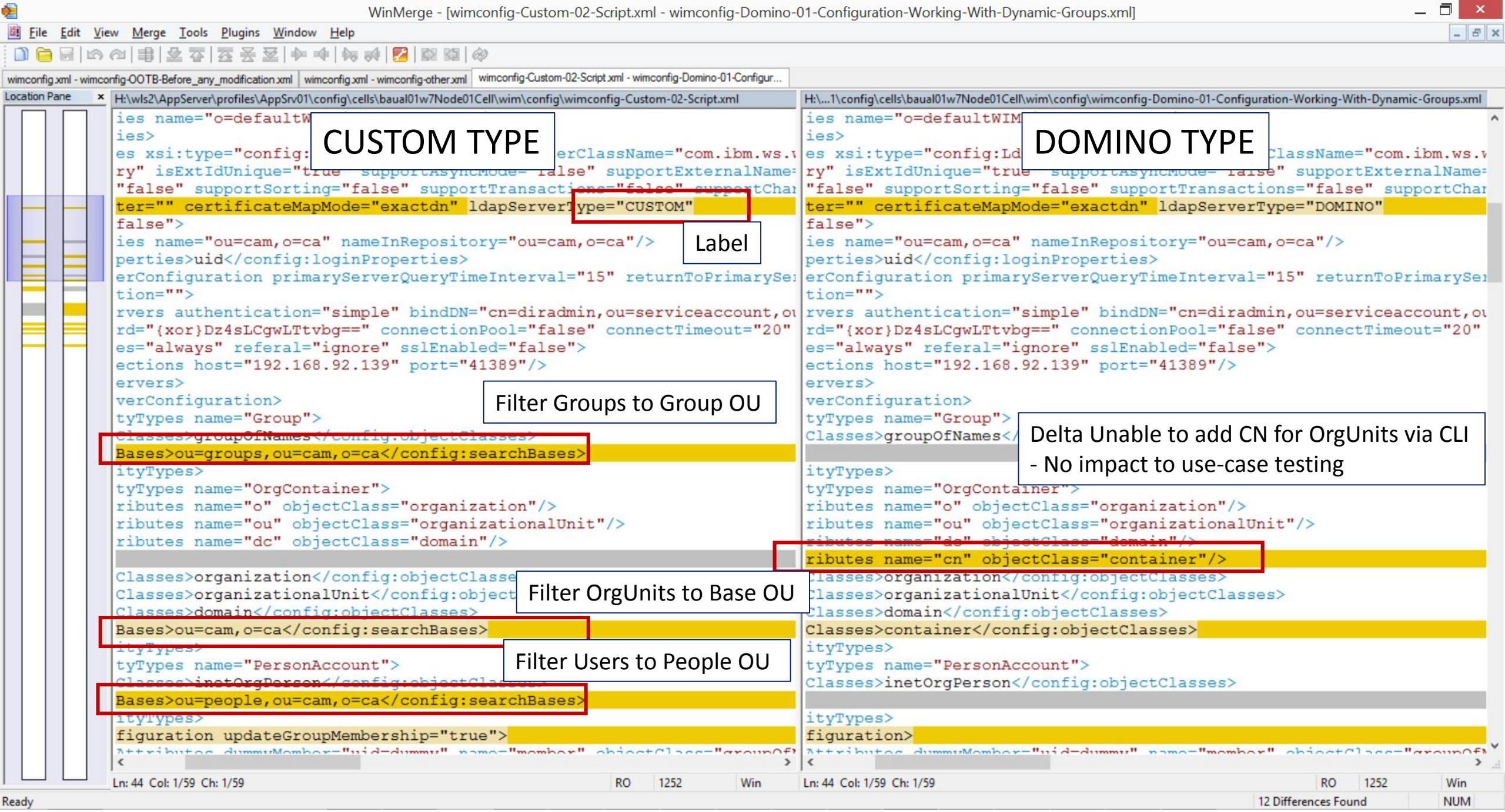
Group name: group02

