Business Process Management

Business Process Management

IBM Business Process Manager V7.5

Managing users and groups

This presentation provides information about working with users and groups when developing process applications using IBM Business Process Manager V7.5.

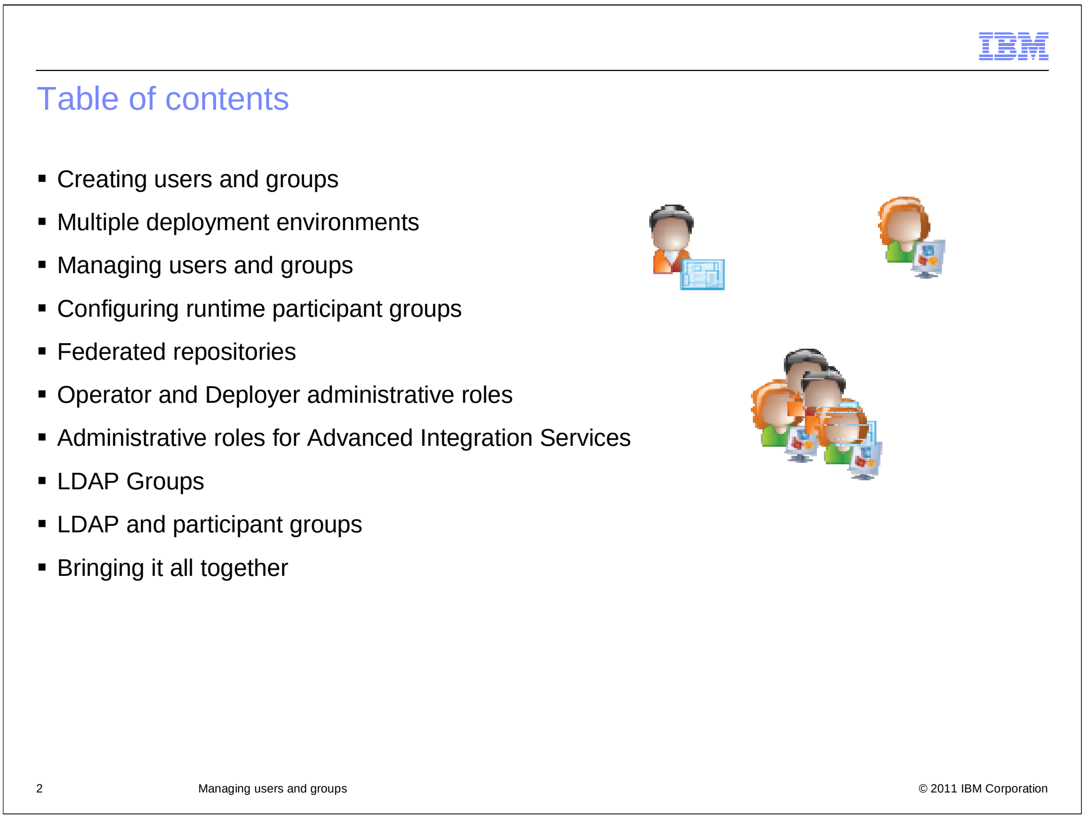


Table of contents

- Creating users and groups
- Multiple deployment environments
- Managing users and groups
- Configuring runtime participant groups
- Federated repositories
- Operator and Deployer administrative roles
- Administrative roles for Advanced Integration Services
- LDAP Groups
- LDAP and participant groups
- Bringing it all together

2 Managing users and groups

Business Process Manager V7.5 uses WebSphere Process Server and WebSphere Application Server as the foundation for the application server infrastructure.

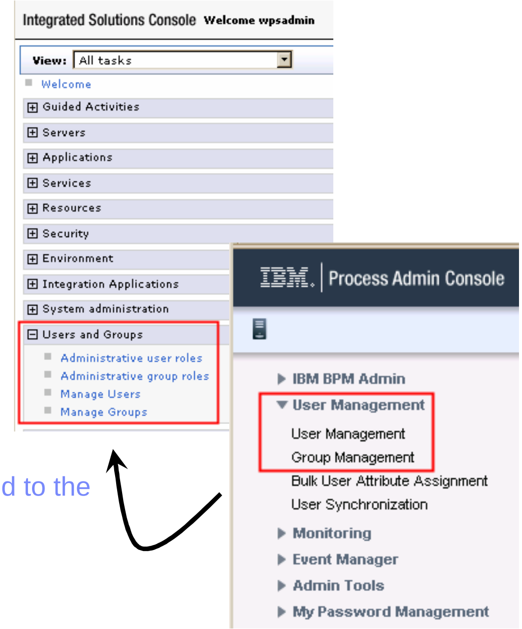
User and group management starts with the WebSphere Application Server administration and is shared with the Process Center. This results in having two places where you can create and manage users.

Because there are multiple user registries, there are a few issues you need to consider before configuring your development and production environments.

This presentation discusses issues around multiple deployment environments, federated repositories, and LDAP.

Creating users and groups

- Places where users and groups are created
  - Integrated Solutions Console
  - Process Admin console
  - LDAP administrative console (optional, and inevitable)
- Additionally, participant groups are created in the…
  - Process Application



Automatically added to the WebSphere users

The integrated solutions console is also know as the WebSphere Adminconsole.

When you first begin working with Business Process Manager you don’t need to worry about the WebSphere part.

It is transparent until you need to use Advanced Integration Services or configure an LDAP user-registry.

