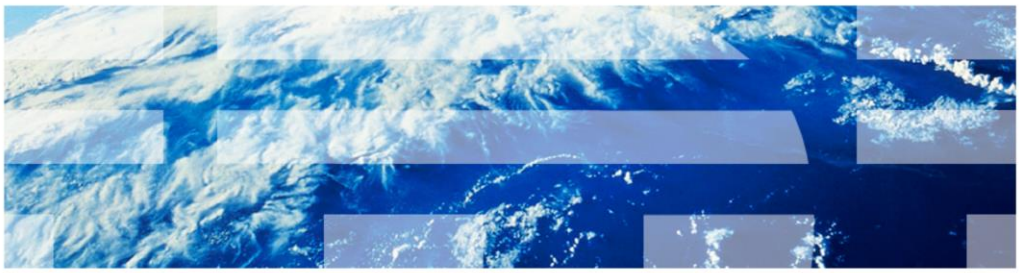
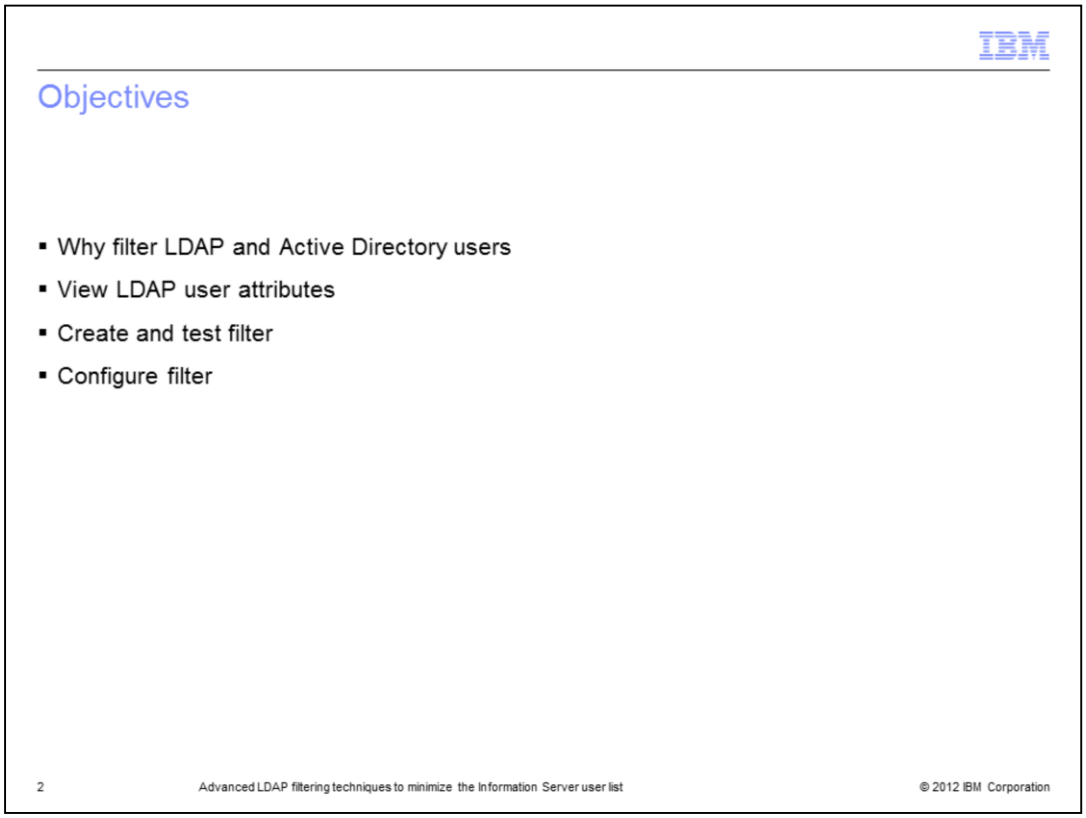
IBM

