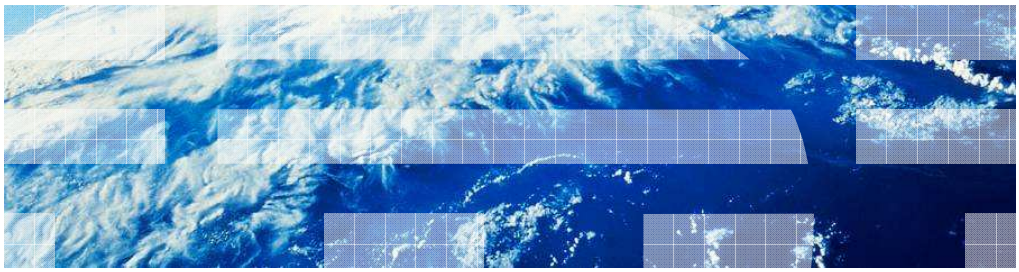
IBM WebSphere CloudBurst Appliance

LDAP integration



WebSphere. software

© 2010 IBM Corporation

This presentation provides an overview of the Lightweight Directory Access Protocol, or LDAP, integration features of the IBM WebSphere® CloudBurst™ Appliance.

Agenda

- Overview
- LDAP authentication configuration
- LDAP user and group management

© 2010 IBM Corporation

This presentation starts with an overview of LDAP integration with WebSphere CloudBurst, then covers how to configure and verify the LDAP authentication, followed by the details of LDAP user and group management.

Section

Overview

© 2010 IBM Corporation

This section of the presentation provides an overview of LDAP integration.

Overview

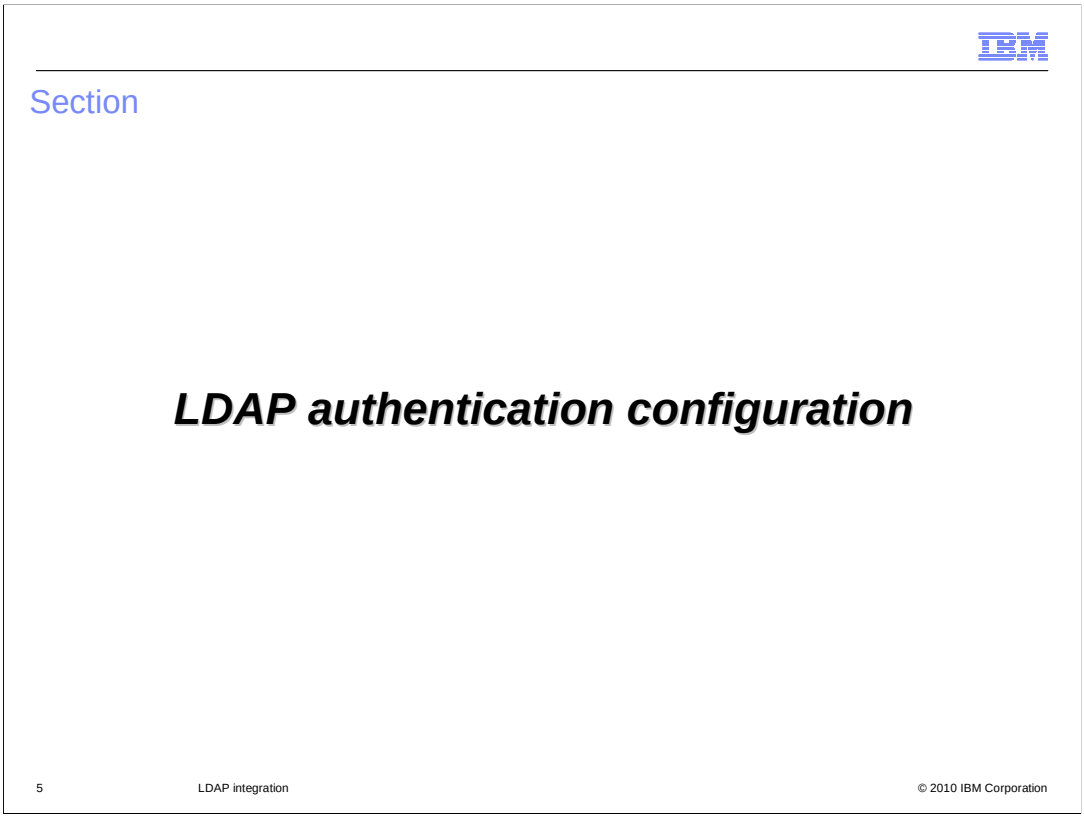
- A Lightweight Directory Access Protocol (LDAP) directory can be used to authenticate users with your WebSphere CloudBurst Appliance
- An administrator must create WebSphere CloudBurst user accounts for each LDAP user and LDAP group member in the LDAP directory who requires access to the appliance
- The cbadmin user can always access the WebSphere CloudBurst Appliance
- LDAP authentication configuration settings can be verified

