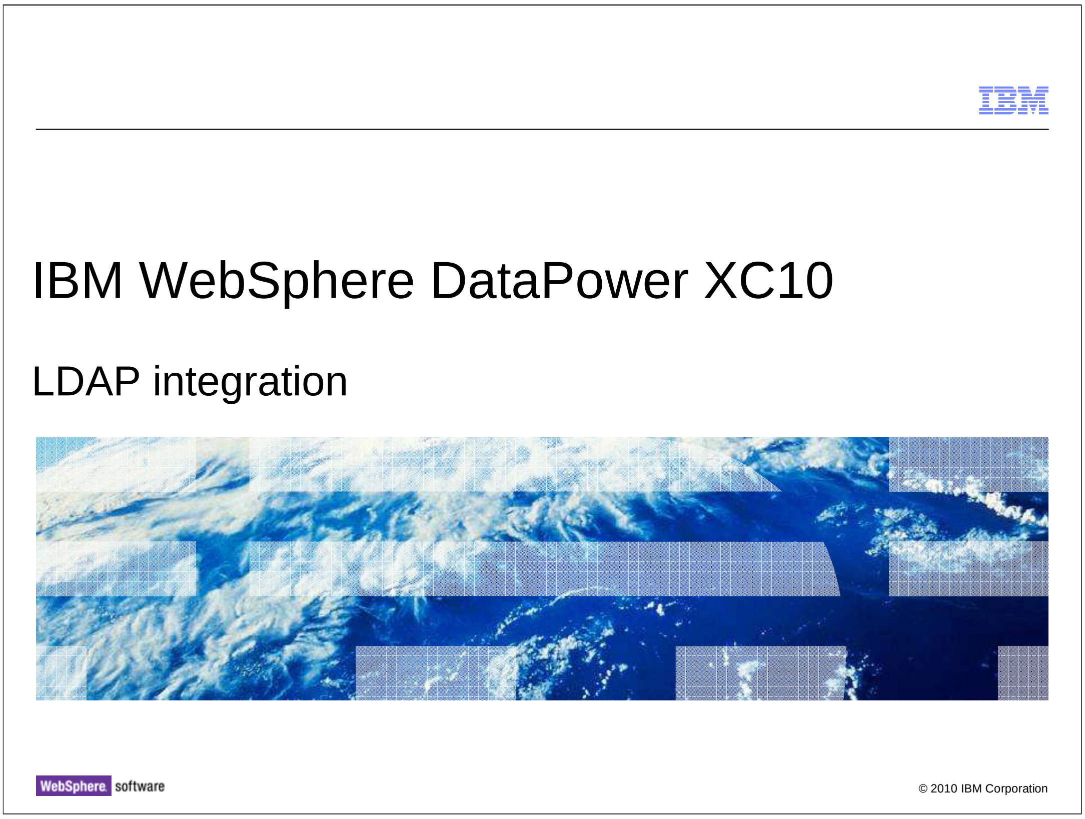
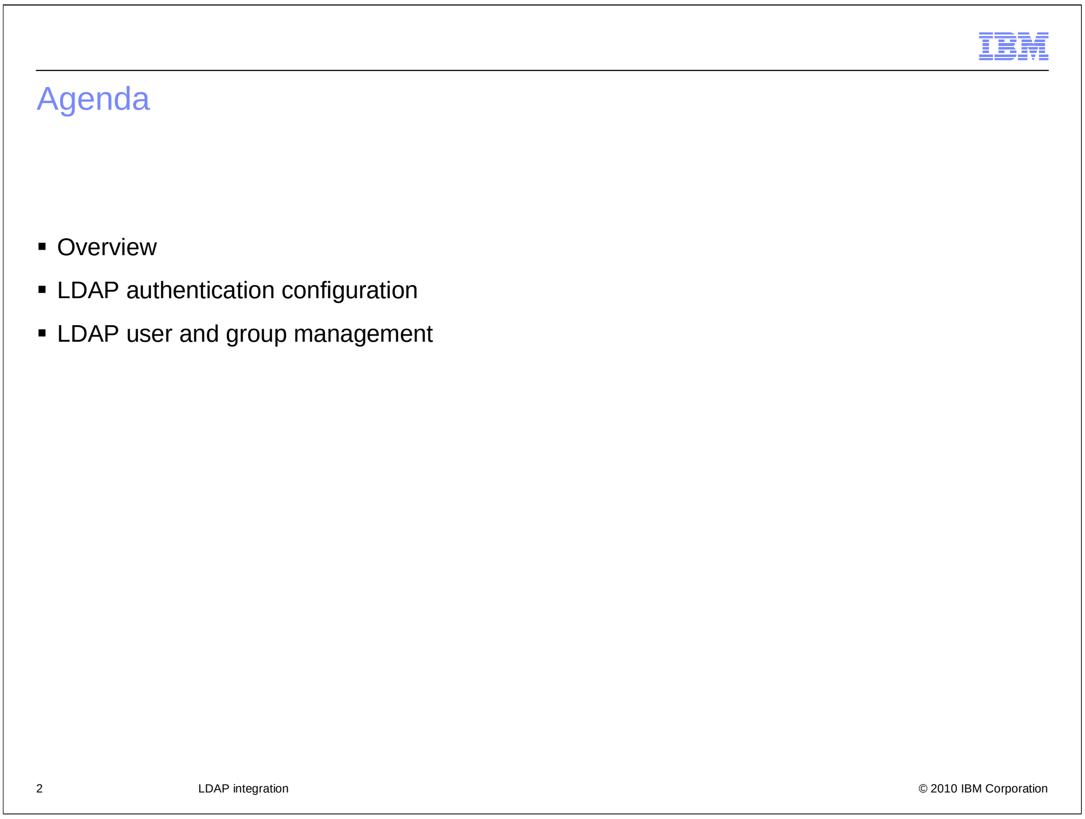