InfoSphere Information Server

Advanced LDAP filtering techniques to minimize the Information Server user list

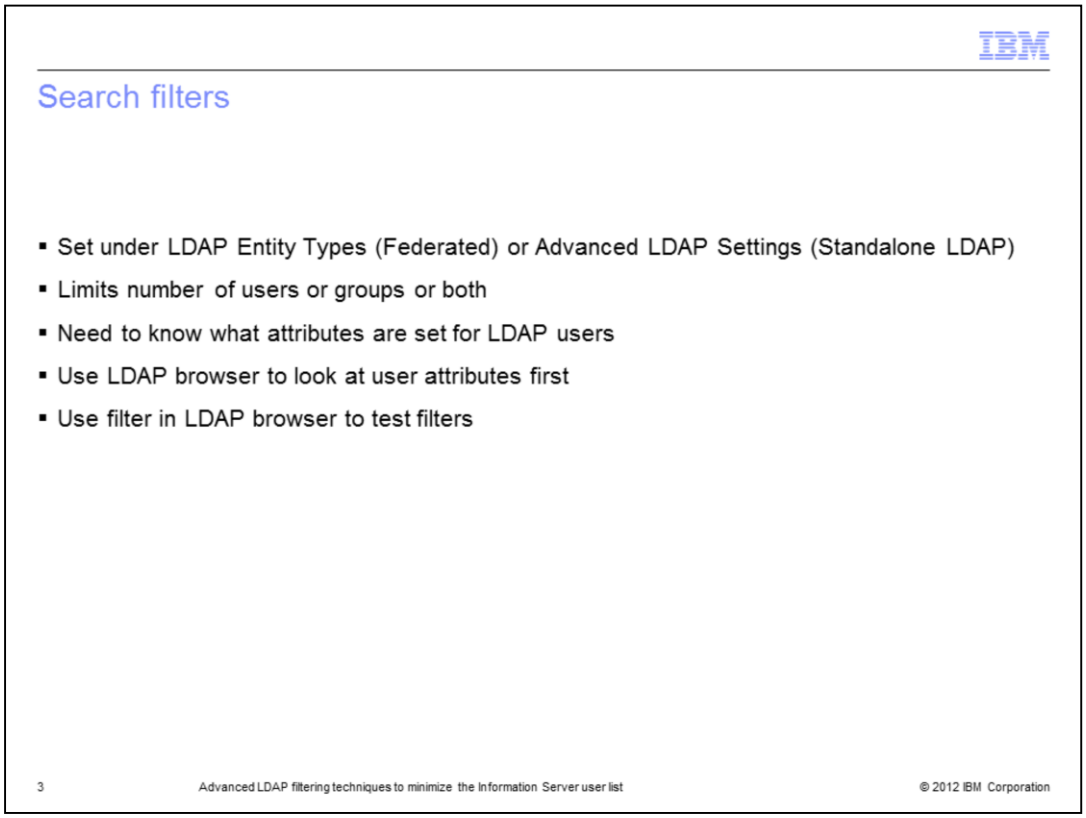


This presentation will discuss how to set up a user filter to minimize the number of users listed in the Information Server Web Console.



This presentation will discuss reasons for filtering your LDAP users, how to view your LDAP user attributes to determine what filter should be used and how to create and test your filter. This presentation will also discuss how to set your filter up in WebSphere® so that only the users you want are displayed in the Information Server Web Console.

The concepts of this presentation are for both LDAP and Active Directory. For simplicity, the term LDAP refers to both. This presentation will also assume that you already have LDAP configured and working with your version of Information Server and WebSphere. This presentation will not discuss how to configure Information Server to use LDAP.

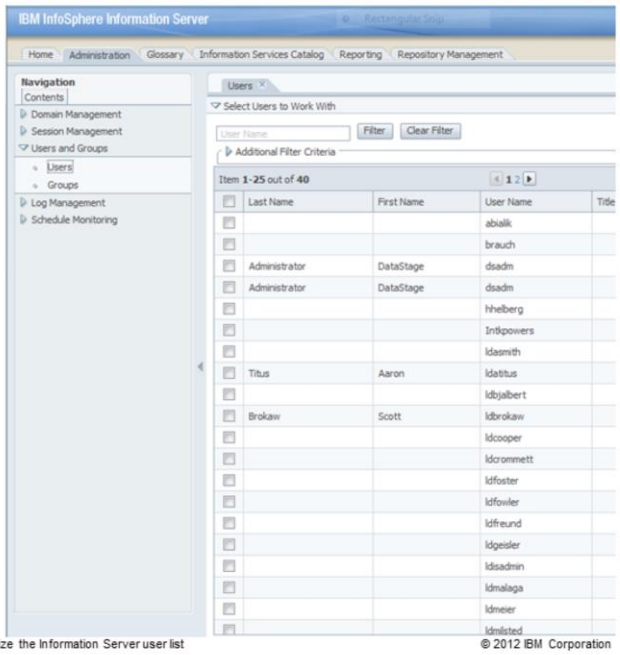


Search filters will help limit the number of users or groups that are returned to WebSphere or Information Server when requesting a list of users or groups. This is especially important in cases where WebSphere is authenticating against multiple domains or one very large domain.