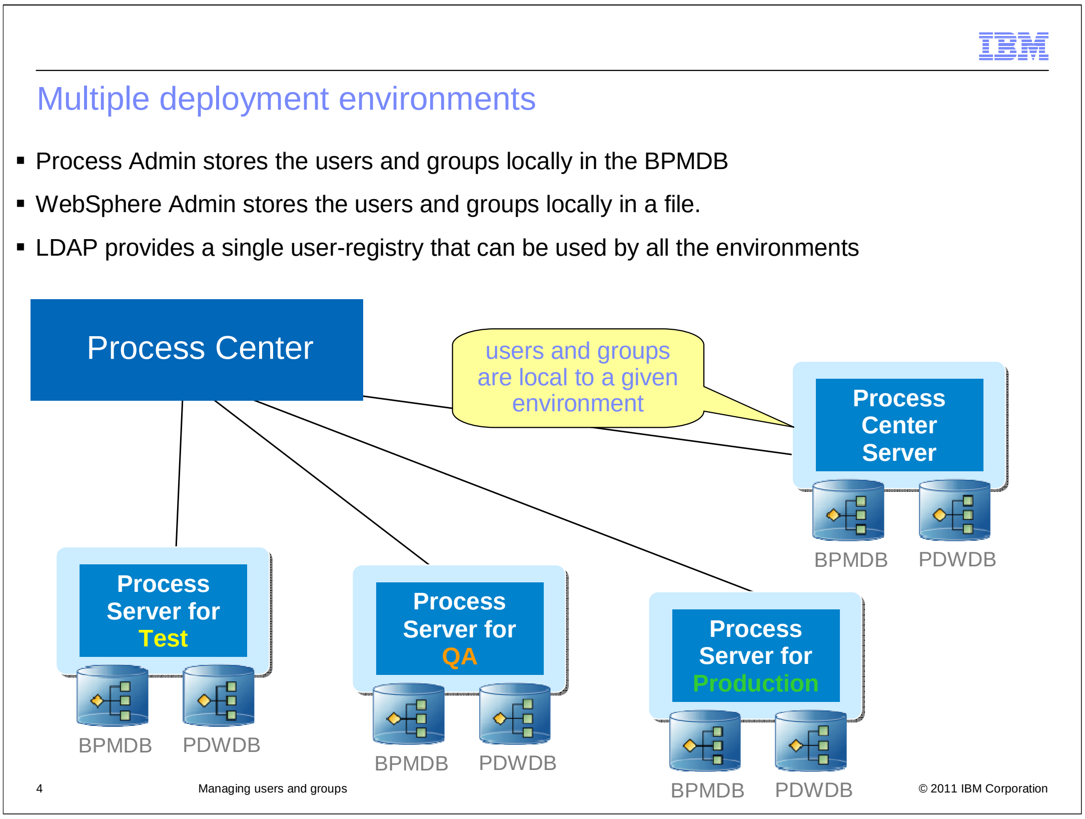
When you add a user to the Process Center using the Process Admin Console, it is automatically added to the WebSphere user-registry. This is not the case with the groups. The groups created in the Process Admin Console are not copied to the WebSphere user-registry.

When you create users in the WebSphere user-registry, they do not show up in the Process Admin user list because they cannot be managed there.

You can however, add them to groups that are defined in the Process Admin Console.

When LDAP is federated into the user-registry, there is a third user and group management system. These all co-exist, so as an administrator, you will need to understand when to use which.

As a best practice, if you are using LDAP, then use that for everything, unless you need to add a user to the WebSphere user registry for administrative purposes.



Multiple deployment environments

- Process Admin stores the users and groups locally in the BPMDB
- WebSphere Admin stores the users and groups locally in a file.
- LDAP provides a single user-registry that can be used by all the environments

Process Center

users and groups are local to a given environment

Process Center Server

BPMDB PDWDB

Process Server for Test

BPMDB PDWDB

Process Server for QA

BPMDB PDWDB

Process Server for Production

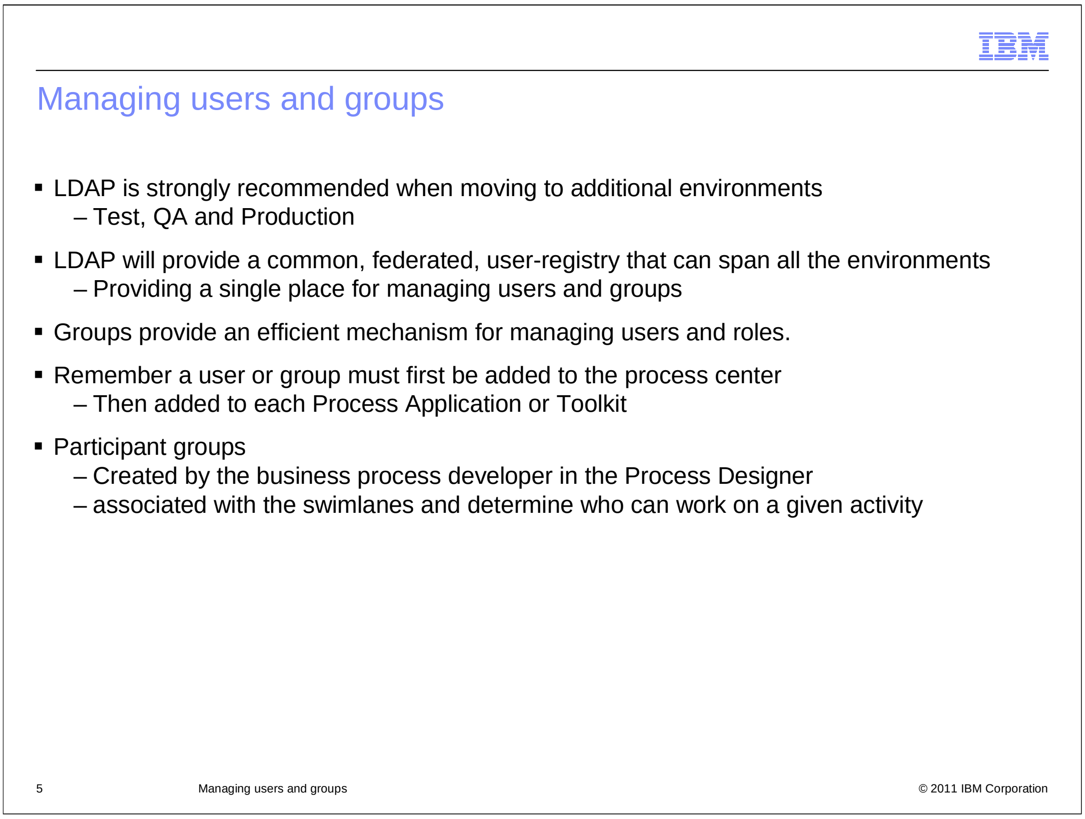
BPMDB PDWDB

4 Managing users and groups

The default user registries are local to a given deployment environment. This means that you have to administer the users and groups for each environment separately.