IBM WebSphere DataPower XC10

LDAP integration

This presentation provides an overview of the Lightweight Directory Access Protocol, or LDAP, integration features of the IBM WebSphere® DataPower™ XC10 Appliance.



Agenda

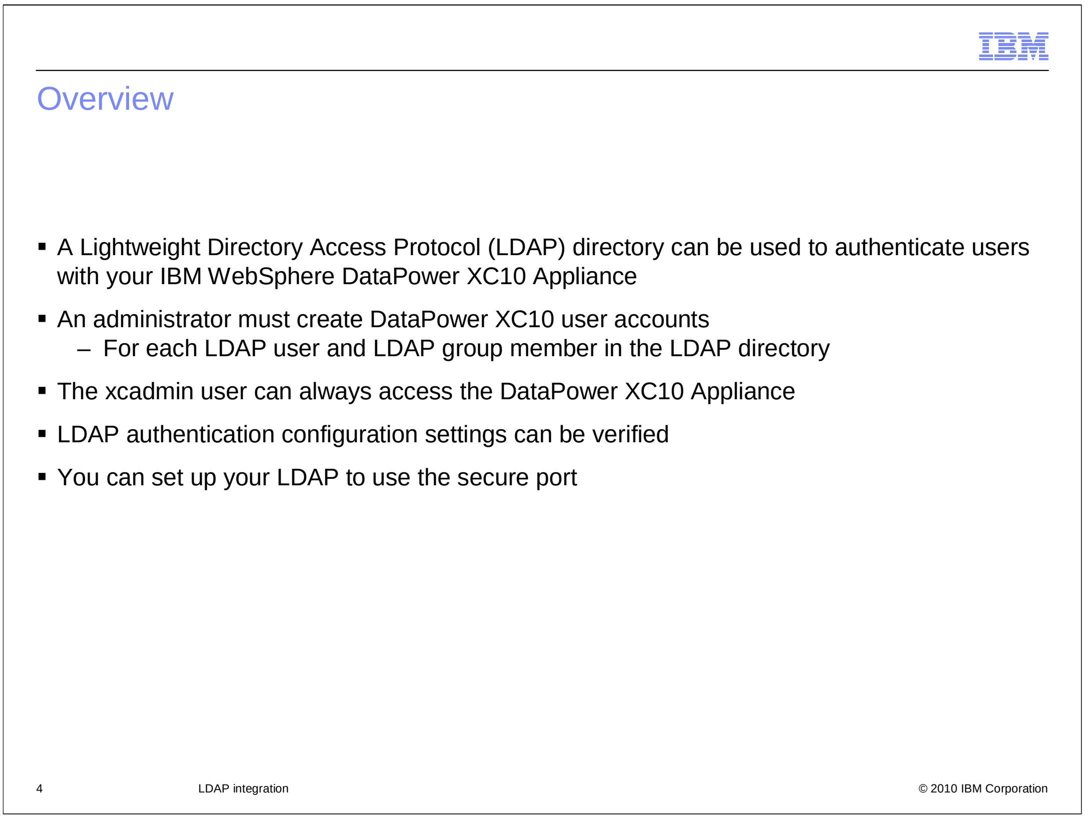
- Overview
- LDAP authentication configuration
- LDAP user and group management

This presentation starts with an overview of LDAP integration with DataPower XC10, then covers how to configure and verify the LDAP authentication, followed by the details of LDAP user and group management.

Section

Overview

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 IBM WebSphere DataPower XC10 Appliance
- An administrator must create DataPower XC10 user accounts
  - For each LDAP user and LDAP group member in the LDAP directory
- The xcadmin user can always access the DataPower XC10 Appliance
- LDAP authentication configuration settings can be verified
- You can set up your LDAP to use the secure port