© 2010 IBM Corporation

Local authentication is a great way to get started with WebSphere CloudBurst. However, if the WebSphere Cloudburst Appliance is going to be shared by a larger organization or a group of people who are not working side by side, you should you use an external authenticator, like a Lightweight Directory Access Protocol, or LDAP directory.

Using an LDAP server to authenticate users is optional. If you choose to use an external LDAP server, then all LDAP users must have WebSphere CloudBurst user accounts created to access the appliance. Furthermore, WebSphere CloudBurst users that are not registered in the LDAP directory cannot be authenticated. The one exception to this rule is the cbadmin user. Credentials for the cbadmin user always rely on the internal appliance security registry, so even if your LDAP directory server is down, the cbadmin user can access the appliance.

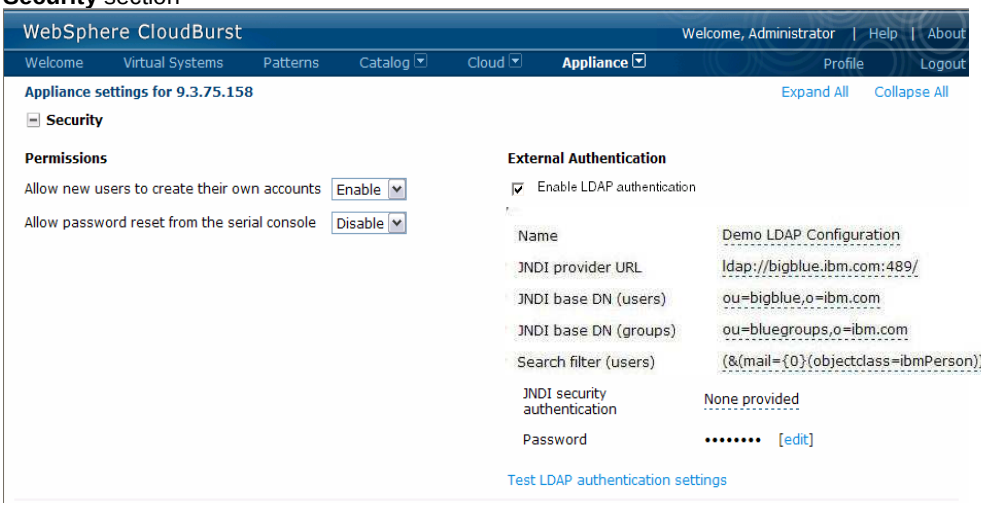
Also, in WebSphere CloudBurst, the product has provided test buttons to verify that the LDAP authentication configuration settings are working as planned.



This section of the presentation focuses on the process of configuring your WebSphere CloudBurst appliance for LDAP authentication using the Web console.

