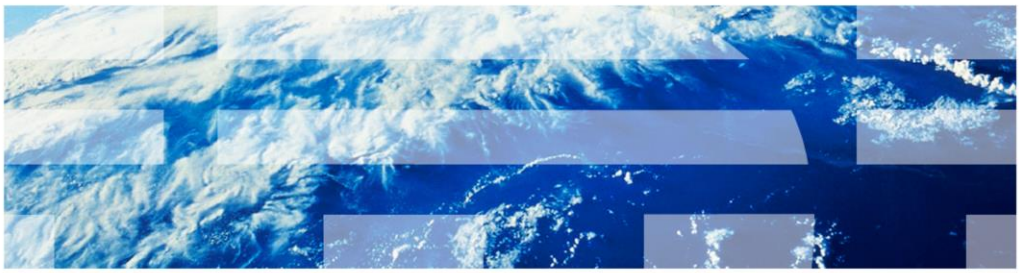
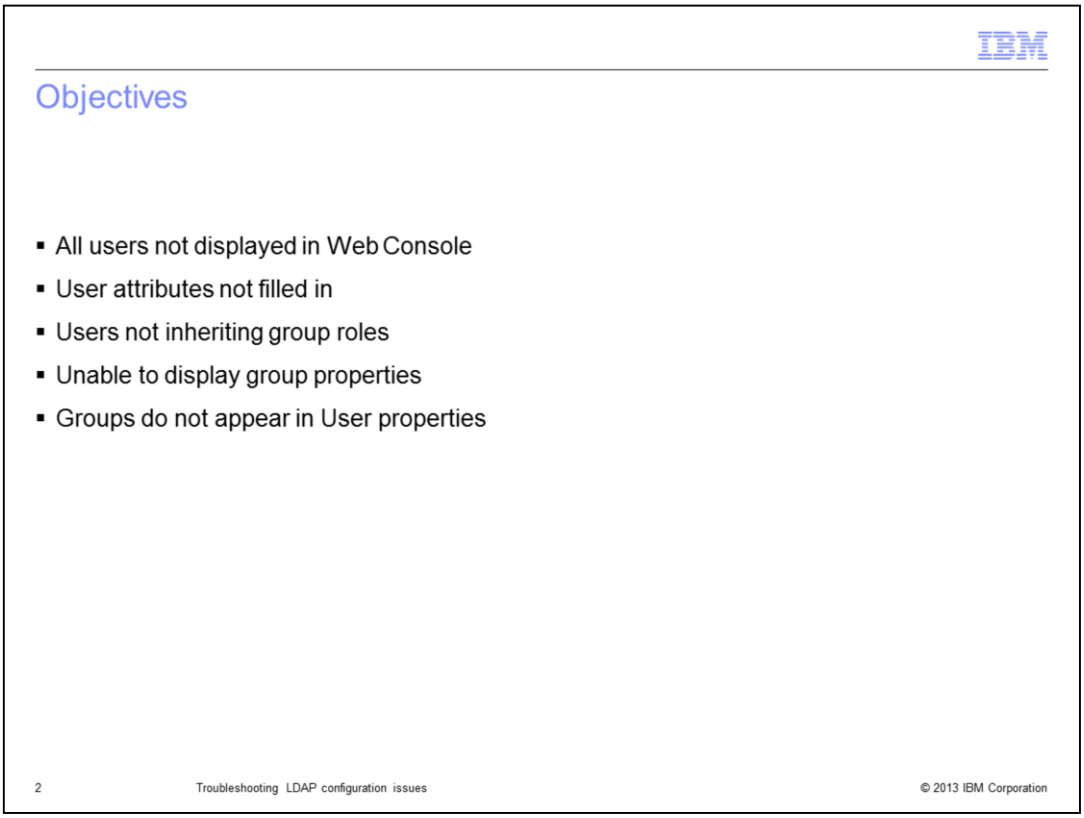
IBM

InfoSphere Information Server

Troubleshooting LDAP configuration issues with Information Server version 8



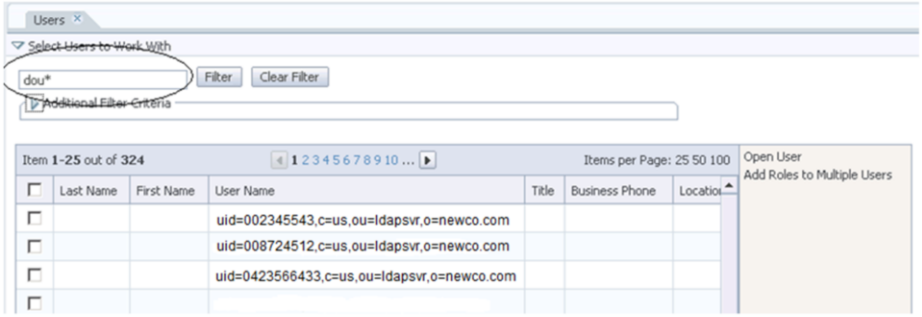
This presentation will discuss some common configuration issues when using a Lightweight Directory Access Protocol user registry with Information Server version 8. Lightweight Directory Access Protocol is referred to as LDAP throughout this presentation.



The objectives of this presentation are to discuss how to troubleshoot issues where all of the LDAP users are not displayed in the Information Server Web Console, the user attributes such as first and last name are not filled in and the users are not inheriting the group roles. Also, group properties will not display properly and groups are not appearing in the user's properties.