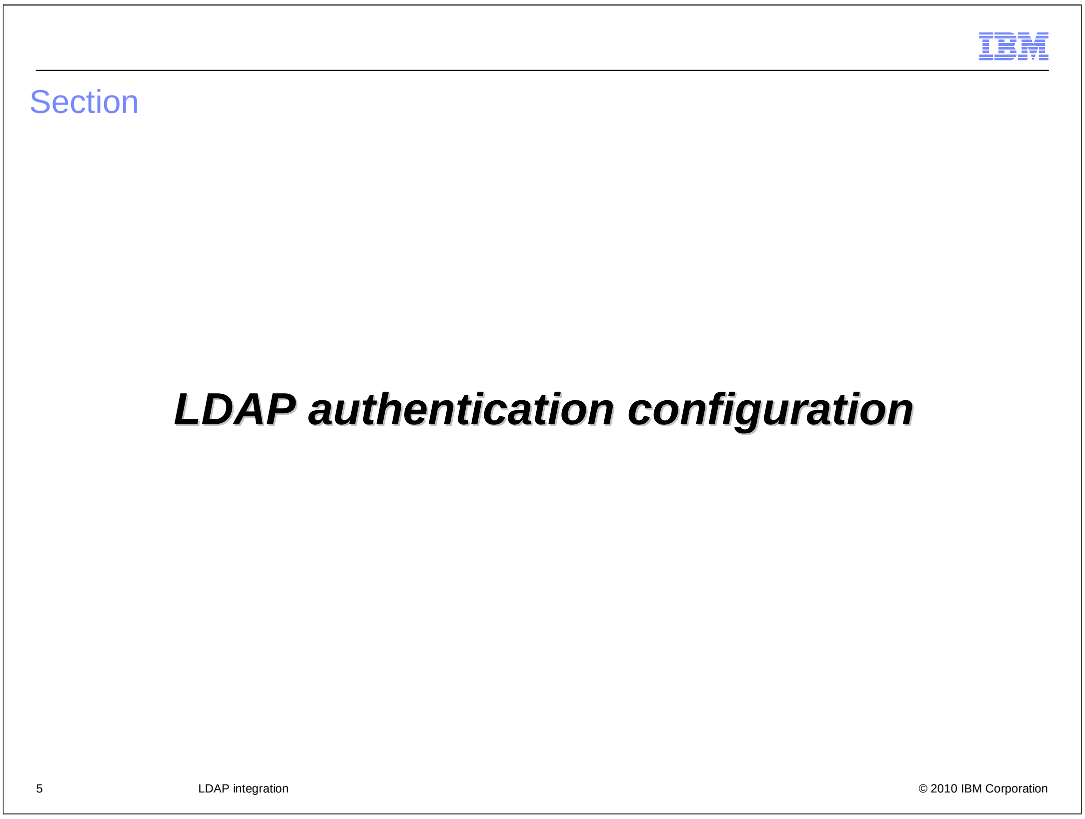
4 LDAP integration © 2010 IBM Corporation

Local authentication is a great way to get started with DataPower XC10. However, if the DataPower XC10 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 DataPower XC10 user accounts created to access the appliance. Furthermore, DataPower XC10 users that are not registered in the LDAP directory cannot be authenticated. The one exception to this rule is the xcadmin user. Credentials for the xcadmin user always rely on the internal appliance security registry, so even if your LDAP directory server is down, the xcadmin user can access the appliance.

You can set up your LDAP to use the secure port. The secure sockets layer (SSL) certificate of the LDAP server must be issued by a publicly trusted certificate authority (CA), which is already in the <JAVA_HOME>/jre/lib/security/cacerts file. WebSphere DataPower XC10 Appliance does not support using self-signed certificates

Additionally, DataPower XC10 product has provided test buttons to verify that the LDAP authentication configuration settings are working as planned.



Section

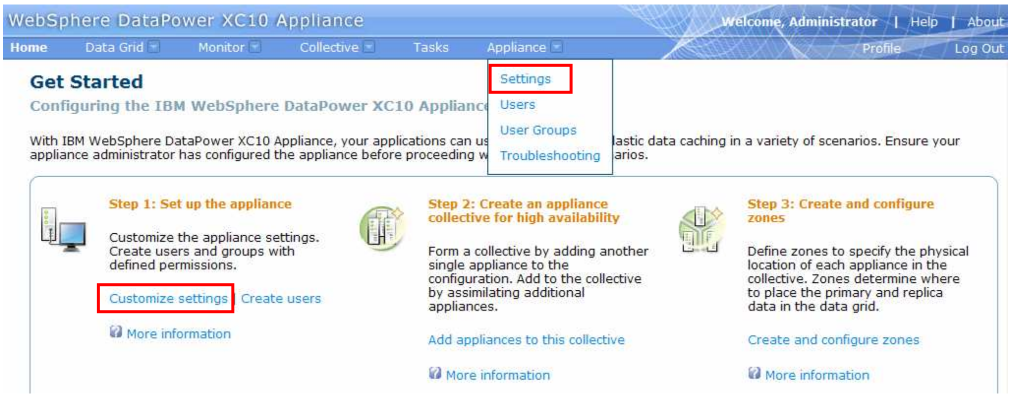
LDAP authentication configuration

5 LDAP integration © 2010 IBM Corporation

This section of the presentation focuses on the process of configuring your DataPower XC10 Appliance for LDAP authentication using the web console.

Navigate to the settings panel

- Go to the **Appliance > Settings** page and expand the **Security** section
- Click **Customize settings** link and expand the **Security** section



Get Started

Configuring the IBM WebSphere DataPower XC10 Applianc

With IBM WebSphere DataPower XC10 Appliance, your applications can us lastic data caching in a variety of scenarios. Ensure your appliance administrator has configured the appliance before proceeding w arios.

Step 1: Set up the appliance

Customize the appliance settings. Create users and groups with defined permissions.

Customize settings | Create users

More information

Step 2: Create an appliance collective for high availability

Form a collective by adding another single appliance to the configuration. Add to the collective by assimilating additional appliances.