Authenticate users with LDAP

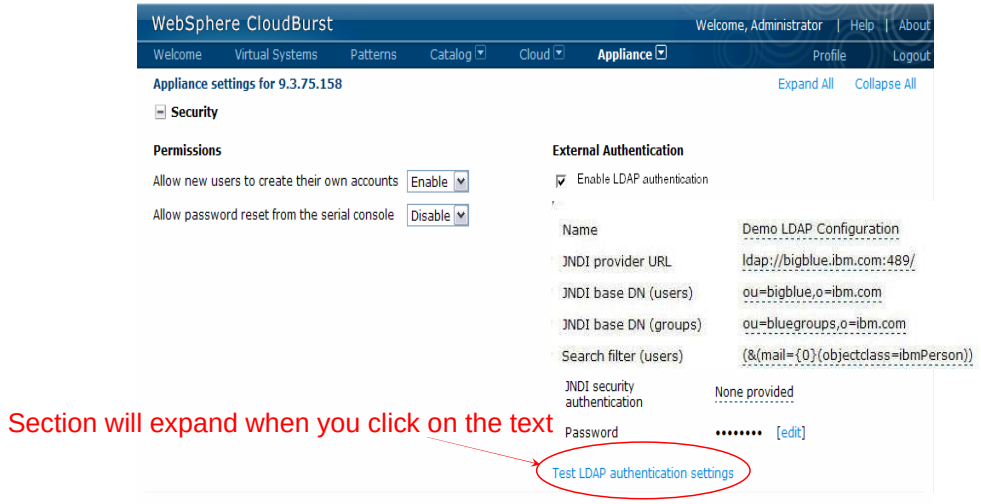
- To enable LDAP authentication, go to the **Appliance > Settings** page and expand the **Security** section



© 2010 IBM Corporation

To configure your appliance to authenticate users with an LDAP directory, go to “Appliance”, then “Settings” from the Web console top menu and expand the “Security” section. The enable LDAP authentication check box is not set by default. You must select the “Enable LDAP authentication” check box and enter the information for your external LDAP server for WebSphere CloudBurst to use the specified LDAP server to authenticate users at log in. You should you perform the LDAP authentication test described in the next two slides, before enabling LDAP security.