All users not displayed in Web Console (1 of 4)

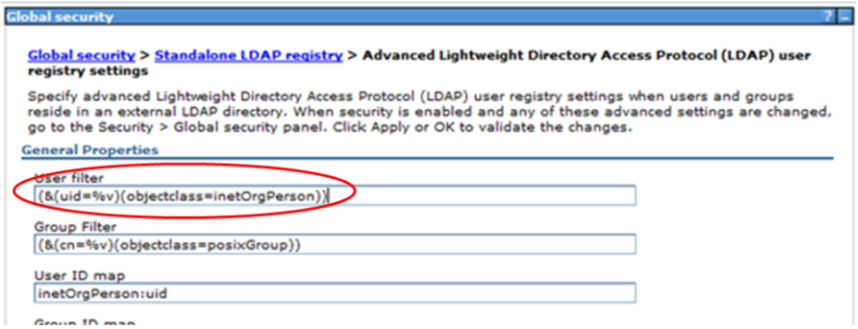
- Web Console does not display all users when configured for LDAP
- Directory service limits number of LDAP users to first 1000 users that it retrieves
- 1000 users retrieved are based on filter criteria



The first issue this presentation will discuss is an issue where LDAP is configured but not all of the users are displayed in the Information Server Web Console. For efficiency purposes, the directory service limits the number of LDAP users to the first 1000 users that it retrieves. The 1000 users that are retrieved are based on filter criteria set in the main filter, as displayed on this slide.

All users not displayed in Web Console (2 of 4)

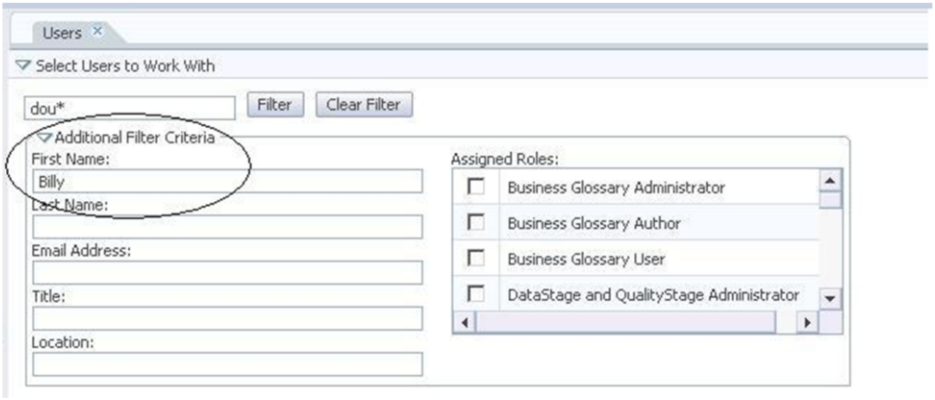
- Check user filter in your WebSphere® LDAP configuration
  - User filter determines LDAP attribute filtered
  - uid by default



Check your user filter in your WebSphere LDAP configuration to determine which LDAP entry the filter is using. The default is normally uid.

All users not displayed in Web Console (3 of 4)

- Additional Filter Criteria
  - Applies to 1000 users already retrieved
  - Has no effect on initial users retrieved