Add appliances to this collective

More information

Step 3: Create and configure zones

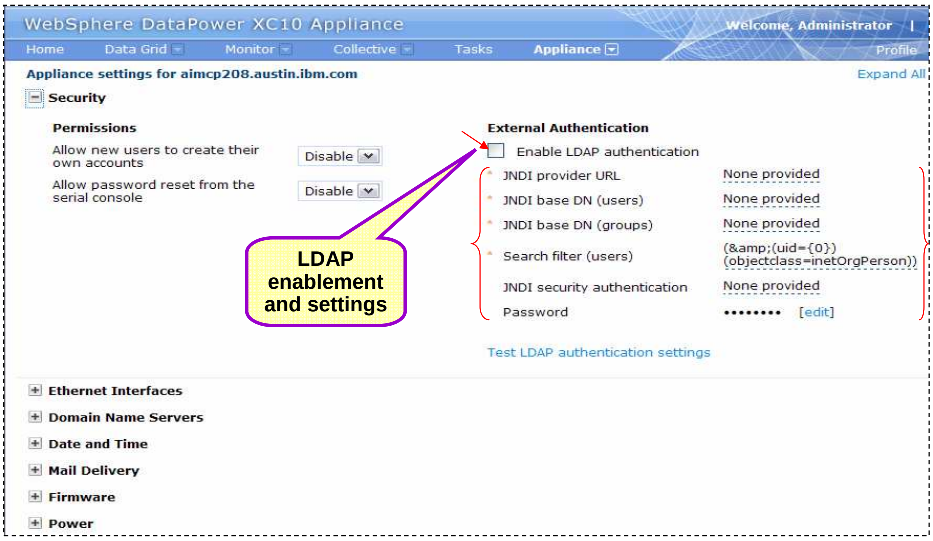
Define zones to specify the physical location of each appliance in the collective. Zones determine where to place the primary and replica data in the data grid.

Create and configure zones

More information

To configure your appliance to authenticate users with an LDAP directory, go to “Appliance”, then “Settings” from the web console top menu. Click “Customize settings” and expand the “Security” section.

Security



Appliance settings for aimcp208.austin.ibm.com

Security

Permissions

Allow new users to create their own accounts	Disable
Allow password reset from the serial console	Disable

External Authentication

□ Enable LDAP authentication

* JNDI provider URL	None provided
* JNDI base DN (users)	None provided
* JNDI base DN (groups)	None provided
* Search filter (users)	(&amp;(uid={0})(objectclass=inetOrgPerson))
JNDI security authentication	None provided
Password	•••••••• [edit]

Test LDAP authentication settings

Ethernet Interfaces

Domain Name Servers

Date and Time

Mail Delivery

Firmware

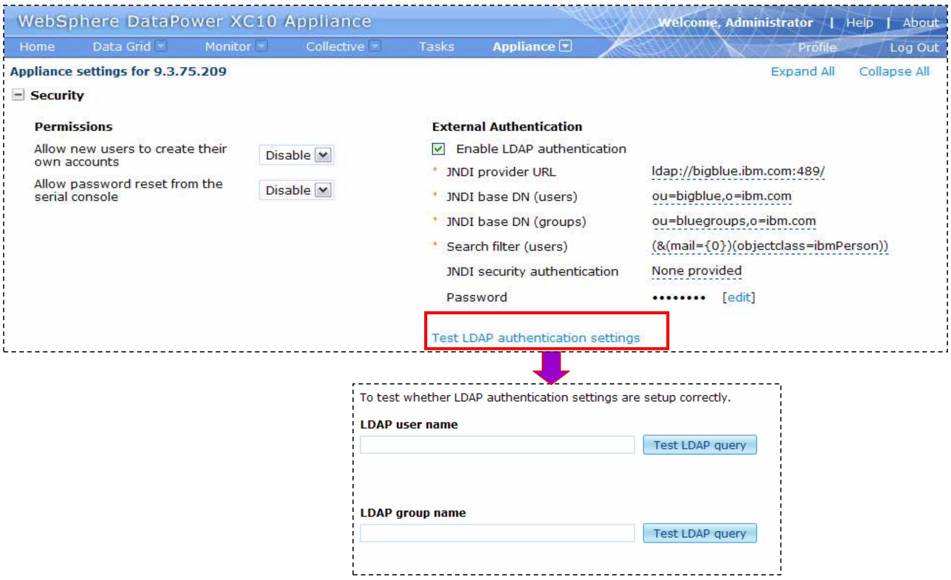
Power

LDAP enablement and settings

Within the security settings section, you can customize some of the settings for permissions and external authentication. Within permissions, you can allow or disallow new users to create their own accounts within the appliance. Also, you can allow or disallow a password reset from within the serial console. External authentication allows you to enable LDAP authentication and provides the capability to test the LDAP settings.

To configure your appliance to authenticate users with an LDAP directory, you must select the “Enable LDAP authentication” check box. The Enable LDAP authentication check box is not selected by default. Selecting this check box enables WebSphere DataPower XC10 appliance to use the specified LDAP server to authenticate users at login.

LDAP authentication test



Appliance settings for 9.3.75.209

Security

Permissions

Allow new users to create their own accounts: Disable

Allow password reset from the serial console: Disable

External Authentication

☑ Enable LDAP authentication

* JNDI provider URL	ldap://bigblue.ibm.com:489/
* JNDI base DN (users)	ou=bigblue,o=ibm.com
* JNDI base DN (groups)	ou=bluegroups,o=ibm.com
* Search filter (users)	(&(mail={0})(objectclass=ibmPerson))
JNDI security authentication	None provided
Password	•••••••• [edit]

Test LDAP authentication settings

To test whether LDAP authentication settings are setup correctly.