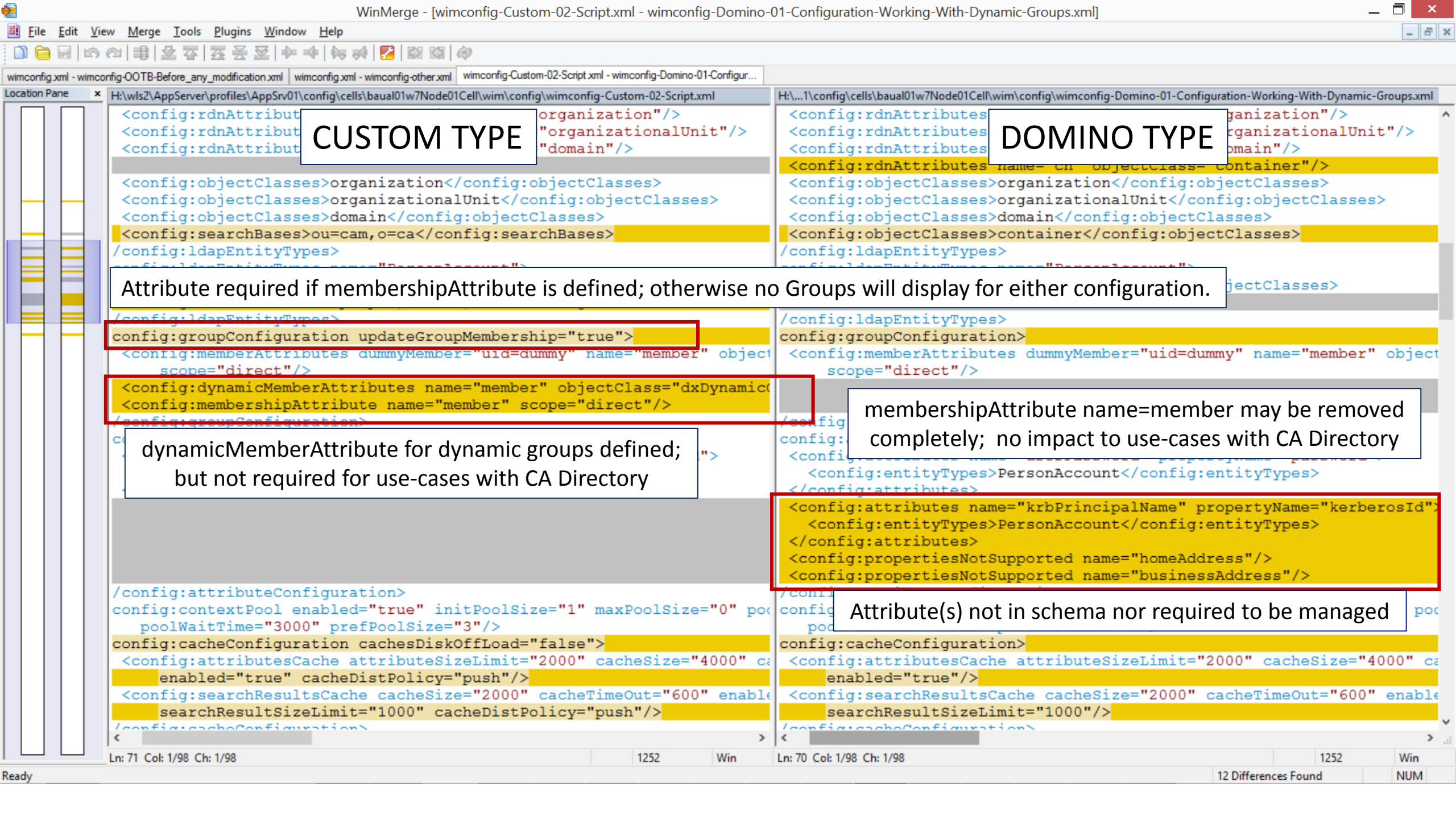
The group has 7 members.