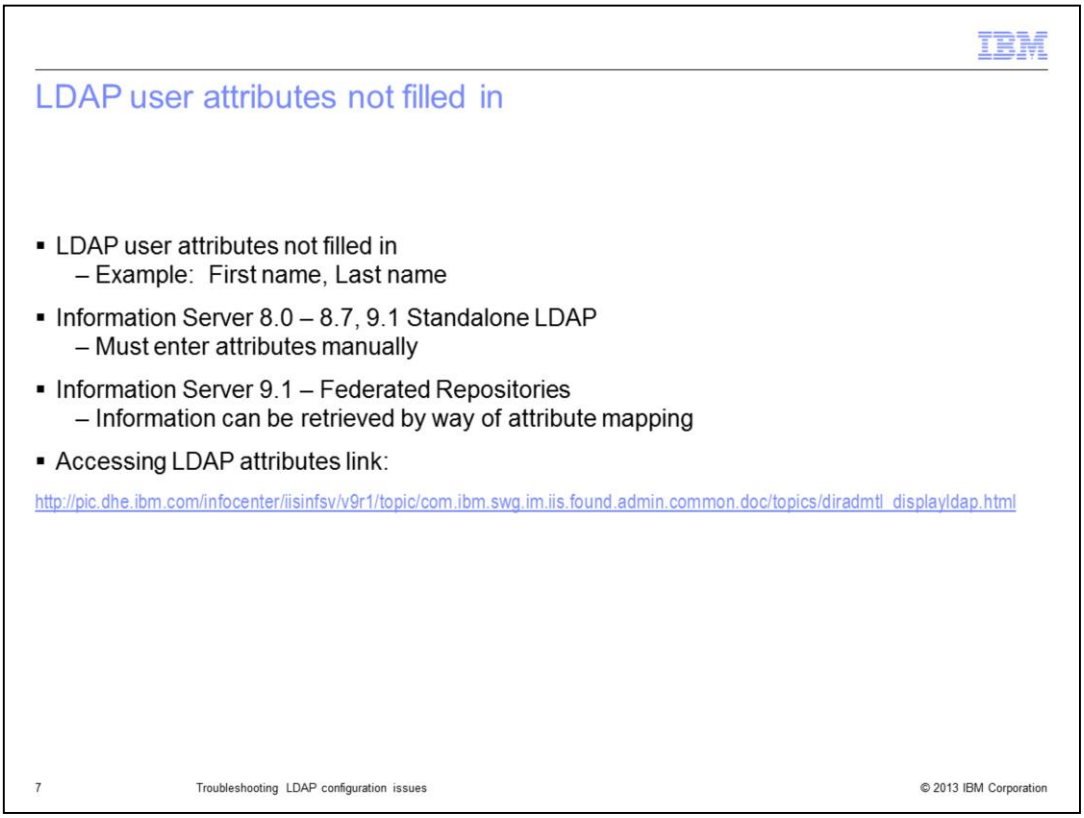


The user list can also be filtered using the Additional Filter Criteria. The difference here is that this filter only applies to the 1000 users that have already been retrieved. It does not effect the initial 1000 users selected.

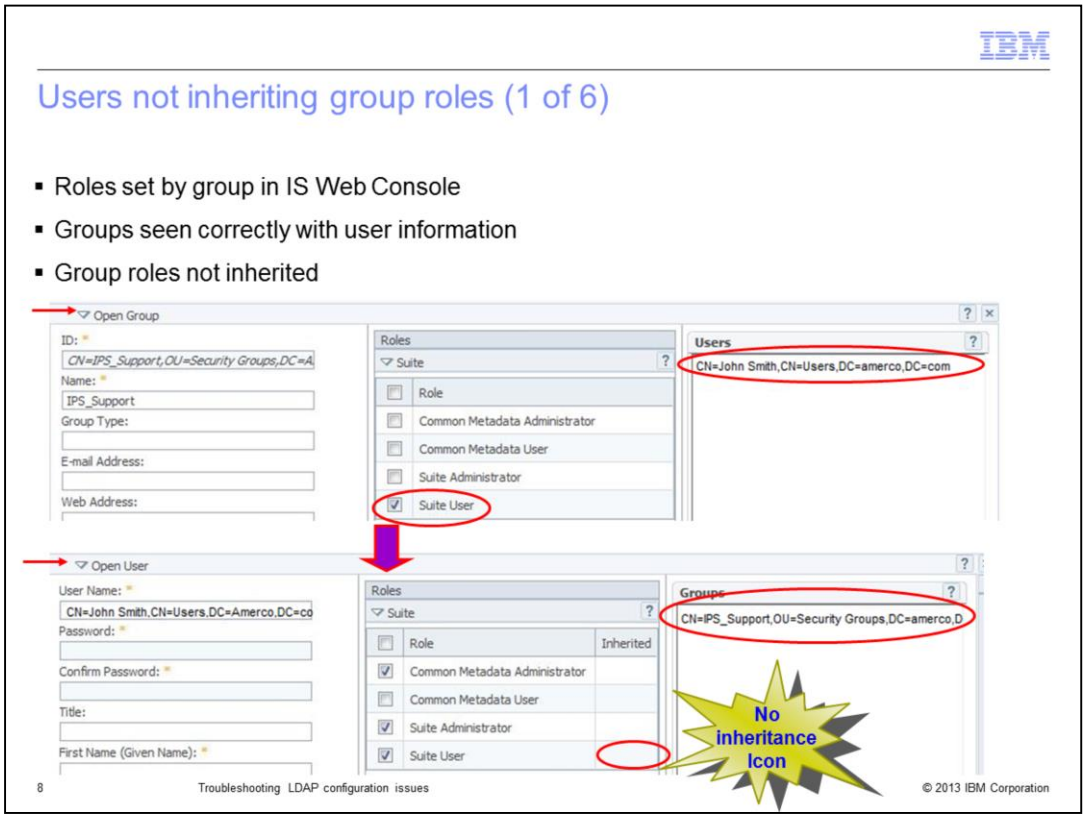
All users not displayed in Web Console (4 of 4)

- Search criteria can be modified
  - Edit User filter
  - Add additional search criteria
- Example
  - Searches on uid or sn (last name)
- IBM Education Assistant module on Advanced LDAP Filtering techniques to minimize InfoSphere® Information Server user list:
  http://www.ibm.com/support/docview.wss?uid=swg27023908

The search criteria for the main filter that effects the initially selected users can be modified to search by an attribute other than the uid. In this example, the filter was modified to allow it to search on either the uid or the sn. sn is normally mapped to the user's last name. See the IBM Education Assistant module on Advanced LDAP Filtering techniques to minimize the Information Server user list for further information on how to set the user filter.