LDAP user name

LDAP group name

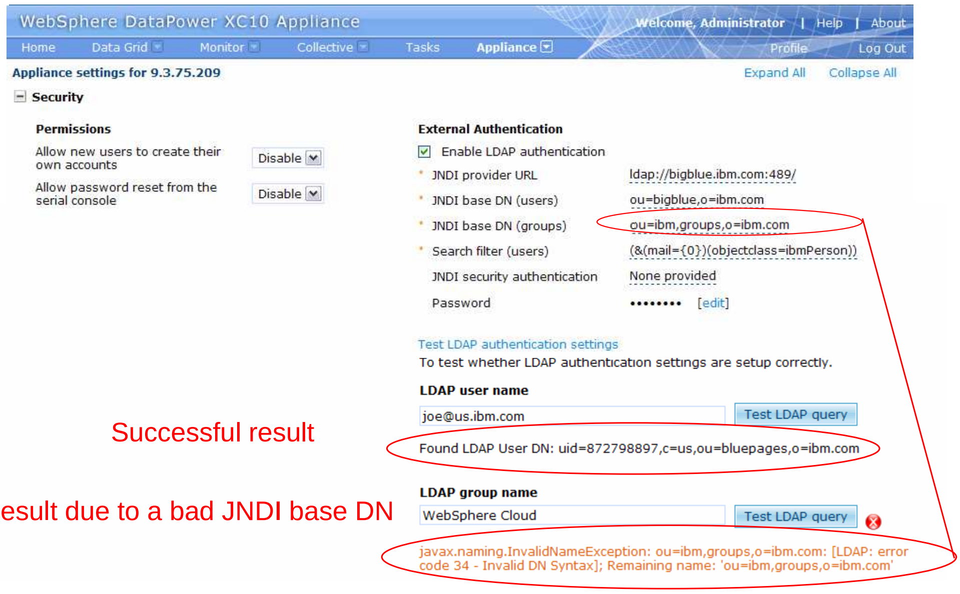
8 LDAP integration © 2010 IBM Corporation

To set up the LDAP external authentication is not an easy task for first time users. In previous releases when LDAP authentication was not working, the only way to find out what was wrong was to look at the logs. DataPower XC10 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. Enter the LDAP user name the click the associated **Test LDAP query** button. If the query is successful, then a message is displayed as follows: *Found LDAP User DN: <user information>*. If the query is not successful, then an error message is displayed

Similarly enter the LDAP group name then click the associated “**Test LDAP query**” button. If the query is successful, then a message is displayed as follows: *Found LDAP Group DN: <user information>*. If the query is not successful, then an error message is displayed.

LDAP authentication test buttons



Appliance settings for 9.3.75.209

Security

Permissions

Allow new users to create their own accounts: Disable

Allow password reset from the serial console: Disable

External Authentication

☑ Enable LDAP authentication

* JNDI provider URL: ldap://bigblue.ibm.com:489/

* JNDI base DN (users): ou=bigblue,o=ibm.com

* JNDI base DN (groups): ou=ibm,groups,o=ibm.com

* Search filter (users): (&(mail={0})(objectclass=ibmPerson))

JNDI security authentication: None provided

Password: •••••••• [edit]

Test LDAP authentication settings

To test whether LDAP authentication settings are setup correctly.

LDAP user name

joe@us.ibm.com [Test LDAP query]

Found LDAP User DN: uid=872798897,c=us,ou=bluepages,o=ibm.com

LDAP group name

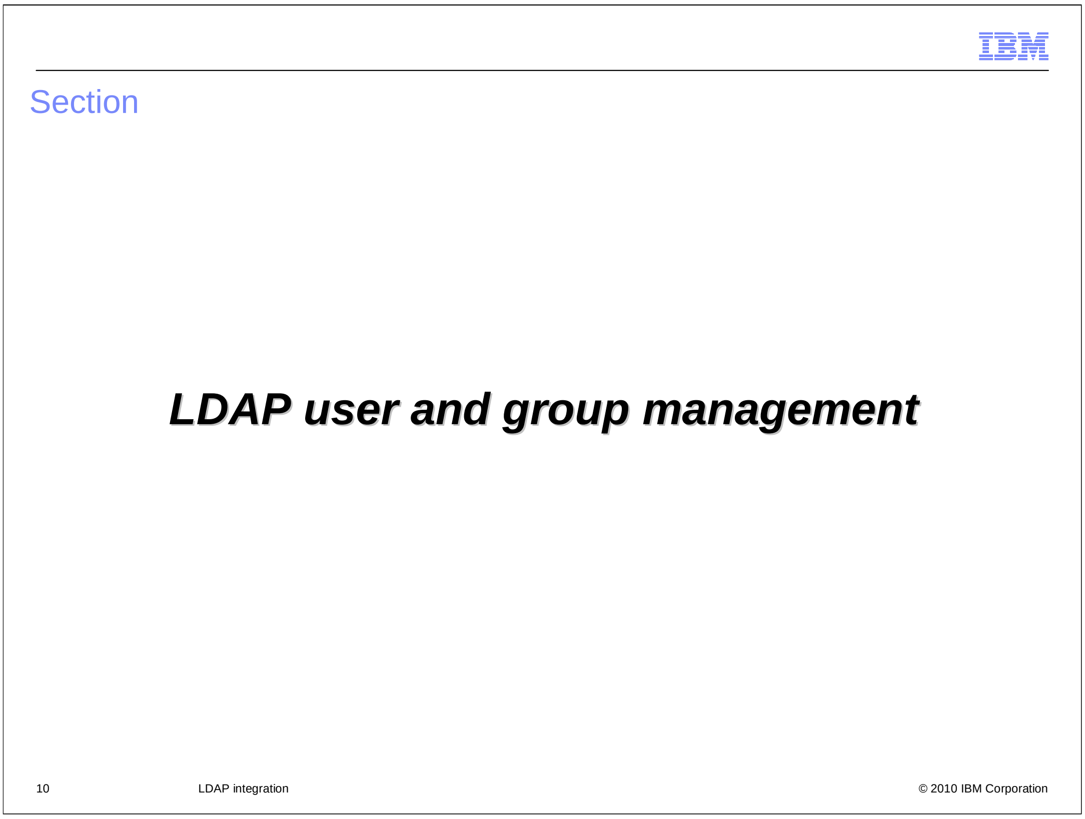
WebSphere Cloud [Test LDAP query]