If there are users that are common between the environments, then as you move from test, to QA, to Production you need to manually add the new users to the registry for each environment. This can quickly become a management burden.

The solution is to use an LDAP user-registry that can be used by all the environments.



Managing users and groups

- LDAP is strongly recommended when moving to additional environments
  - Test, QA and Production
- LDAP will provide a common, federated, user-registry that can span all the environments
  - Providing a single place for managing users and groups
- Groups provide an efficient mechanism for managing users and roles.
- Remember a user or group must first be added to the process center
  - Then added to each Process Application or Toolkit
- Participant groups
  - Created by the business process developer in the Process Designer
  - associated with the swimlanes and determine who can work on a given activity

5 Managing users and groups

Once you create a test environment, it quickly becomes apparent that there is a need to have a user-registry that spans all the deployment environments. Without a centralized user-registry that is common to all the environments, the administrators must manually populate and maintain the users and groups for each environment. Chances are, there are users and groups common to all the environments.

The common user-registry of choice is an LDAP registry. The LDAP registry will provide a centralized user management console for most of your needs. The users and groups defined in the LDAP registry is available in the Process Admin console, and the Process Center. You won’t be able to edit them there, but you can use them.

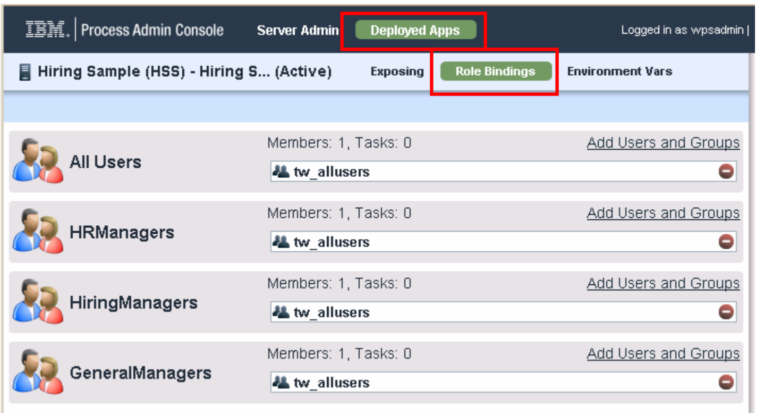
When managing user privileges, it is most efficient to use groups. You can set up the privileges for the group and then just add and remove the users from the groups. If you are using LDAP, then you can manage the groups and their membership list from the LDAP console.

You manage the privileges for the groups in the Process Center and, if working with Advanced Services, in the WebSphere Adminconsole.

The participant groups are yet another level of creating groups. Participant groups are created by the business process developer, rather than the administrator. They are the groups associated with the swimlanes that determine who can work on a given activity.

Configuring runtime participant groups

- Configuring runtime participant groups
  - When promoting Process Applications through test, QA and then production
    - different sets of users are working with the Process Applications
  - Participant groups for a snapshot can be changed by the administrator using the *Process Admin* console
    - Select the *Deployed Apps* tab and then the *Role Bindings*



All Users — Members: 1, Tasks: 0 — Add Users and Groups — tw_allusers

HRManagers — Members: 1, Tasks: 0 — Add Users and Groups — tw_allusers

HiringManagers — Members: 1, Tasks: 0 — Add Users and Groups — tw_allusers

GeneralManagers — Members: 1, Tasks: 0 — Add Users and Groups — tw_allusers

As you move the business process application through the different environments, test, QA, and production, the users that are in the participant groups change.

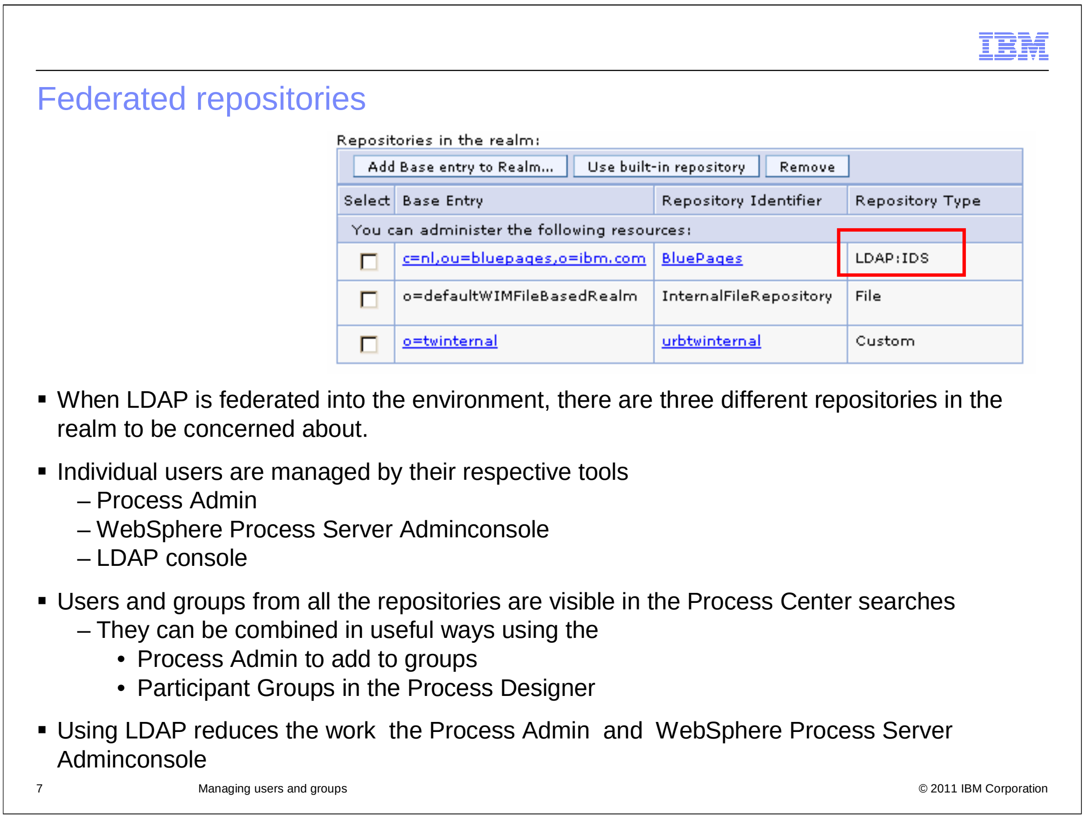
After the process application has been deployed, you need to update the users and groups that are in the participant groups.