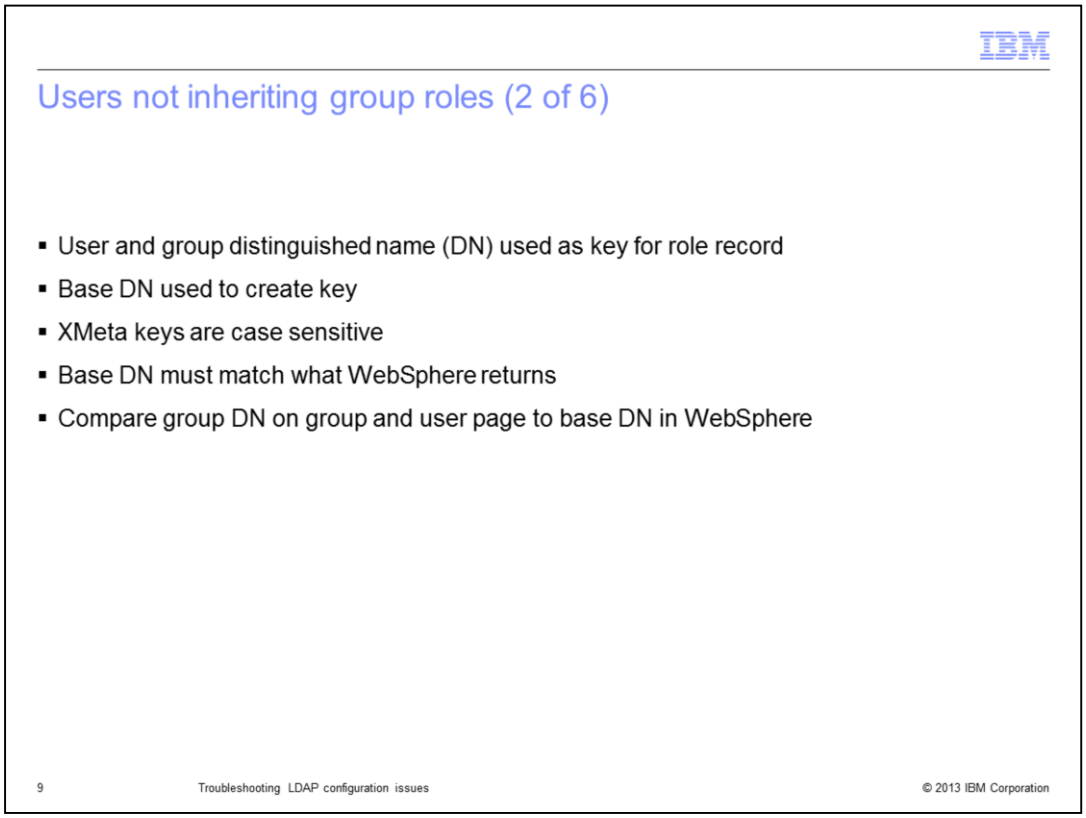


Another common issue is that many of the LDAP attributes, such as first and last name, are not automatically filled in in the user information in the Information Server Web Console. For Information Server version 8.0 through 8.7 and Information Server version 9.1 using a stand-alone LDAP registry, this is not possible. Instead, the attributes must be manually entered. Configuring Information Server version 9.1 to use Federated Repositories will allow the administrator to map Information Server attributes, such as first and last name, to LDAP attributes. This mapping will automatically fill in the user information in the Information Server Web Console.

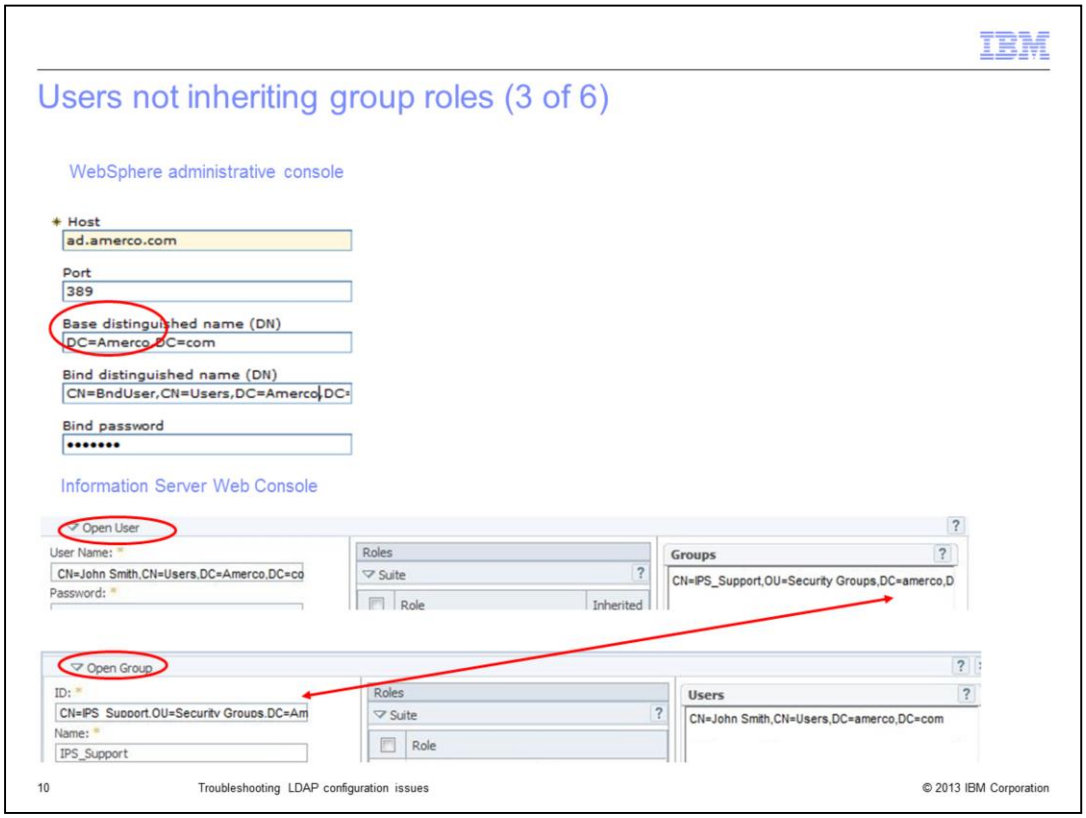


The next issue this presentation will discuss is an issue where the Information Server roles are assigned at the group level in the Information Server Web Console but are not inherited by the users who are members of that group. In the example displayed on this slide, the group IPS_Support has the Suite User role assigned to it. In the group properties, the user John Smith shows up as a member of the IPS_Support group.