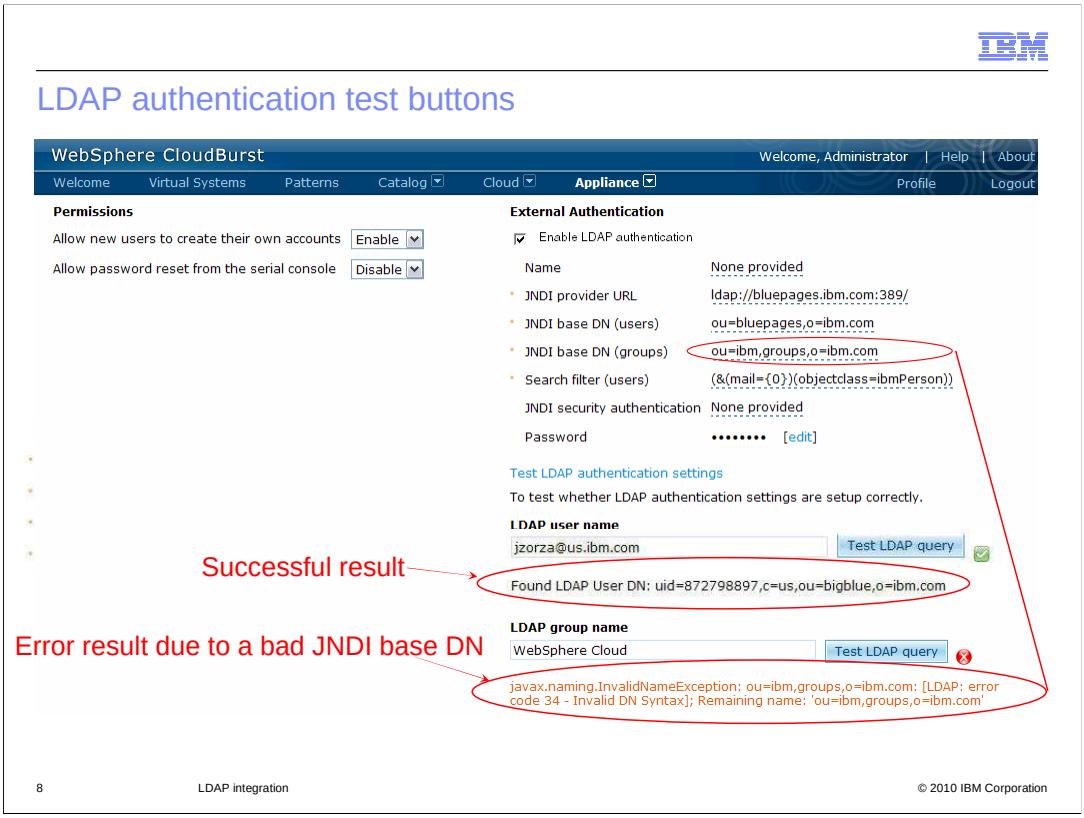
LDAP authentication test



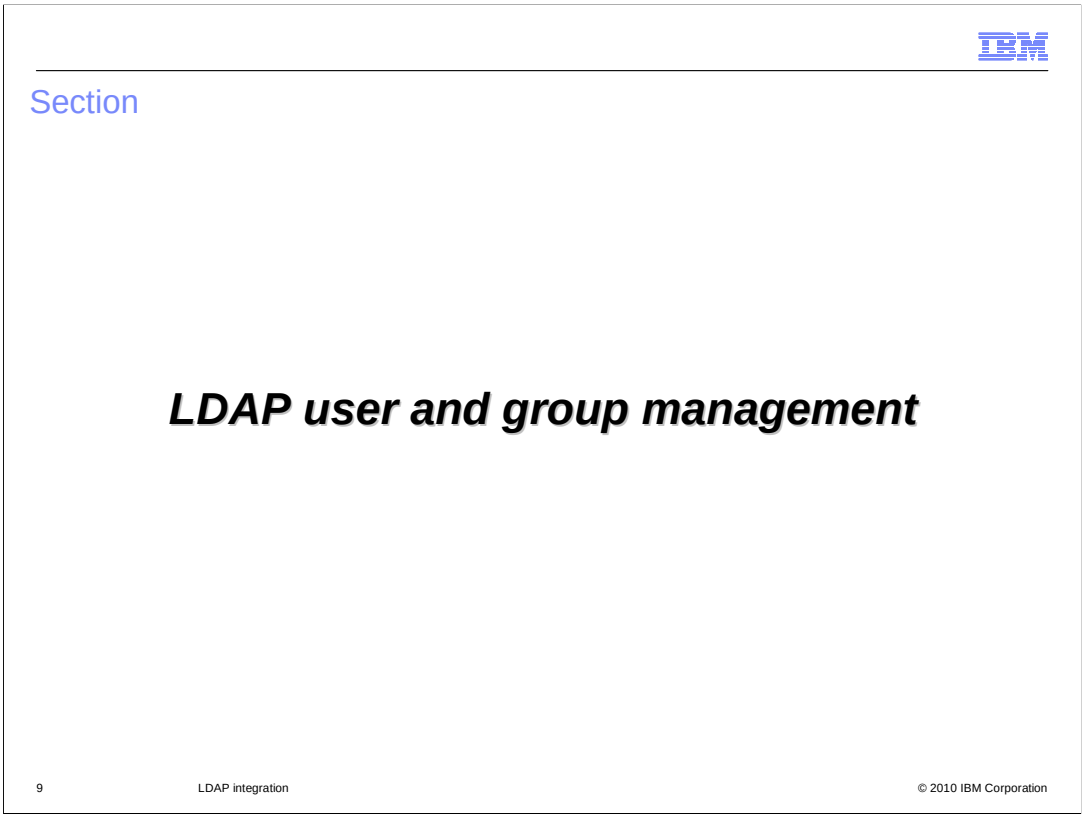
7 LDAP integration © 2010 IBM Corporation

Initial LDAP setup for new users can be a challenging task. In previous releases when LDAP authentication was not working, the only way to find out what was wrong was to enable trace, look at the trace.log, and find exceptions in the log. Therefore, the WebSphere CloudBurst product has provided some test buttons to verify the LDAP integration is working. Again, you should use the “Test LDAP authentication” function before enabling LDAP security.