To help you manage this there is a feature in the Process Admin console for reassigning the role bindings.

Go to the deployed application in the Process Admin console of the server where the application has been deployed,

select Deployed Apps and then Role Bindings.

Here you can see the different participant groups that are used for the Hiring Sample. If you are using an LDAP user-registry, then when you select add users and groups, you’ll have the same pool of users and groups available that you had for the Process Center Server.



Federated repositories

Repositories in the realm:

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

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
□	c=nl,ou=bluepages,o=ibm.com	BluePages	LDAP:IDS
□	o=defaultWIMFileBasedRealm	InternalFileRepository	File
□	o=twinternal	urbtwinternal	Custom

- When LDAP is federated into the environment, there are three different repositories in the realm to be concerned about.
- Individual users are managed by their respective tools
  - Process Admin
  - WebSphere Process Server Adminconsole
  - LDAP console
- Users and groups from all the repositories are visible in the Process Center searches
  - They can be combined in useful ways using the
    - Process Admin to add to groups
    - Participant Groups in the Process Designer
- Using LDAP reduces the work the Process Admin and WebSphere Process Server Adminconsole

7 Managing users and groups © 2011 IBM Corporation

Adding LDAP means configuring Global Security in the WebSphere Process Server Adminconsole and adding a new base entry to the federated realm.

When you do this for the first time you will notice that there are already two base entries.

<note to reader for the line below…. Say whim for WIM >

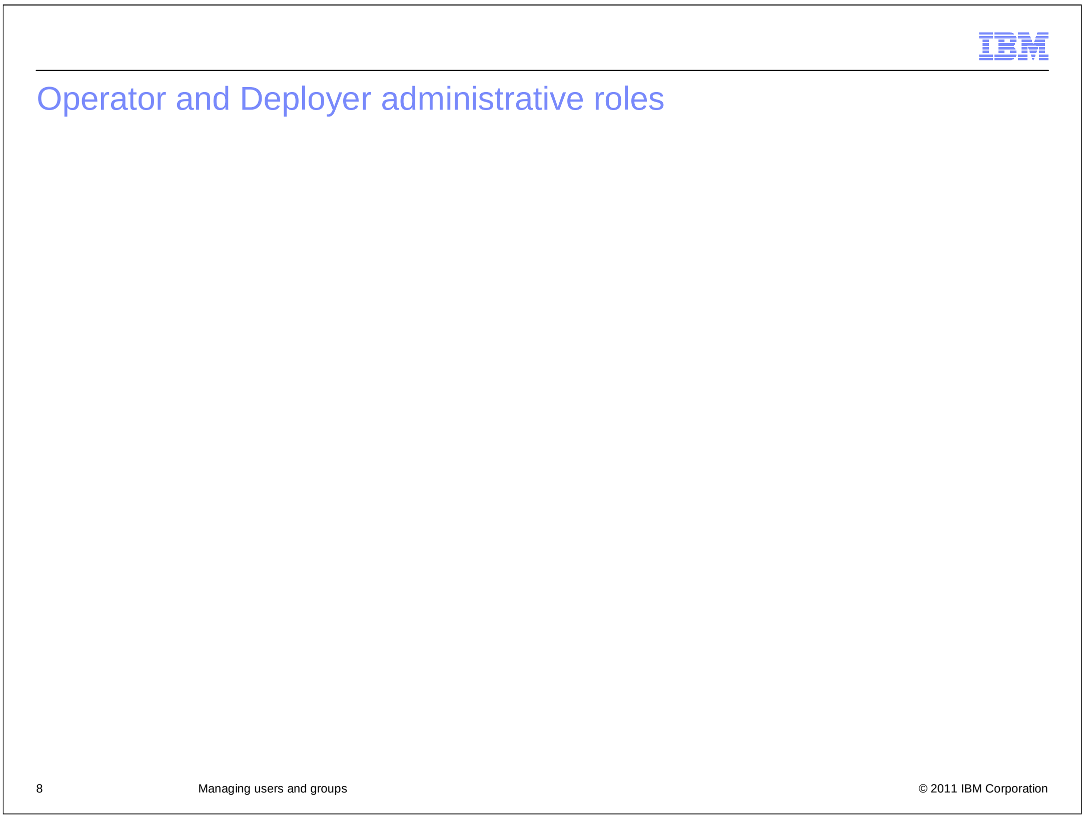
The default WIM file based realm is the contribution from WebSphere Process Server.

The tw internal base entry is from the Process Center.

When LDAP is federated into the environment, there are three different repositories in the realm to be concerned about.

Each one provides a different way to add and manage users and groups.

Since the LDAP entities are propagated to the Process Center, judicious use of groups will reduce the amount of user management you need to do in the Process Admin Console or the WebSphere Process Server Adminconsole.



Operator and Deployer administrative roles

Advanced Integration Services use SCA components.

In the world of WebSphere Process Server and SCA, the administrative roles are used to manage who can deploy applications, operate, and configure them.

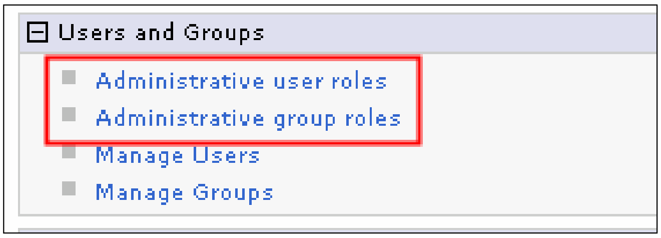
Failure to add these administrative roles to your users and groups will cause the error dialog shown here to be displayed.