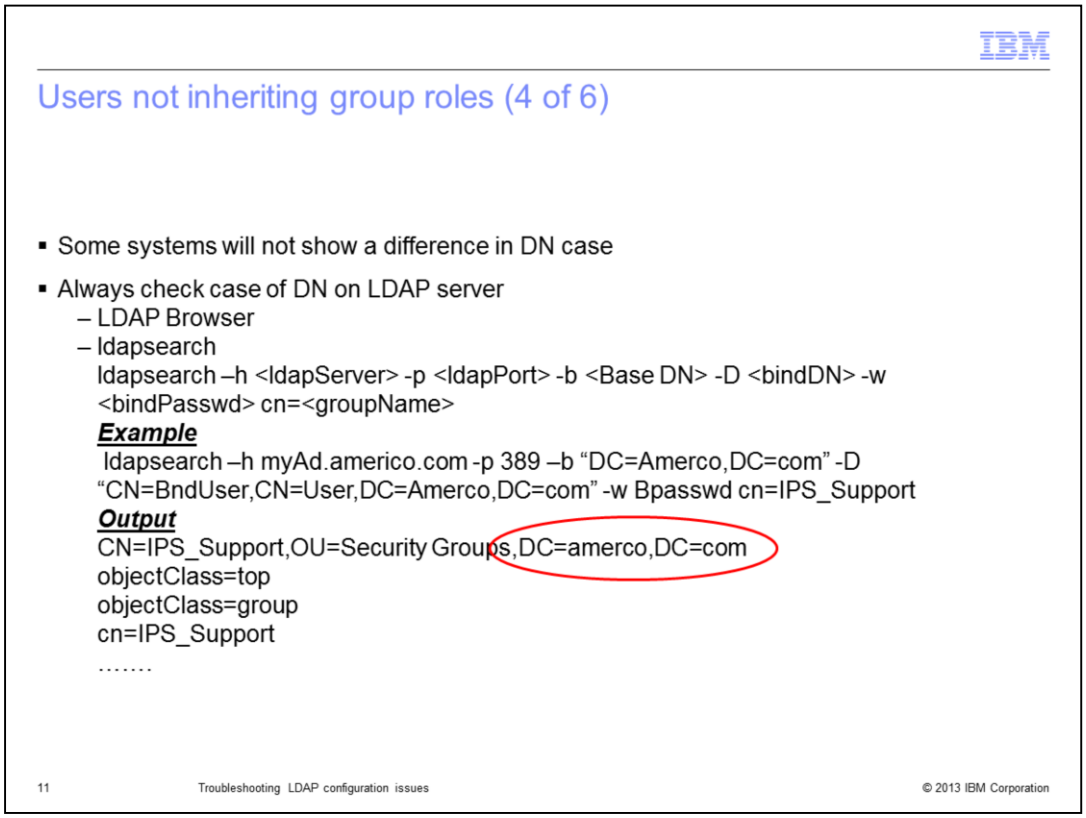
When the user properties for John Smith are opened in the Web Console, the list of groups that he is a member of correctly displays the IPS_Support group but the icon indicating the Suite User roles that is inherited from the group, is not displayed.



When roles are assigned to users and groups in the Information Server Web Console, the distinguished name for the user or group is used as the key for the role record when it is saved into XMeta. When the key is created, the base DN that is set in the LDAP configuration is used. Information Server keys in XMeta are case sensitive and if the case of the base DN does not match the case that is returned from WebSphere, Information Server is not able to find the group role record in XMeta. Compare the group's distinguished name that is displayed on the right side of the user's property box to the group's distinguished name displayed in the ID field of the group properties.



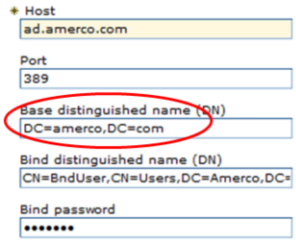
In the example displayed on this slide, the base DN in the LDAP configuration in WebSphere is incorrectly set to DC=Amerco,DC=com where the “A” in Amerco is uppercase. When the User’s properties are displayed in the Information Server Web Console, the groups that the user is a member of are displayed on the right side of the screen. The group’s distinguished name in the user properties has a lower case “a” in amerco. When the group properties are displayed for this group, the ID, which is the distinguished name of the group, uses the same uppercase A as the Base DN set in the WebSphere configuration. Since Information Server is case sensitive, when it queries for the group roles, it looks for a group ID using the distinguished name that shows up with the user properties. Since the case is different than how the roles for the group are actually saved, it is unable to find the roles that were set for the group.



It is important to note that on some systems the group DN will show in the users properties with the same case as the ID for the group. In either case, use an LDAP browser or a tool such as ldapsearch to retrieve the proper case from the LDAP server.