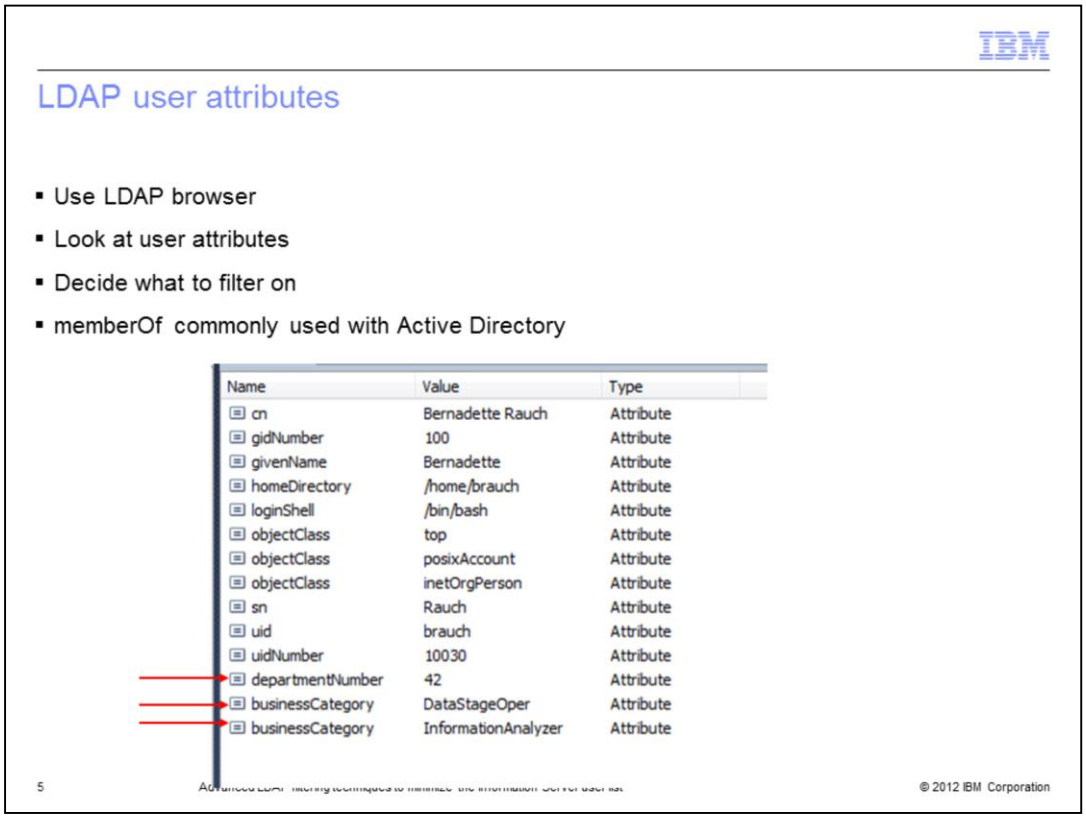
In order to create a filter, you must know what attributes are set up for the LDAP users. The easiest way to tell is with an LDAP browser. The LDAP browser will allow you to see the attributes for a user or group and it will also allow you to test your filters before adding them into WebSphere. Each time you add or change a filter in WebSphere, you need to stop and restart WebSphere for the changes to take effect. This can be very time consuming. It is much easier to test your filter in your LDAP browser and then update WebSphere once you have the filter correct.

Information Server Web Console default user list

- By default, all LDAP users are displayed
- LDAP servers may have thousands of users
- Only want to see Information Server users



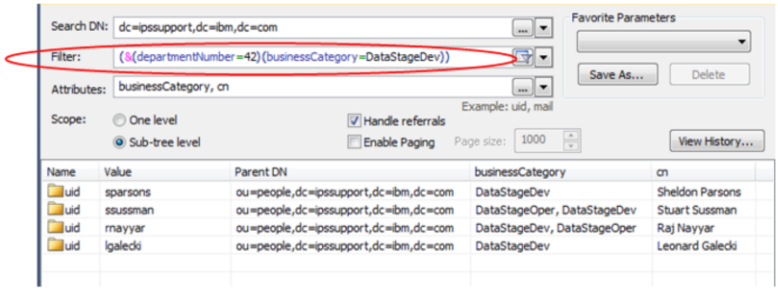
When you open the Information Server Web Console, by default, you will see all the LDAP users. When querying against multiple domains or a very large domain, the result of the search may yield thousands of users. These large searches can also take a long time to return and may result in an error if the result set it too large. It is much more manageable to see just a list of your Information Server users.



The first step is to open an LDAP browser and look at the attributes of a user that you will want to include in your user list. When you set up a filter, you are basically telling the LDAP server what to search for. If you wanted to search for the user in the example on this slide, you can set the filter up to search for users where their department number equals 42. A very common attribute to use with Active Directory is memberOf. This attribute is set for each group the user is a member of.

Search filters – Example (1 of 4)

- Filters use standard LDAP filter syntax
- Example:
  - Use businessCategory and departmentNumber
  - Create filter with attributes
    - businessCategory = DataStageDev
    - departmentNumber = 42
    - Use “&” for “AND” operation
      (&(departmentNumber=42)(businessCategory=DataStageDev))
- Test filter in LDAP browser

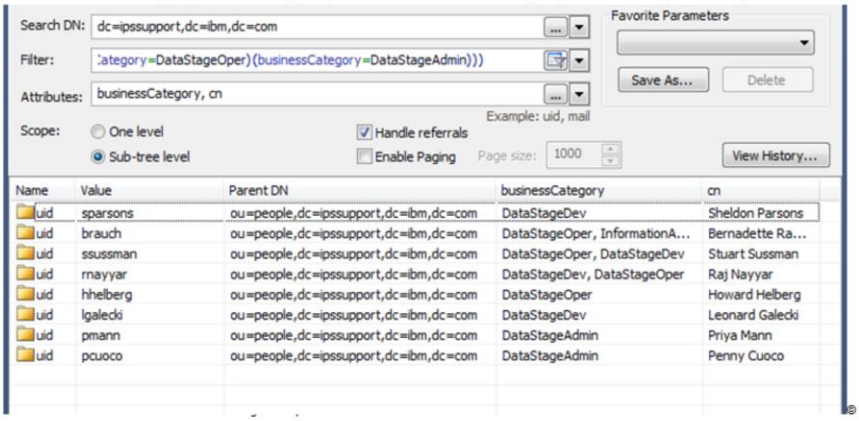


The syntax that WebSphere uses for filtering is the standard LDAP filter syntax. This example will use the user attributes businessCategory and departmentNumber. The filter will look for users where businessCategory is set to DataStageDev and departmentNumber is 42. The “&” tells the filter that both criteria must be met.