It is a clear message, and now that you know about it, you’ll know exactly what to do to fix it.

Without these roles assigned, you will get the error when adding, publishing, running or deploying a Process Application or Toolkit that has SCA components,

to test, QA or production.

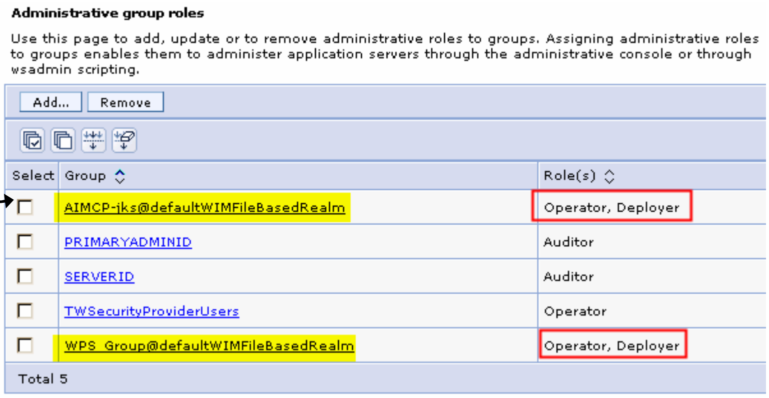
Administrative roles for Advanced Integration Services



Learn more about Administrative roles

This is from LDAP

Although it does not Look like it…. It is OK, working as designed



Administrative group roles

Use this page to add, update or to remove administrative roles to groups. Assigning administrative roles to groups enables them to administer application servers through the administrative console or through wsadmin scripting.

Select	Group	Role(s)
□	AIMCP-jks@defaultWIMFileBasedRealm	Operator, Deployer
□	PRIMARYADMINID	Auditor
□	SERVERID	Auditor
□	TWSecurityProviderUsers	Operator
□	WPS_Group@defaultWIMFileBasedRealm	Operator, Deployer

Total 5

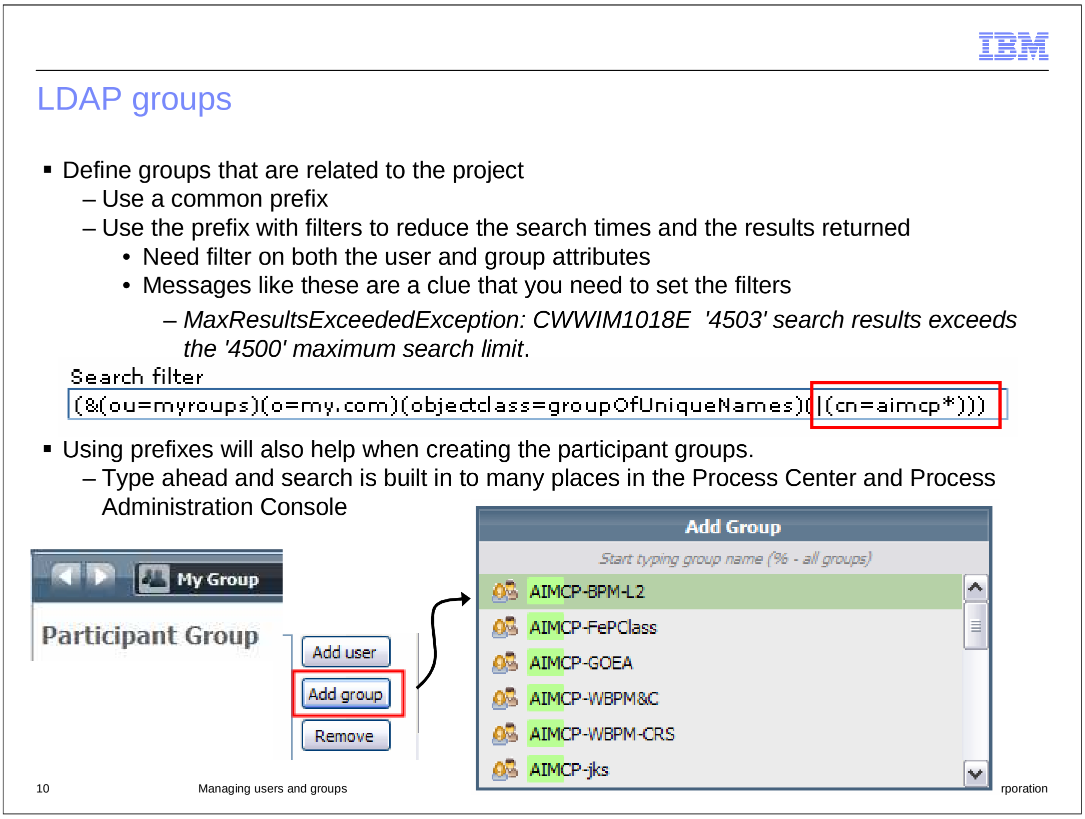
To set the operator and deployer roles in the WebSphere Process Server Adminconsole, you use the Administrative roles in the users and groups section.

Select the link to learn more about the administrative roles.

The lower screen capture shows the group list after the roles have been set for the two user-defined groups.

Notice that the first entry, the group AIMCP-jks, looks like it is coming from the default WIM File Based Realm. It is actually a group that is defined and managed in the LDAP registry. For the purpose of the privileges, a reference is made in the default realm.

Select the link to learn more about the administrative roles.



LDAP groups

- Define groups that are related to the project
  - Use a common prefix
  - Use the prefix with filters to reduce the search times and the results returned
    - Need filter on both the user and group attributes
    - Messages like these are a clue that you need to set the filters
      - *MaxResultsExceededException: CWWIM1018E '4503' search results exceeds the '4500' maximum search limit*.