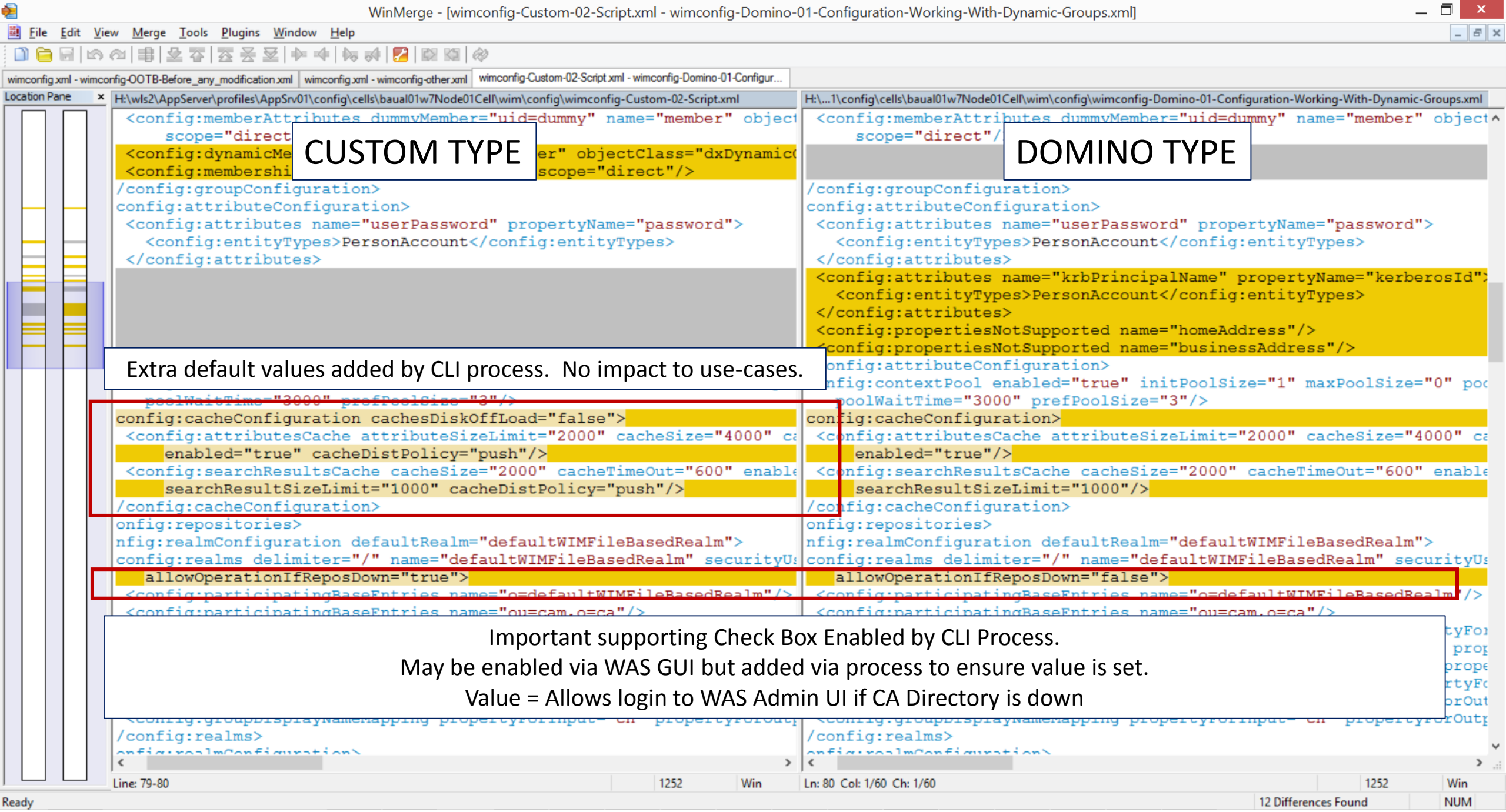
Add Users... | Add Groups... | Remove

Select	ID	Type	Unique Name
☐	bugsbunny		cn=BUGSBUNNY,ou=PEOPLE,ou=CAM,o=CA
☐	daffyduck		cn=daffyduck,ou=people,ou=cam,o=ca
☐	idmadmin		cn=idmadmin,ou=serviceaccount,ou=cam,o=ca
☐	idmembedded		cn=idmembedded,ou=serviceaccount,ou=cam,o=ca
☐	idmfeed		cn=idmfeed,ou=serviceaccount,ou=cam,o=ca
☐	idminbound		cn=idminbound,ou=serviceaccount,ou=cam,o=ca
☐	idmpublic		cn=idmpublic,ou=serviceaccount,ou=cam,o=ca