This particular filter is only returning four users which is too restrictive. The filter needs to be modified so that all of the Information Server users are returned.

Search filters – Example (2 of 4)

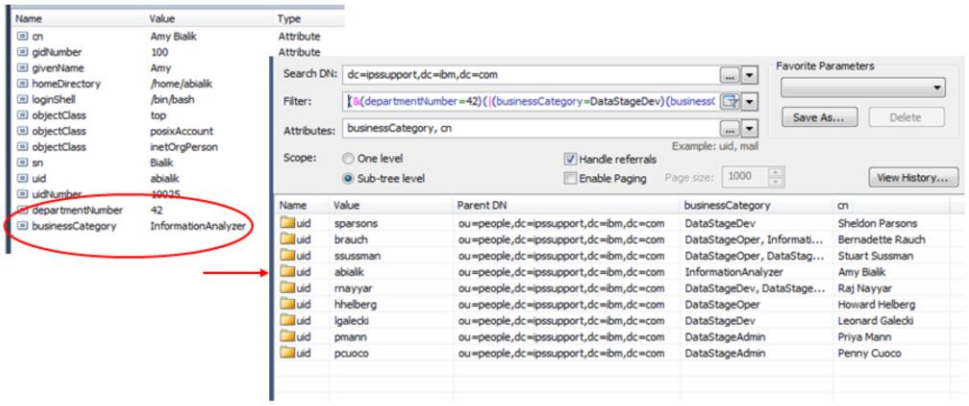
- Add businessCategtory "DataStageOper" and "DataStageAdmin"
- Still need "departmentNumber=42" and "businessCategory=DataStageDev"
- "|" = OR
- (&(departmentNumber=42)(|(businessCategory=DataStageDev)(businessCategory=DataStageOper)(businessCategory=DataStageAdmin)))
- Filter reads
  - departmentNumber = 42 AND (businessCategory=DataStageDev OR businessCategory=DataStageOper OR businessCategory=DataStageAdmin)



In order to make the filter less restrictive and return more of the Information Server users, the filter will keep the departmentNumber at 42 and the businessCategory of dataStageDev and will add the businessCategory of DataStageOper and DataStageAdmin. This search will need to do both an "And" and an "OR" to yield the correct results. The pipe symbol is used for an OR operation. The search results of this filter is better because it correctly shows all of the DataStage users but it is missing the Information Analyzer users that do not have a DataStage businessCategory.

Search filters – Example (3 of 4)

- Filter missing Information Analyzer user
- User only has one businessCategory attribute
  - InformationAnalyzer
- (&(departmentNumber=42)(|(businessCategory=DataStageDev)(businessCategory=DataStageOper)(businessCategory=DataStageAdmin)(businessCategory=InformationAnalyzer)))
- Standalone LDAP - WebSphere Admin user **must be part of the result set**



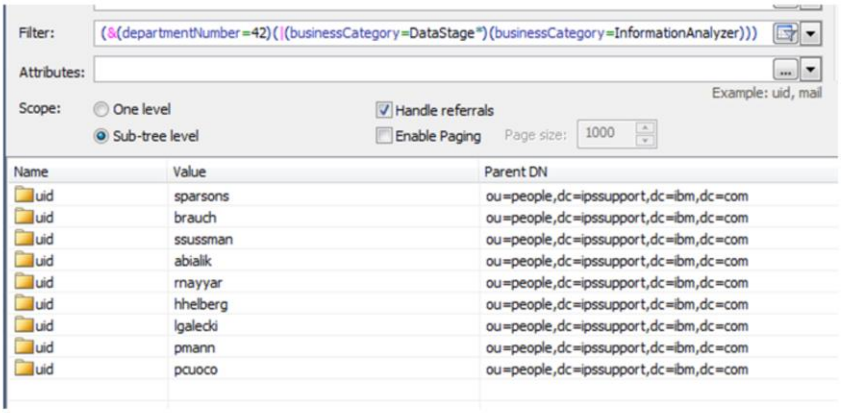
In this example, user abialik is missing from the list because Amy is not a DataStage user but only an Information Analyzer user. In order to include this user as well, add one last addition to the filter of businessCategory=InformationAnalyzer. The list now contains all the users that you want to see in the user list in the Information Server Web Console. When configuring stand-alone LDAP, it is important to make sure this list includes your WebSphere admin user or the WebSphere admin user is not able to authenticate.