Search filter

```
(&(ou=myroups)(o=my.com)(objectclass=groupOfUniqueNames)(|(cn=aimcp*)))
```

- Using prefixes will also help when creating the participant groups.
  - Type ahead and search is built in to many places in the Process Center and Process Administration Console

10 Managing users and groups rporation

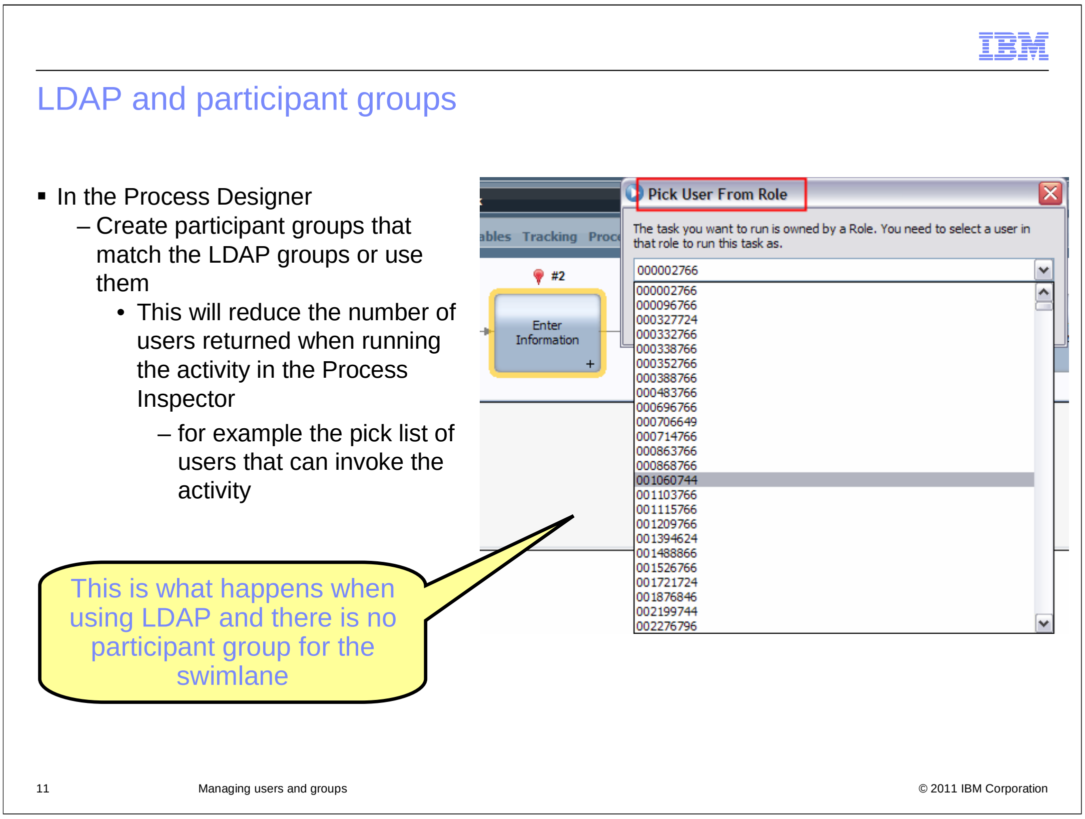
When creating LDAP groups, use a prefix that can be used in creating LDAP filters.

The LDAP filters are used in the configuration of the federated user-registry when configuring LDAP with WebSphere Process Server.

Having filters will reduce the number of results returned when the doing the LDAP searches.

The screen capture here shows the selection dialog for groups when creating a participant group. You start typing the name of the group and the search begins.

If you use a prefix then they will all come up together, quickly.



LDAP and participant groups

- In the Process Designer
  - Create participant groups that match the LDAP groups or use them
    - This will reduce the number of users returned when running the activity in the Process Inspector
      - for example the pick list of users that can invoke the activity

Pick User From Role

The task you want to run is owned by a Role. You need to select a user in that role to run this task as.

000002766

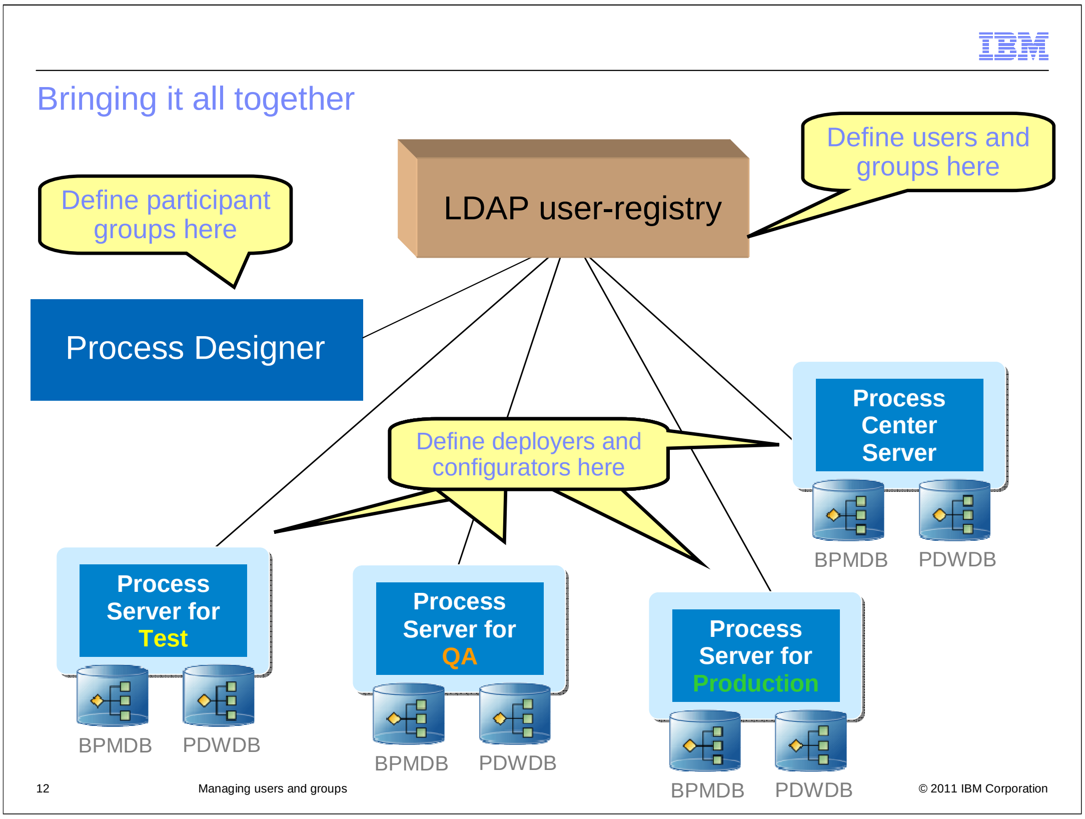
```
000002766
000096766
000327724
000332766
000338766
000352766
000388766
000483766
000696766
000706649
000714766
000863766
000868766
001060744
001103766
001115766
001209766
001394624
001488866
001526766
001721724
001876846
002199744
002276796
```

This is what happens when using LDAP and there is no participant group for the swimlane

Once the LDAP is configured, you want to always define your participant groups for your swimlanes. If you are using LDAP groups, then be sure to use them whenever possible when creating participant groups.