javax.naming.InvalidNameException: ou=ibm,groups,o=ibm.com: [LDAP: error code 34 - Invalid DN Syntax]; Remaining name: 'ou=ibm,groups,o=ibm.com'

Successful result

Error result due to a bad JNDI base DN

The way the validation works is by submitting a query to find a particular LDAP user name or LDAP group name. When successful, the 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 is displayed. If there is an error with the LDAP parameters or if a connection to the LDAP server cannot be established, an exception.getMessage() is displayed. The example here shows an error result due to a bad JNDI base DN parameter.

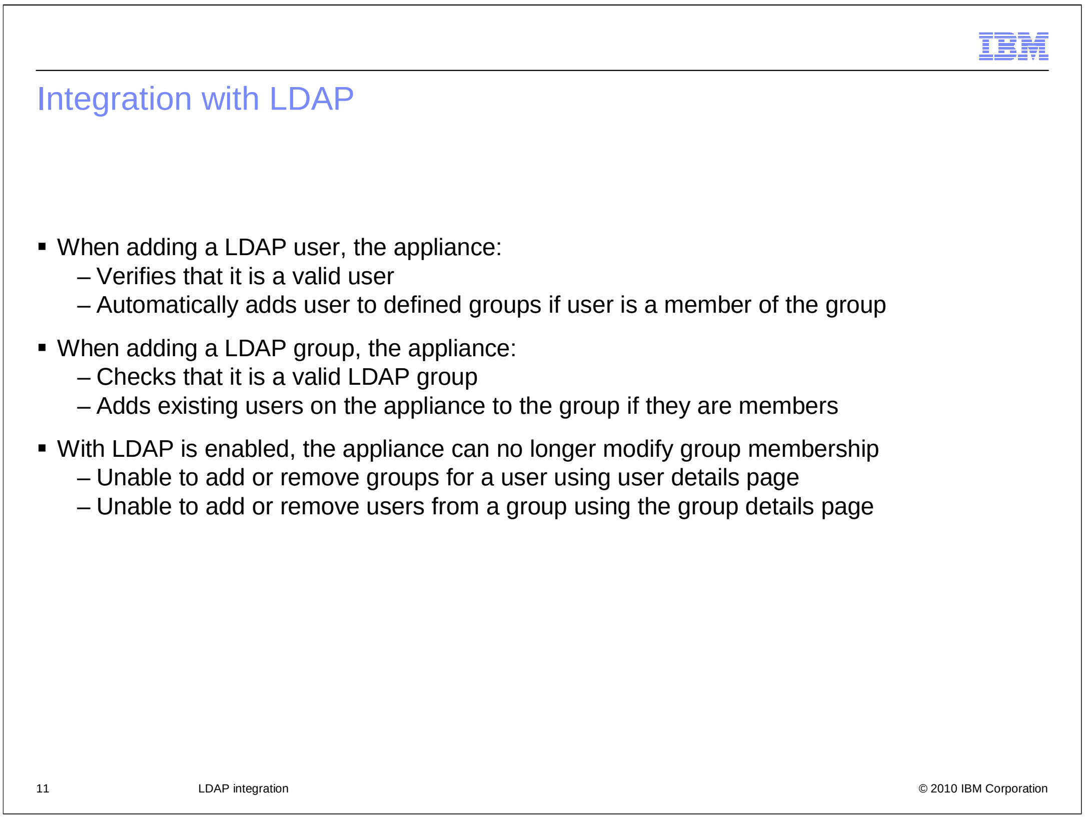


Section

LDAP user and group management

10 LDAP integration © 2010 IBM Corporation

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



Integration with LDAP

- When adding a LDAP user, the appliance:
  - Verifies that it is a valid user
  - Automatically adds user to defined groups if user is a member of the group
- When adding a LDAP group, the appliance:
  - Checks that it is a valid LDAP group
  - Adds existing users on the appliance to the group if they are members
- With LDAP is enabled, the appliance can no longer modify group membership
  - Unable to add or remove groups for a user using user details page
  - Unable to add or remove users from a group using the group details page

11 LDAP integration © 2010 IBM Corporation

The appliance has two authentication schemes -- you can either use the local registry or an LDAP server, but not both (except for the xcadmin 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. When adding an LDAP user, DataPower XC10 will verify that it is a valid user with the LDAP directory. It will also define that user locally and will automatically adds user to any groups to which they have been assigned.