Search Filters – Example (4 of 4)

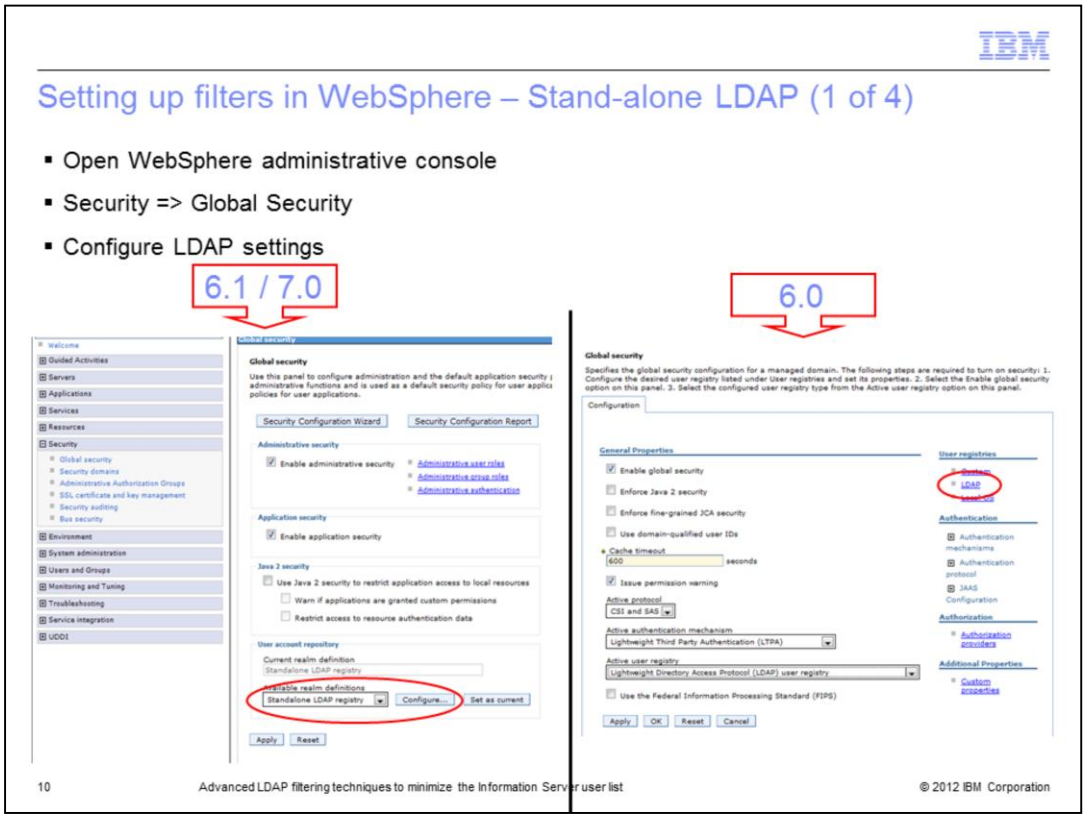
- LDAP syntax allows wild card – "*"

(&(departmentNumber=42)(|(businessCategory=DataStage*)(businessCategory=InformationAnalyzer)))

- Wild card may not be used with all attributes
  - Example: memberOf



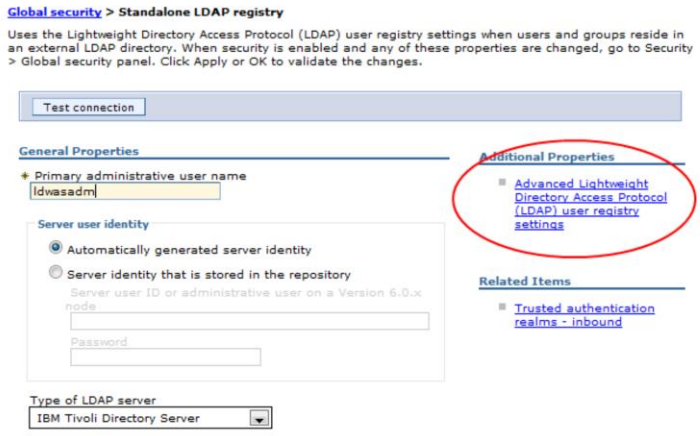
LDAP syntax also allows for the use of an asterisk as a wild card in some instances. In this last example, the search filter from the previous slide was shortened by using the wild card syntax businessCategory=DataStage*. Not all attributes allow this, for example, this will not work with memberOf on Active Directory. At this point, you are ready to add the filter to WebSphere.



The first example is setting up the filter in a stand-alone LDAP configuration. Begin by opening the WebSphere administrative console as your WebSphere admin user. For WebSphere 7.0 that ships with Information Server 8.5 and 8.7, make sure the Available realm definition is set to Standalone LDAP registry and click Configure. If you are using Information Server 8.0 or 8.1, which ships with WebSphere 6.0, click the LDAP link under User Registries.