If you don’t associate a participant group with a swimlane, then when you run an activity in the Inspector, it will attempt to list all the users in your LDAP registry. This is typically very large. In the example shown here, it is attempting to list all the users in the directory.

Using the participant groups, restricts the search to those in the group. Using groups is much more efficient and reliable.



Bringing it all together

Define participant groups here

Process Designer

LDAP user-registry

Define users and groups here

Define deployers and configurators here

Process Center Server

BPMDB PDWDB

Process Server for Test

BPMDB PDWDB

Process Server for QA

BPMDB PDWDB

Process Server for Production

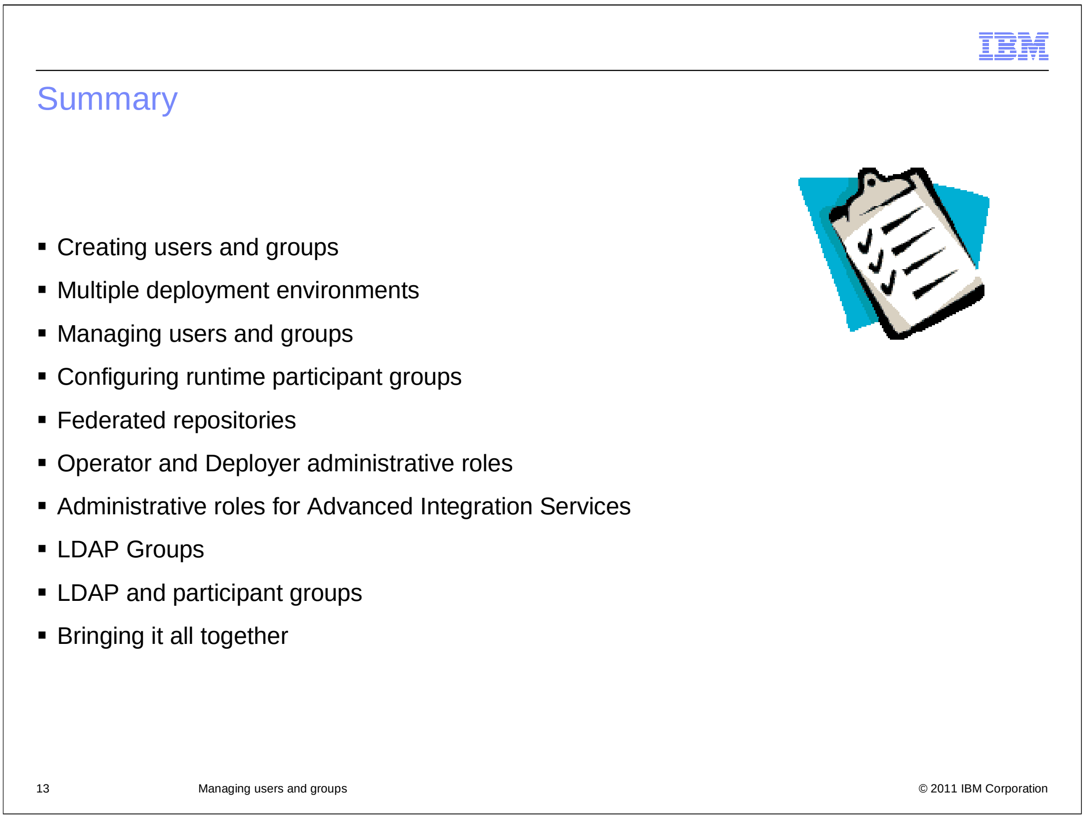
BPMDB PDWDB

12 Managing users and groups

To reduce the overhead of managing the users and groups across all the environments, use a centralized LDAP registry.

The participant groups are created using the Process Designer.

The deployers and configurators are only needed if you are using the Advanced Integration Services. They are configured using the WebSphere Process Server Adminconsole.



IBM

Summary

- Creating users and groups
- Multiple deployment environments
- Managing users and groups
- Configuring runtime participant groups
- Federated repositories
- Operator and Deployer administrative roles
- Administrative roles for Advanced Integration Services
- LDAP Groups
- LDAP and participant groups
- Bringing it all together

13 Managing users and groups © 2011 IBM Corporation

Managing users and groups is a critical task for any business process management project.