When adding an LDAP group to the appliance, DataPower XC10 will verify that it is a valid group with the LDAP directory. It will also 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 DataPower XC10 user account creation process.

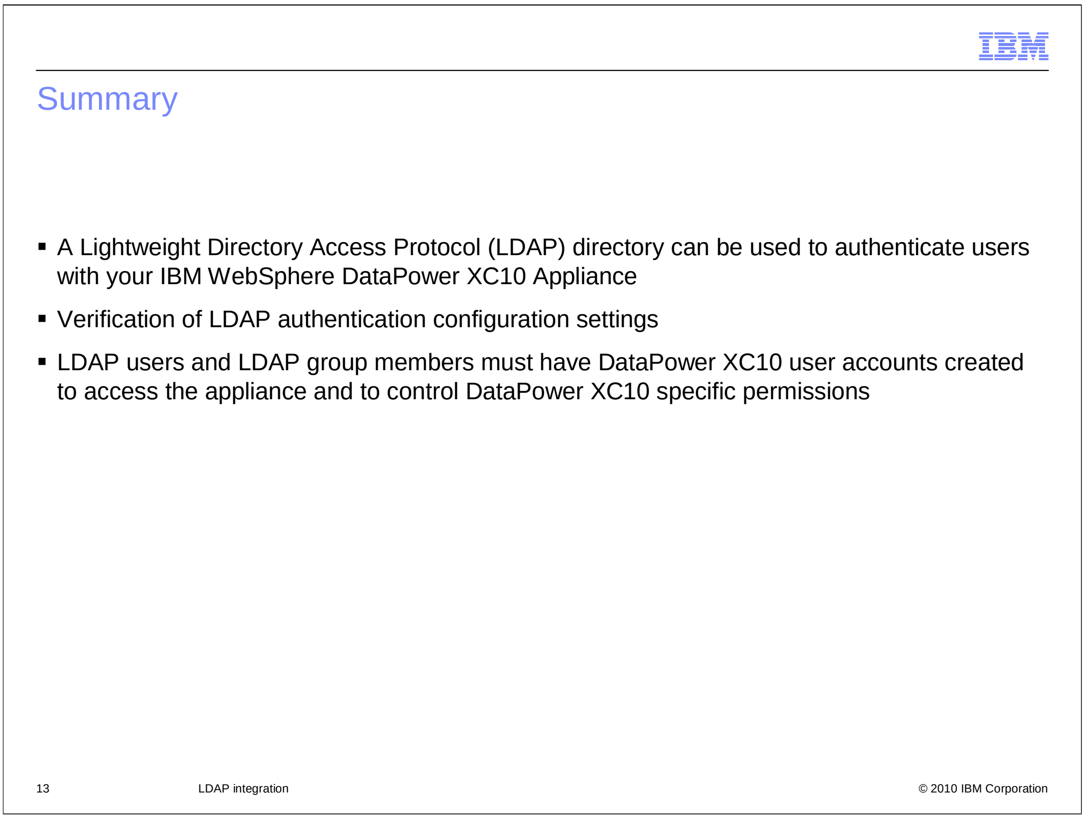
Defining an LDAP group with DataPower XC10 does not allow all users of that group automatic access to the DataPower XC10 Appliance. In fact, the primary reason for defining LDAP groups with DataPower XC10 is so you can set permissions all at once at the group level, permitting all users in the group access to the appliance.

Since the LDAP account and group creation is restricted by whoever controls the LDAP directory, LDAP group membership cannot be modified from the DataPower XC10 Appliance. Therefore, 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. This means that you can no longer modify group membership from the appliance.

Section

Summary

This section provides a summary of the presentation.