Setting up filters in WebSphere – Stand-alone LDAP (2 of 4)

- Additional Properties => Advanced LDAP user registry settings

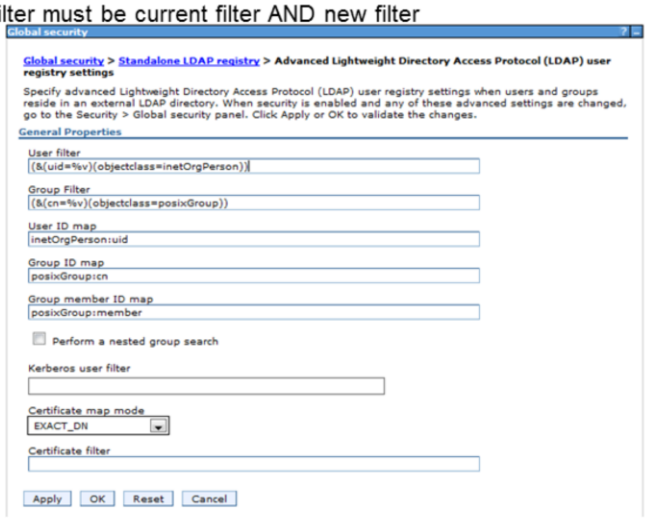


Advanced LDAP filtering techniques to minimize the Information Server user list

Next, click Advanced LDAP user registry settings under Additional Properties. The WebSphere 6.0 screen will look slightly different than this screen capture displayed on this slide but will still contain the Advanced LDAP link in the same location on the right side of the screen.

Setting up filters in WebSphere – Stand-alone LDAP (3 of 4)

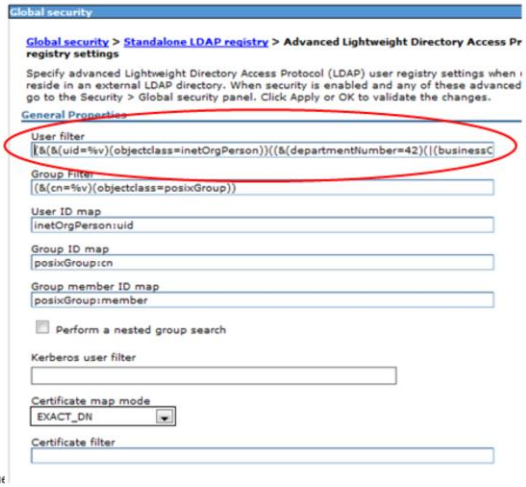
- User filter
  (&(uid=%v)(objectclass=inetOrgPerson))
- Add new filter to current filter
- New filter must be current filter AND new filter



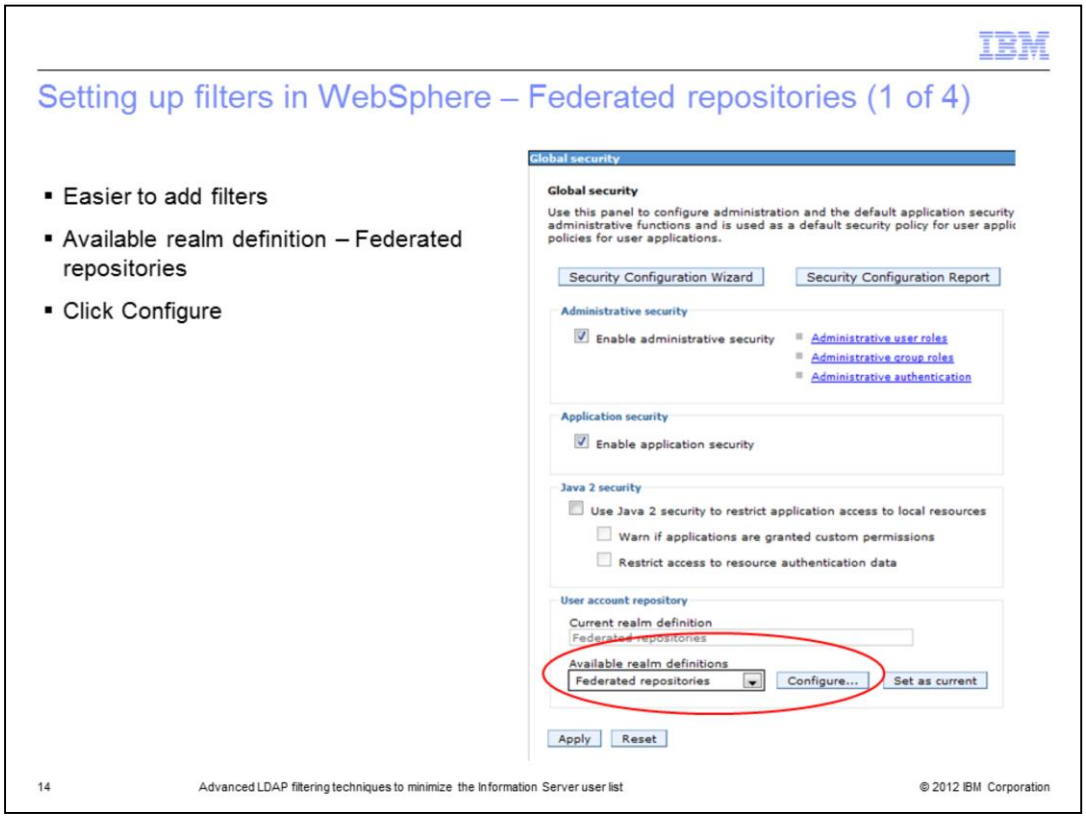
Your screen will show the user and group filters that have been set up so far. The next step is to add the filter that was created using the LDAP browser to the user filter. Since the current filter does the user search, the new filter must be added to the current filter. It cannot replace the current filter.