Users not inheriting group roles (5 of 6)

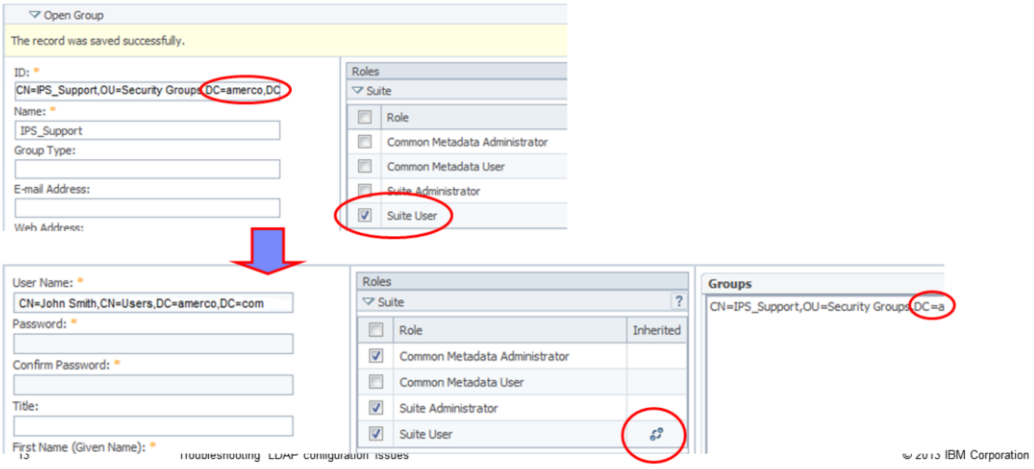
- Update LDAP configuration with correct case for base DN
- Stop and restart WebSphere
- Administrative user may not be able to login to Web Console
  - Run DirectoryAdmin to reset administrative roles
    <IS_Home>/ASBServer/bin/DirectoryAdmin.sh –admin –user –userid ISadminDN
    - ISadminDN = Fully distinguished name for Information Server administrative user
    - Case of DN must match



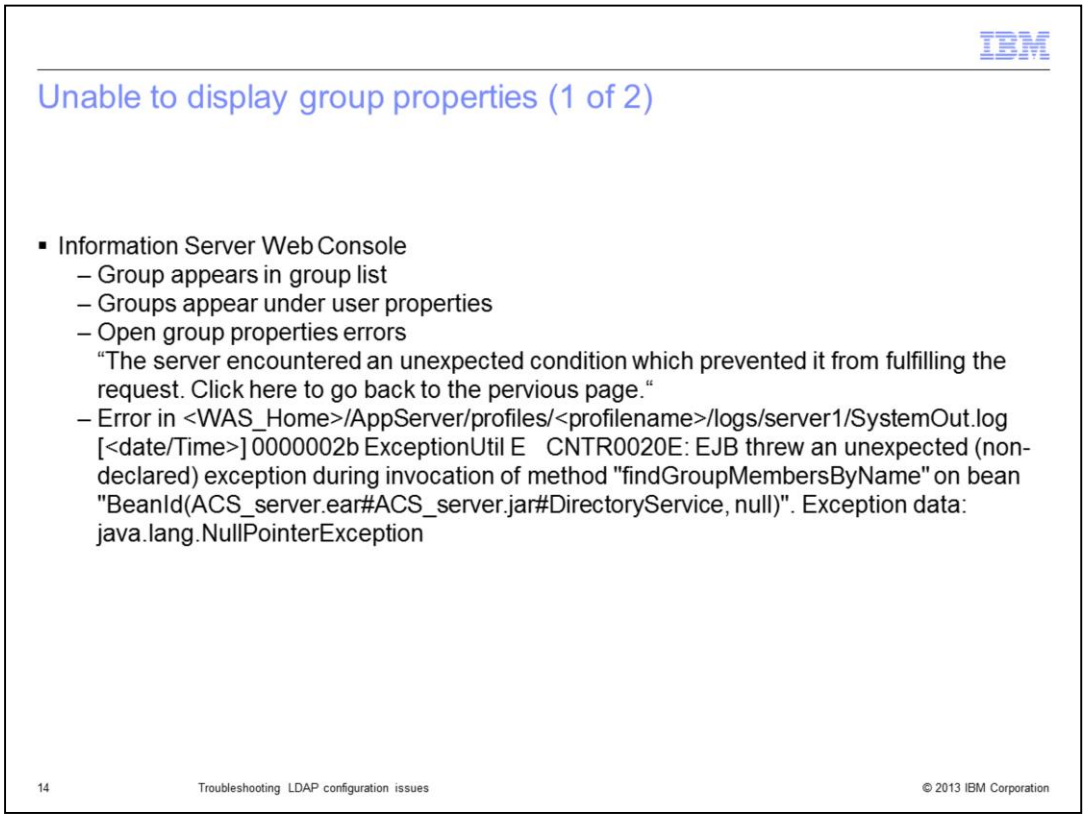
Once the proper case is determined, open the WebSphere Administrative Console and change the Base DN in the LDAP configuration to match the case returned by the LDAP server. Stop and restart the WebSphere server for the changes to take effect. Since the ID of the Information Server users are also case sensitive, the Information Server administrative user's login to the Information Server Web Console may now fail with an Access Denied error because the user no longer has the administrative roles. Information Server is searching for an ID with the new base DN but the roles are saved with the old DN. In this case, run the DirectoryAdmin command as shown on this slide to add the administrative user back in. Be sure to enter the administrative user's fully distinguished name in the proper case.

Users not inheriting group roles (6 of 6)

- Reassign roles to group
- Roles correctly shows as inherited



The last step is to go back into the Web Console and reassign the roles to the appropriate groups. In this example, the base portion of the groups distinguished name now matches in the group ID field and in the user's properties. When the roles are reset on the group, the roles are correctly inherited by the user.