Page 1 of 1 — Total: 7


WinMerge - [wimconfig-Custom-02-Script.xml - wimconfig-Domino-01-Configuration-Working-With-Dynamic-Groups.xml]
File Edit View Merge Tools Plugins Window Help
wimconfig.xml - wimconfig-OOTB-Before_any_modification.xml
wimconfig.xml - wimconfig-other.xml
wimconfig-Custom-02-Script.xml - wimconfig-Domino-01-Configur...
Location Pane
H:\wls2\AppServer\profiles\AppSrv01\config\cells\baual01w7Node01Cell\wim\config\wimconfig-Custom-02-Script.xml
H:\...1\config\cells\baual01w7Node01Cell\wim\config\wimconfig-Domino-01-Configuration-Working-With-Dynamic-Groups.xml
CUSTOM TYPE
DOMINO TYPE
ldapServerType="CUSTOM"
ldapServerType="DOMINO"
Label
Filter Groups to Group OU
Bases>ou=groups,ou=cam,o=ca</config:searchBases>
Filter OrgUnits to Base OU
Bases>ou=cam,o=ca</config:searchBases>
Filter Users to People OU
Bases>ou=people,ou=cam,o=ca</config:searchBases>
Delta Unable to add CN for OrgUnits via CLI
- No impact to use-case testing
ributes name="cn" objectClass="container"/>
Classes>container</config:objectClasses>
Ln: 44 Col: 1/59 Ch: 1/59
RO
1252
Win
Ready
12 Differences Found
NUM


WinMerge - [wimconfig-Custom-02-Script.xml - wimconfig-Domino-01-Configuration-Working-With-Dynamic-Groups.xml]
File Edit View Merge Tools Plugins Window Help
wimconfig.xml - wimconfig-OOTB-Before_any_modification.xml
wimconfig.xml - wimconfig-other.xml
wimconfig-Custom-02-Script.xml - wimconfig-Domino-01-Configur...
Location Pane
H:\wls2\AppServer\profiles\AppSrv01\config\cells\baual01w7Node01Cell\wim\config\wimconfig-Custom-02-Script.xml
H:\...1\config\cells\baual01w7Node01Cell\wim\config\wimconfig-Domino-01-Configuration-Working-With-Dynamic-Groups.xml
CUSTOM TYPE
DOMINO TYPE
Attribute required if membershipAttribute is defined; otherwise no Groups will display for either configuration.
dynamicMemberAttribute for dynamic groups defined; but not required for use-cases with CA Directory
membershipAttribute name=member may be removed completely; no impact to use-cases with CA Directory
Attribute(s) not in schema nor required to be managed
Ln: 71 Col: 1/98 Ch: 1/98
1252
Win
Ln: 70 Col: 1/98 Ch: 1/98
1252
Win
Ready
12 Differences Found
NUM


WinMerge - [wimconfig-Custom-02-Script.xml - wimconfig-Domino-01-Configuration-Working-With-Dynamic-Groups.xml]
File Edit View Merge Tools Plugins Window Help
wimconfig.xml - wimconfig-OOTB-Before_any_modification.xml
wimconfig.xml - wimconfig-other.xml
wimconfig-Custom-02-Script.xml - wimconfig-Domino-01-Configur...
Location Pane
H:\wls2\AppServer\profiles\AppSrv01\config\cells\baual01w7Node01Cell\wim\config\wimconfig-Custom-02-Script.xml
H:\...1\config\cells\baual01w7Node01Cell\wim\config\wimconfig-Domino-01-Configuration-Working-With-Dynamic-Groups.xml
CUSTOM TYPE
DOMINO TYPE
Extra default values added by CLI process. No impact to use-cases.
Important supporting Check Box Enabled by CLI Process.
May be enabled via WAS GUI but added via process to ensure value is set.
Value = Allows login to WAS Admin UI if CA Directory is down
Line: 79-80
1252
Win
Ln: 80 Col: 1/60 Ch: 1/60
1252
Win
Ready
12 Differences Found
NUM