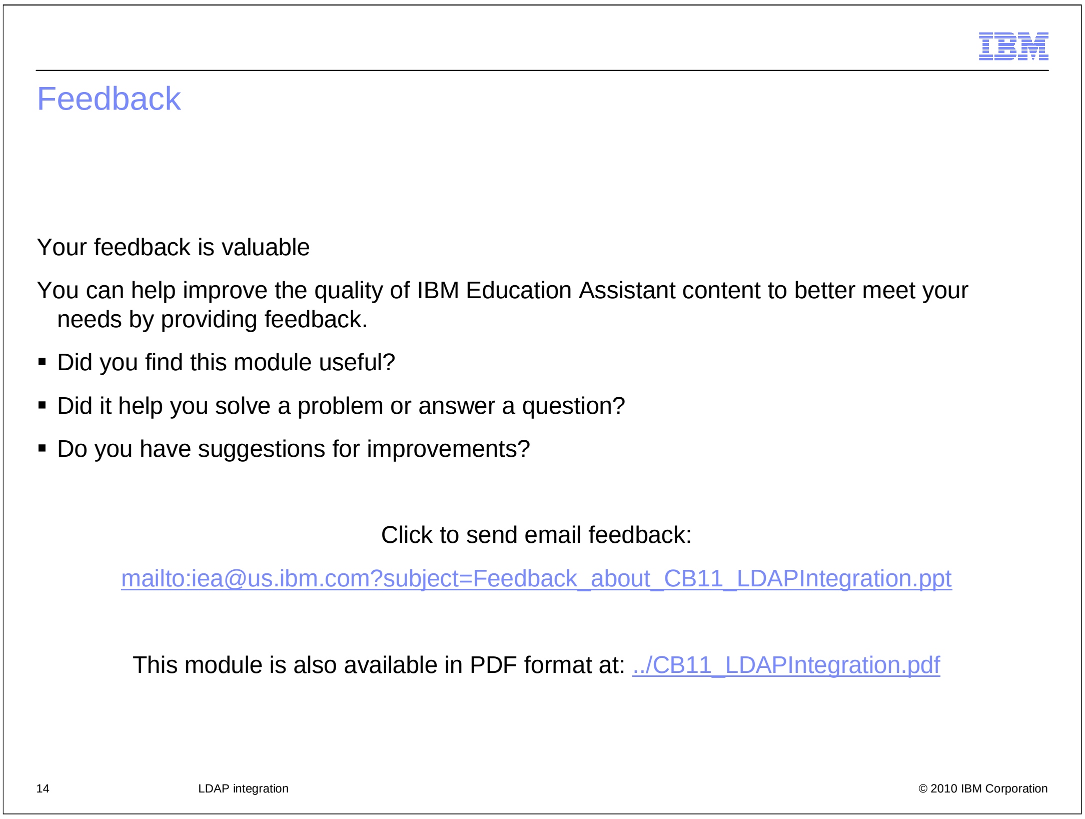


Summary

- A Lightweight Directory Access Protocol (LDAP) directory can be used to authenticate users with your IBM WebSphere DataPower XC10 Appliance
- Verification of LDAP authentication configuration settings
- LDAP users and LDAP group members must have DataPower XC10 user accounts created to access the appliance and to control DataPower XC10 specific permissions

13 LDAP integration © 2010 IBM Corporation

The IBM WebSphere DataPower XC10 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 DataPower XC10 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.

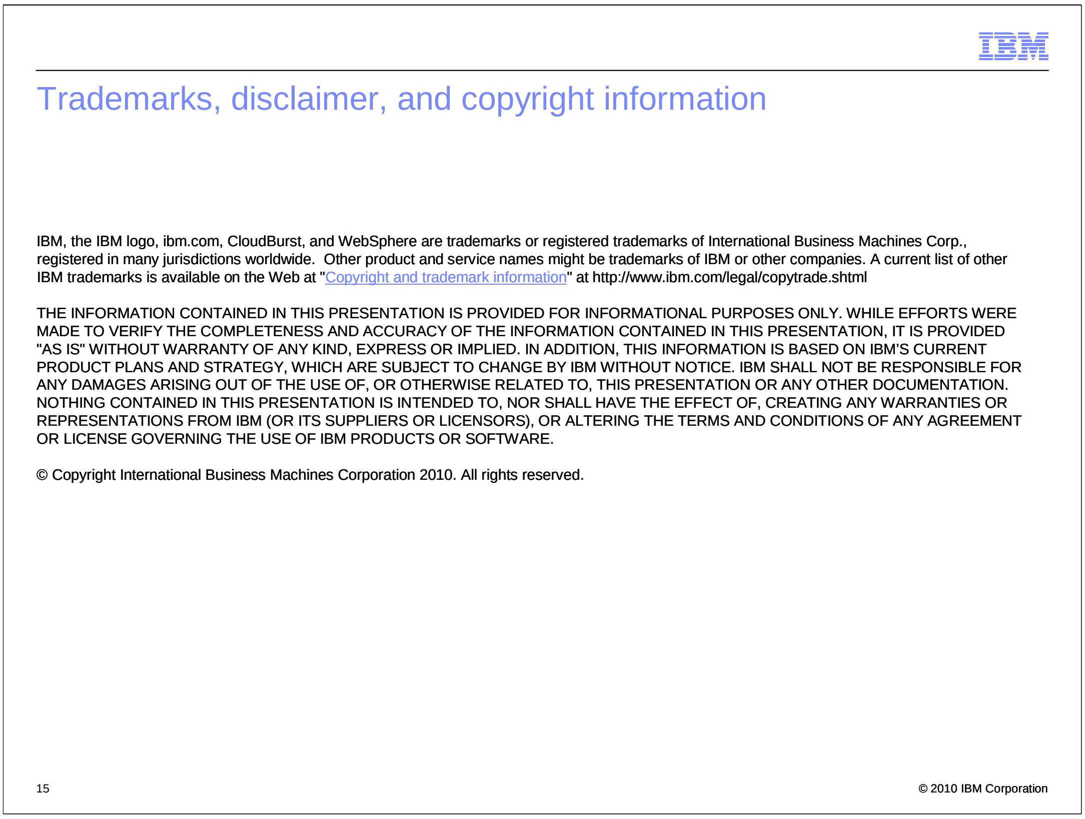
- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

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

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

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.