The next issue that may be seen in the Information Server Web Console, is an issue where the group properties will not display. When the Web Console is opened, and groups is clicked, the list of groups is correctly displayed. If a group is selected and open group is clicked, an error is received: “The server encountered an unexpected condition which prevented it from fulfilling the request. Click here to go back to the pervious page.”

If a user’s property page is opened instead, the groups are correctly listed on the right side of the screen. Examine the SystemOut.log file and look for an error during the invocation of the method “findGroupMembersByName” and look to see if there is a NullPointerException error. If this is the case, then the issue is a null user ID in the registry.

Unable to display group properties (2 of 2)

- Null user ID exists in registry
- Obtain DeleteUser tool from Support
  - Client side tool
- Check if null user exists
  C:\IBM\InformationServer\ASBNode\bin>.\DeleteUser -user <isadmin> -password <AdminPasswd> -server <Server> -port <Port> -listall -find (null)

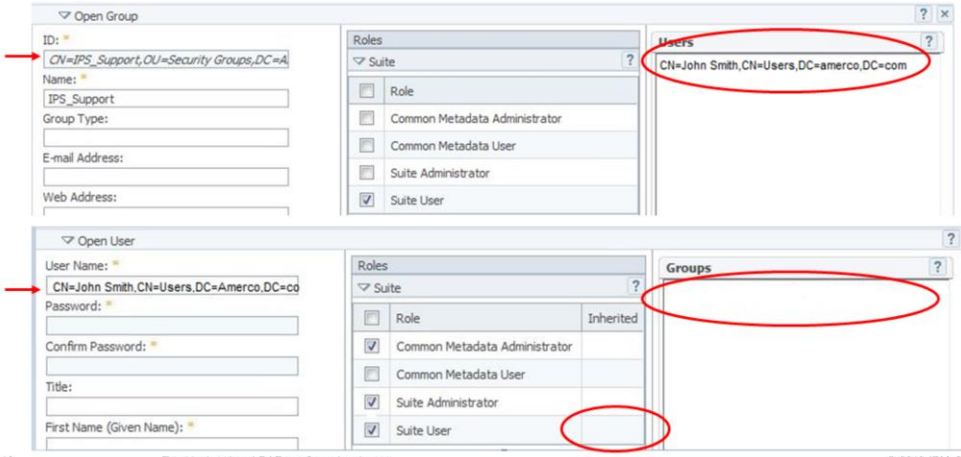
  1 total users found.
  (null) :: (null) :: Security Directory
- Remove null user
  C:\IBM\InformationServer\ASBNode\bin>.\DeleteUser -user <isadmin> -password <AdminPassword> -server <Server> -port 9080 -delete (null)

  Deleting user (null)...
- <Server> = Name of Services Tier server

The first step is to obtain the DeleteUser tool from Customer Support. Once DeleteUser is installed per the readme file, run the command to check if a null user exists in the repository. If it finds a null user, remove it by running DeleteUser again with the –delete argument as displayed on this slide. This will correct the issue.

Groups do not appear in User properties (1 of 7)

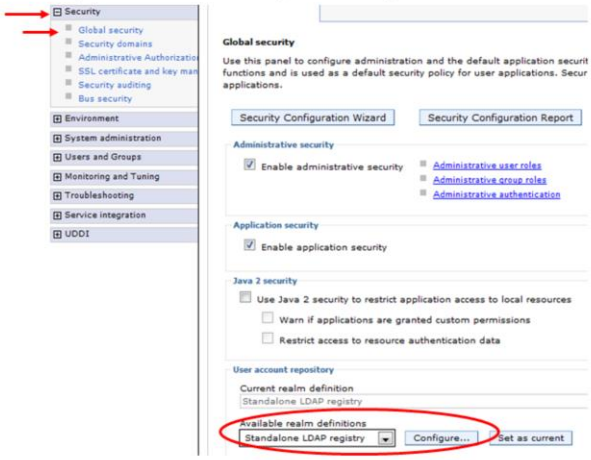
- Users show up in group property list
- Groups do not show up in user property list
- Group roles are not inherited



The next issue that this presentation will discuss is an issue where the groups a user belongs to do not appear in the Groups box on the right side of the user's property page. When the properties for a group are opened, the users in that group are correctly displayed in the Users box on the right side of the page. If the properties for a user in that list is opened, the group does not appear in the Groups box and the roles are not inherited by the user.

Groups do not appear in User properties (2 of 7)

- Check LDAP filters
  - Group member ID map
- Standalone LDAP
  - Security => Global Security => Configure



This issue generally occurs when the Group member ID map is set incorrectly. To correct this when using Standalone LDAP, open the WebSphere Administrative Console, go to Security, Global security, and click Configure.