Setting up filters in WebSphere – Stand-alone LDAP (4 of 4)

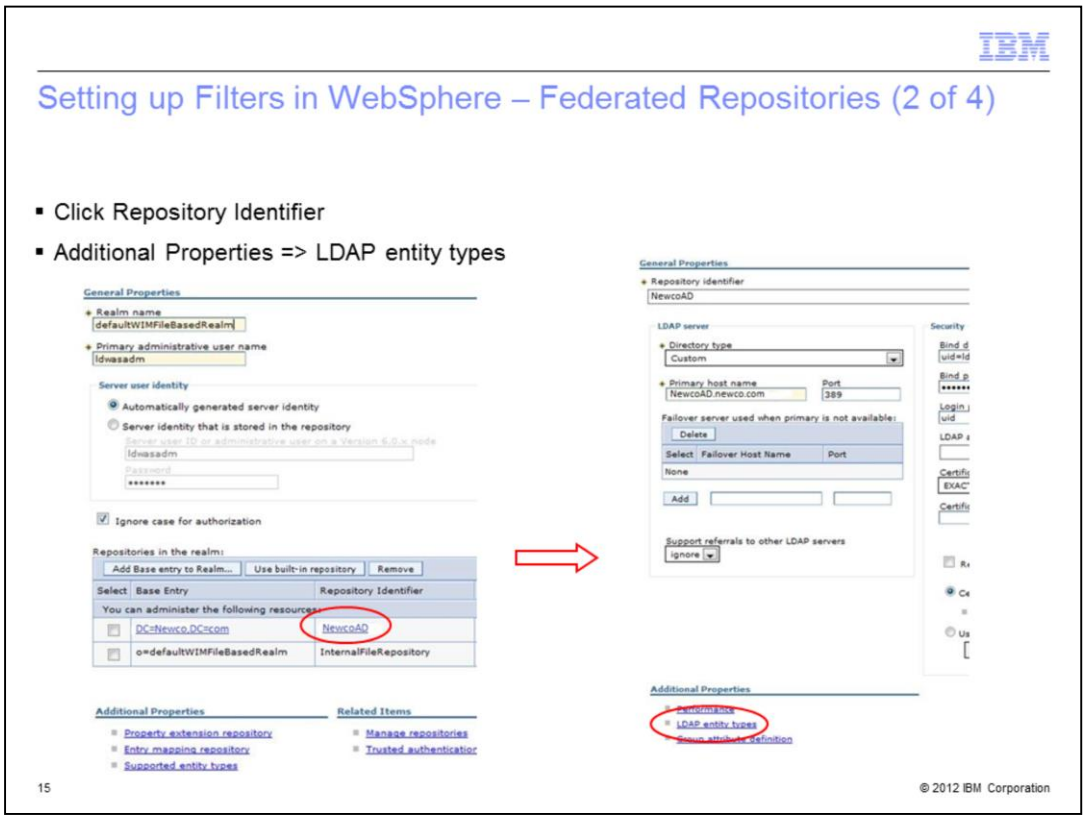
- User filter => Original user filter AND new user filter (&(&(uid=%v)(objectclass=inetOrgPerson))((&(departmentNumber=42)(|(businessCategory=DataStage*)(businessCategory=InformationAnalyzer))))
- Save and restart WebSphere



The user filter now contains the original filter and the new filter that was created earlier wrapped with an “AND” clause. Save the settings and restart WebSphere.



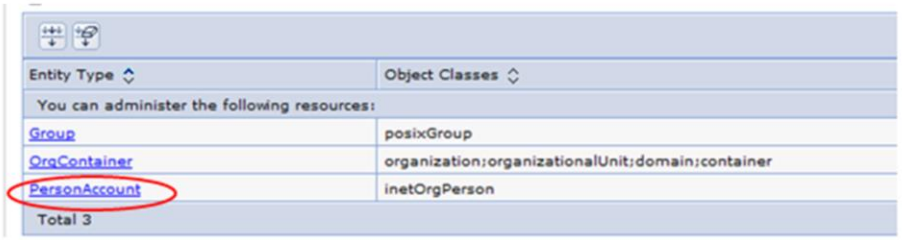
The next example shows how to set up the same user filter under Federated repositories. WebSphere version 6.1 introduced federated repositories. Federated repositories makes setting up the user filters much easier than under stand-alone LDAP. If you are using Information Server 8.5 or 8.7 and have set WebSphere up to use federated repositories, you need to be sure the Available realm definition is set to Federated repositories and then click configure.