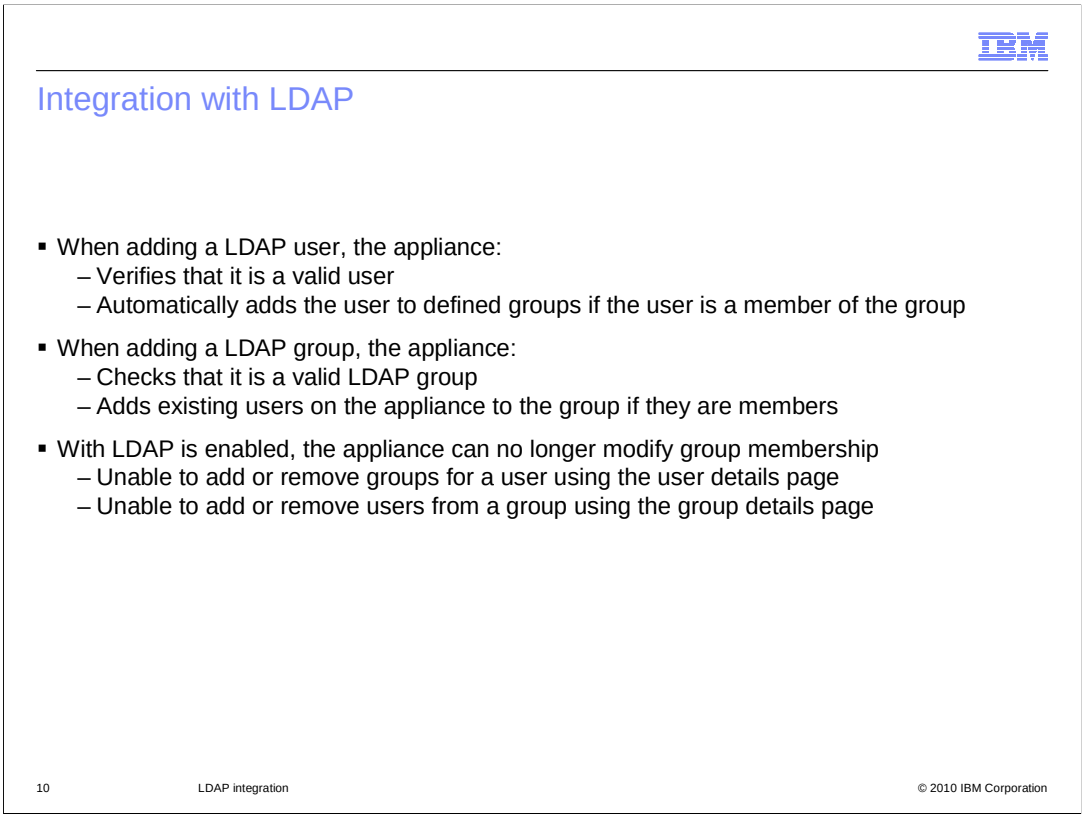
To work with these test tools, click the blue “Test LDAP authentication settings” text to expand the verification section.



WebSphere CloudBurst has provided a validation function to test the connection to the LDAP server by submitting a query to find a particular LDAP user name or LDAP group name. When successful, the user Distinguished Name (DN) or group Distinguished Name is displayed. When the query is unsuccessful, a “Could not find LDAP user name or group name” message will be displayed. If there is an error with the LDAP parameters or if a connection to the LDAP server can not be established, an exception.getMessage() will be displayed. The example here shows an error result due to a bad JNDI base DN parameter.



This section of the presentation focuses on the management of LDAP users and groups.



The appliance has two authentication schemes -- you can either use the local registry or an LDAP server, but not both (except for the cbadmin user which is always stored locally). When LDAP authentication is enabled, defined users are stored locally on the appliance, but the authentication happens against the LDAP directory server. So, when adding a LDAP user, WebSphere CloudBurst will verify that it is a valid user with the LDAP directory, define that user locally and will automatically add the user to any groups to which the user has been assigned.