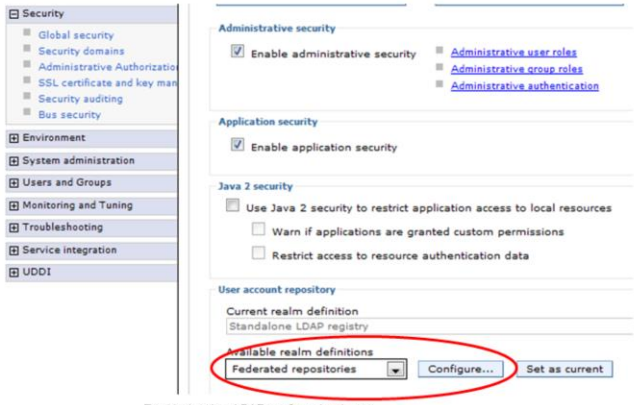
Groups do not appear in User properties (3 of 7)

- Additional properties => Advanced LDAP user registry settings
- Correct Group member ID map
- Save and restart WebSphere

Next, under Additional properties, click Advanced user registry settings. Look at the Group member ID map and verify with your LDAP administrator that this value is correct for your configuration, update the group member ID map, save, and restart WebSphere.

Groups do not appear in User properties (4 of 7)

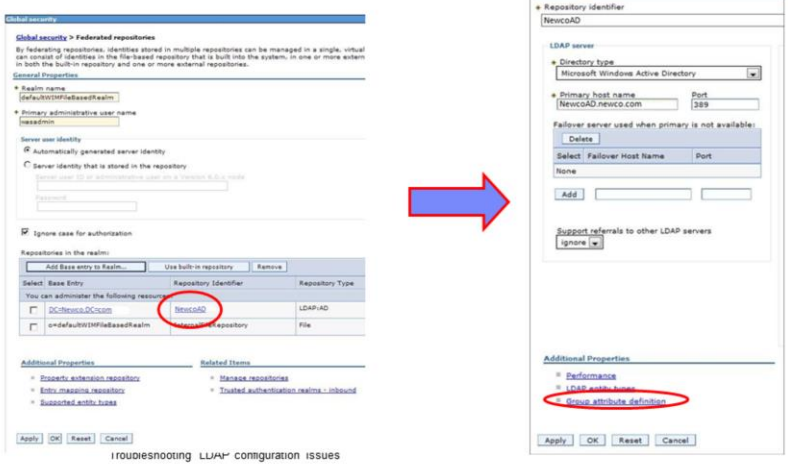
- Federated Repositories
  - Security => Global Security => Configure



When using Federated Repositories, go into Security, Global Security, select Federated repositories under the Available realm definition and click Configure.

Groups do not appear in User properties (5 of 7)

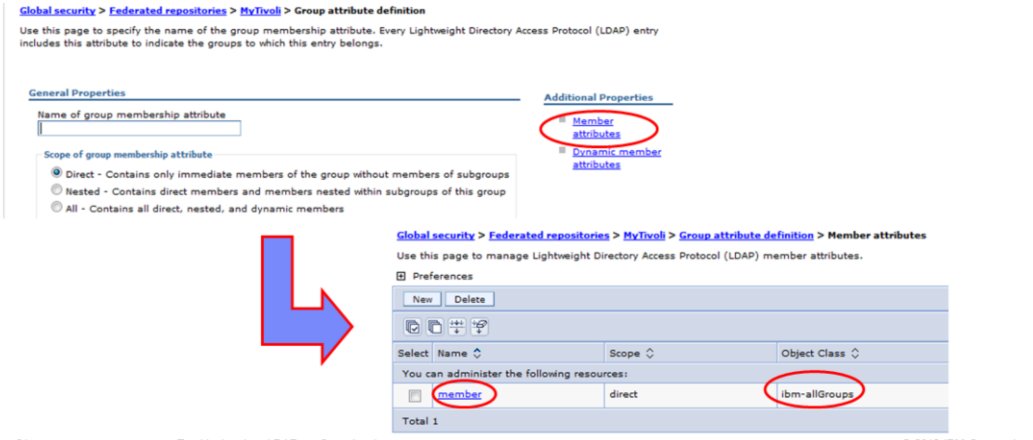
- Click Repository identifier
- Click Group attribute definition



Next, click the Repository identifier for the repository with the issue. Click Group attribute definition under Additional Properties.

Groups do not appear in User properties (6 of 7)

- Click Member Attributes
- Check name and object class
  - Click Name to change object class
  - Delete and Add to change name and object class

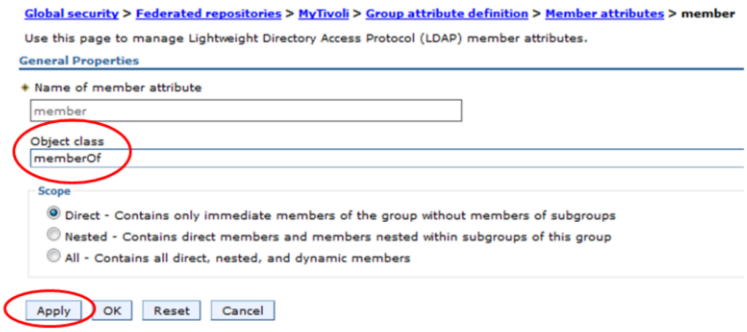


21 Troubleshooting LDAP configuration issues

Next, click Member Attributes under additional properties. This will show you the attribute name and object class. Check with your LDAP administrator for the correct values. You can change the object class of the existing attribute if the name is correct, or delete the current attribute and add a new one if the name is incorrect. If the attribute name is correct, click the attribute name to change the object class.

Groups do not appear in User properties (7 of 7)

- Correct object class
- Click Apply
- Restart WebSphere



Type in the correct object class and click Apply and Save at the top of the screen. WebSphere must be restarted for the changes to take effect.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, InfoSphere, 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 other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

Other company, product, or service names may be trademarks or service marks of others.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.