Next, under the list of the Repositories in the realm, click the Repository identifier of the repository you want to add the filter to. On the next screen, go to the bottom of the screen under Additional Properties and click LDAP entity types.

Setting up Filters in WebSphere – Federated Repositories (3 of 4)

- Click PersonAccount



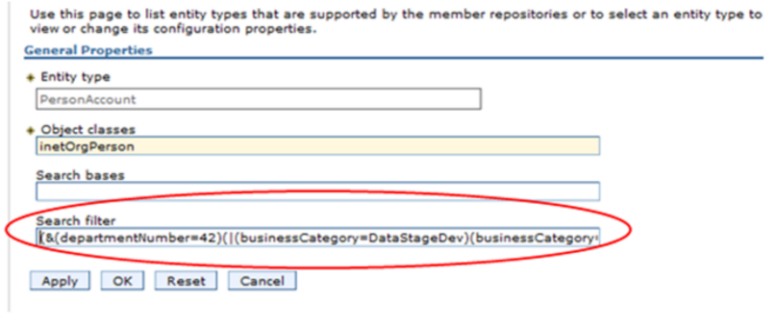
Entity Type	Object Classes
You can administer the following resources:	
Group	posixGroup
OrgContainer	organization;organizationalUnit;domain;container
PersonAccount	inetOrgPerson
Total 3	

16

Since the filter that was created is a filter for the user list, click PersonAccount.

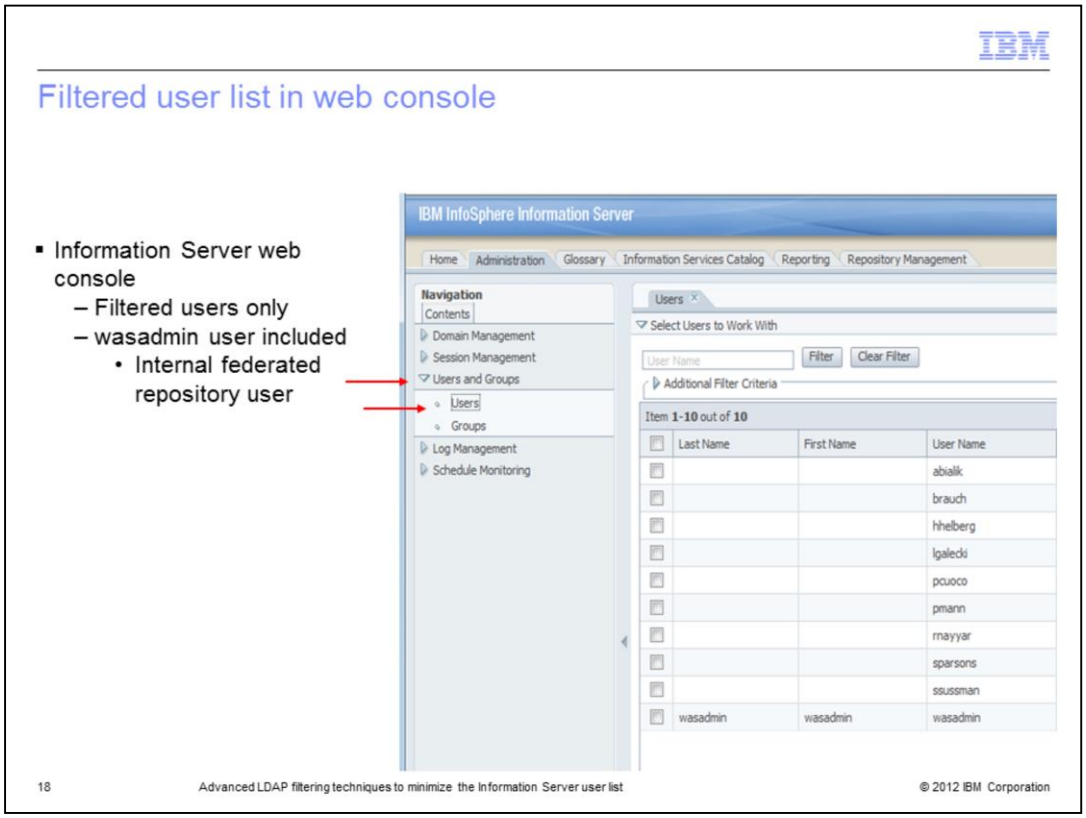
Setting up Filters in WebSphere – Federated Repositories (4 of 4)

- Add new filter to Search Filter
- No need to append to a user filter as with stand-alone LDAP
- Save and restart WebSphere



Next, add the filter that was created with the LDAP browser in the Search filter field. This value is the exact same value that was used in the LDAP browser. You do not have to append it to a user filter as you did with stand-alone LDAP.

Click apply, save and restart WebSphere.



Once WebSphere has been restarted, open the Information Server administrative console. Click Users and Groups and then Users. You will now see that the only users that appear are the ones displayed in the filter including the WebSphere admin user. This screen capture shows a list from federated repositories where the WebSphere admin user is an internal service account and not in LDAP.

Trademarks, disclaimer, and copyright information