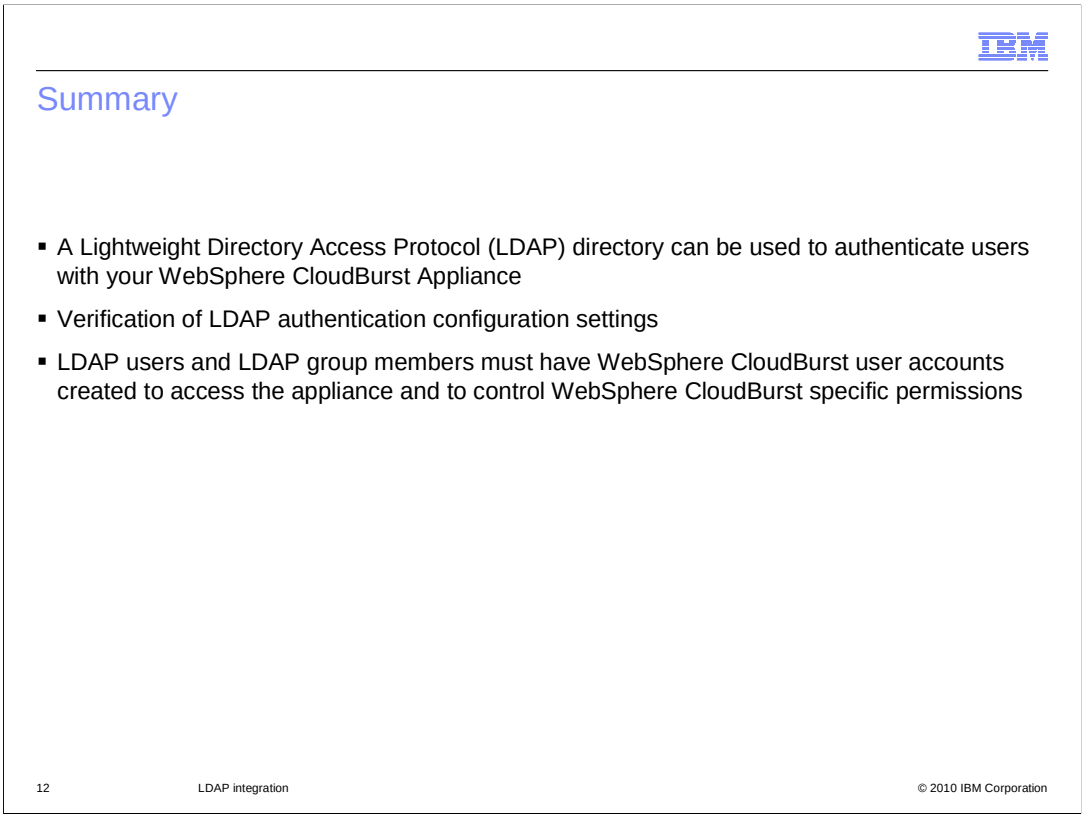
When adding an LDAP group to the appliance, WebSphere CloudBurst will verify that it is a valid group with the LDAP directory and will add any users who have been defined on the appliance to the group if they are members.

Every user that will need to access the appliance must be defined using the normal WebSphere CloudBurst user account creation process.

Defining an LDAP group with WebSphere CloudBurst does not allow all users of that group automatic access to the WebSphere CloudBurst Appliance. In fact, the primary reason to define LDAP groups with WebSphere CloudBurst is so you can set permissions all at once at the group level, not to permit all users in the group access to the appliance.

Since the LDAP account and group creation is restricted by whoever controls the LDAP directory, LDAP group membership can not be modified from the WebSphere CloudBurst Appliance. So, when LDAP is enabled, the “Add more…” text field under the “User groups” section of the User panel and the Add more…” text field under “Group membership” section of the “User Groups” panel are not displayed, so you can no longer modify group membership from the appliance.

This section is the summary.



IBM WebSphere CloudBurst Appliance offers LDAP integration to provide an additional layer of security to the appliance and LDAP authentication verification tools to verify the correct configuration of the LDAP server. When LDAP security is enabled, the LDAP directory server manages user authentication and group membership; while permissions and authorization to WebSphere CloudBurst resources are handled by the appliance.

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 e-mail feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_CB11_LDAPIntegration.ppt

This module is also available in PDF format at: ../CB11_LDAPIntegration.pdf

© 2010 IBM Corporation

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

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, CloudBurst, 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

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.

© Copyright International Business Machines Corporation 2010. All rights reserved.

© 2010 IBM Corporation