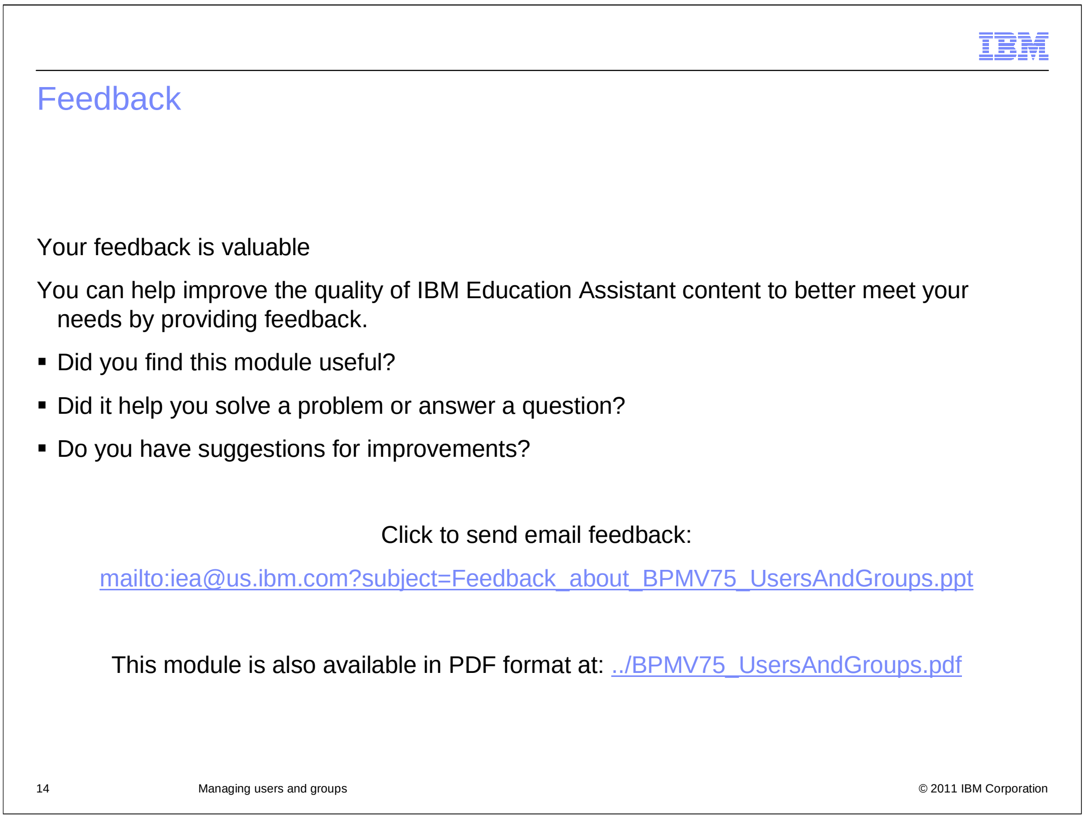
This presentation discussed issues pertaining to the management of users and groups that you will experience when you promote your process applications through the different environments, such as test, quality assurance and production.

Because the default user registries for each environment are local to that environment, the use of a centralized LDAP user-registry is recommended.

When federating the LDAP user-registry into the Business Process Manager user-registry, proper configuration of the LDAP filters and the use of groups with prefixes is essential for performance. With the addition of the LDAP registry, there are three repositories in the realm and therefore three separate user management consoles to work with. The recommendation is to use the LDAP registry for managing the users and groups and to use the WebSphere Process Server Adminconsole and the Process Center to set the privileges on the groups as needed. The use of groups will reduce the management overhead and prevent errors due to incorrect privileges.

If using Advanced Integration Services, you will need to manage the Administrative roles using the WebSphere Process Server Adminconsole.

And finally, when using LDAP, be sure to specify the participant groups for the swimlanes to avoid LDAP queries that retrieve all the users.



Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

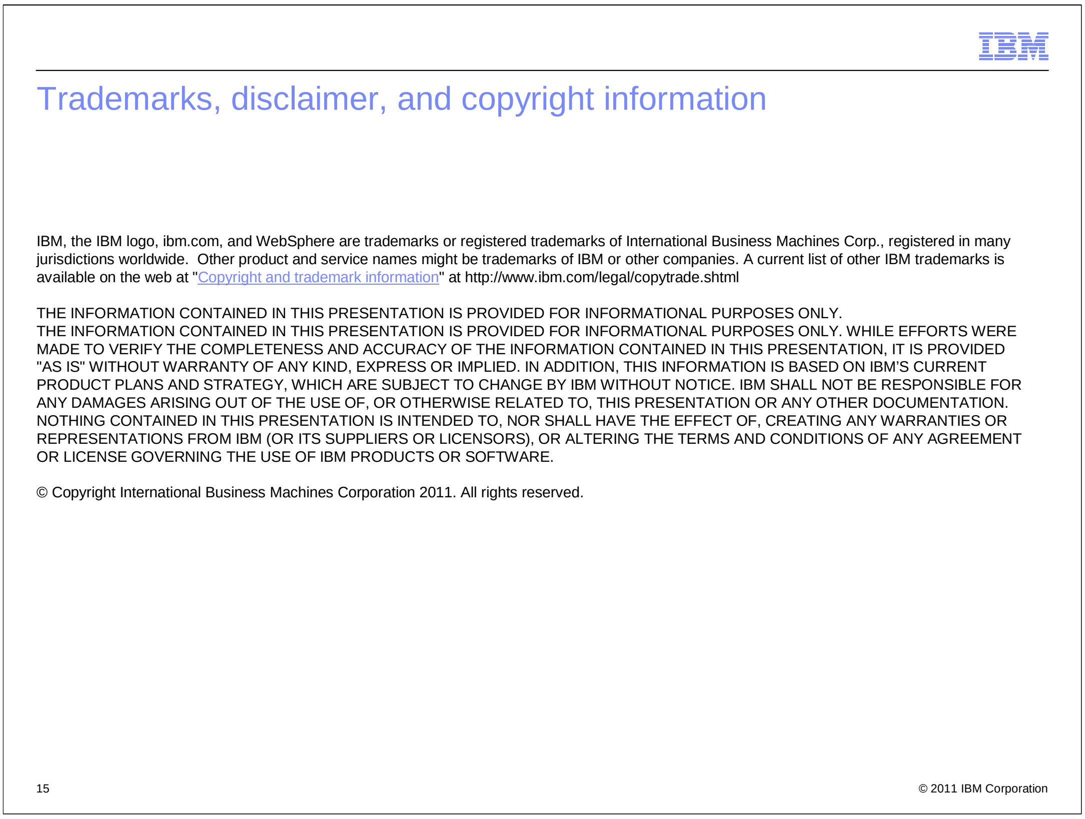
Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_BPMV75_UsersAndGroups.ppt

This module is also available in PDF format at: ../BPMV75_UsersAndGroups.pdf

14 Managing users and groups © 2011 IBM Corporation

You can help improve the quality of IBM Education Assistant content by providing feedback.



Trademarks, disclaimer, and copyright information

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY.
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.