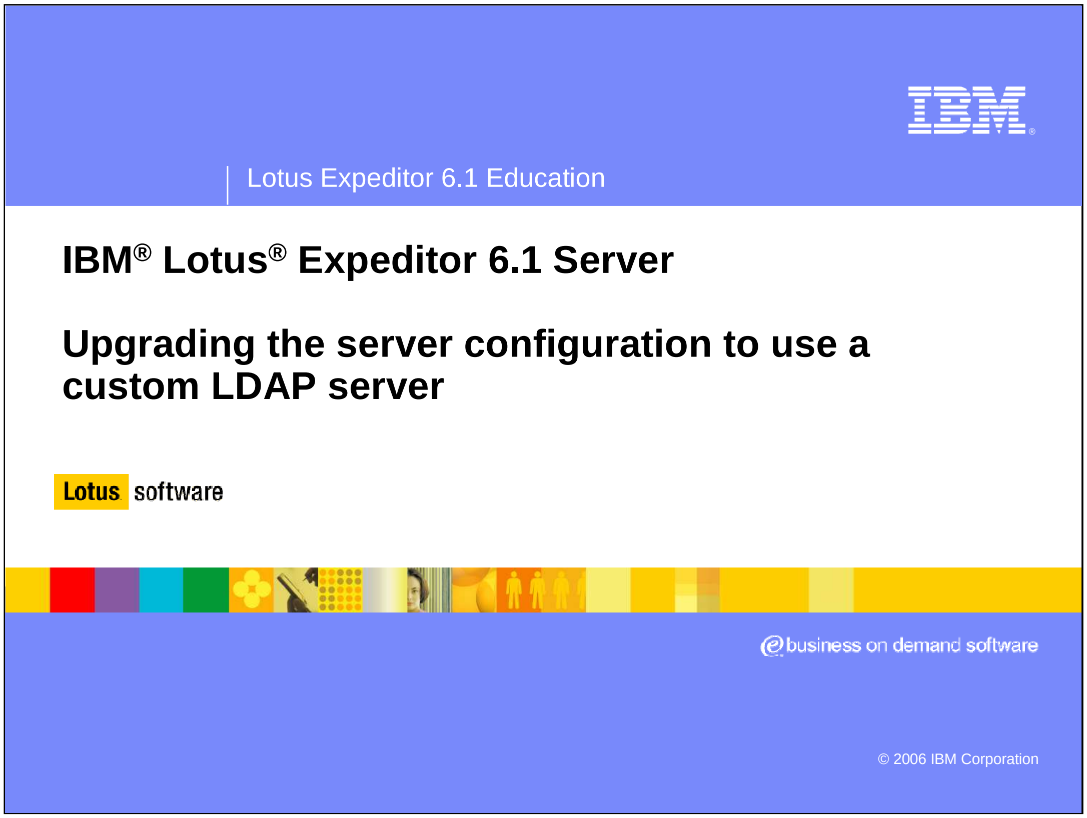


Lotus Expeditor 6.1 Education

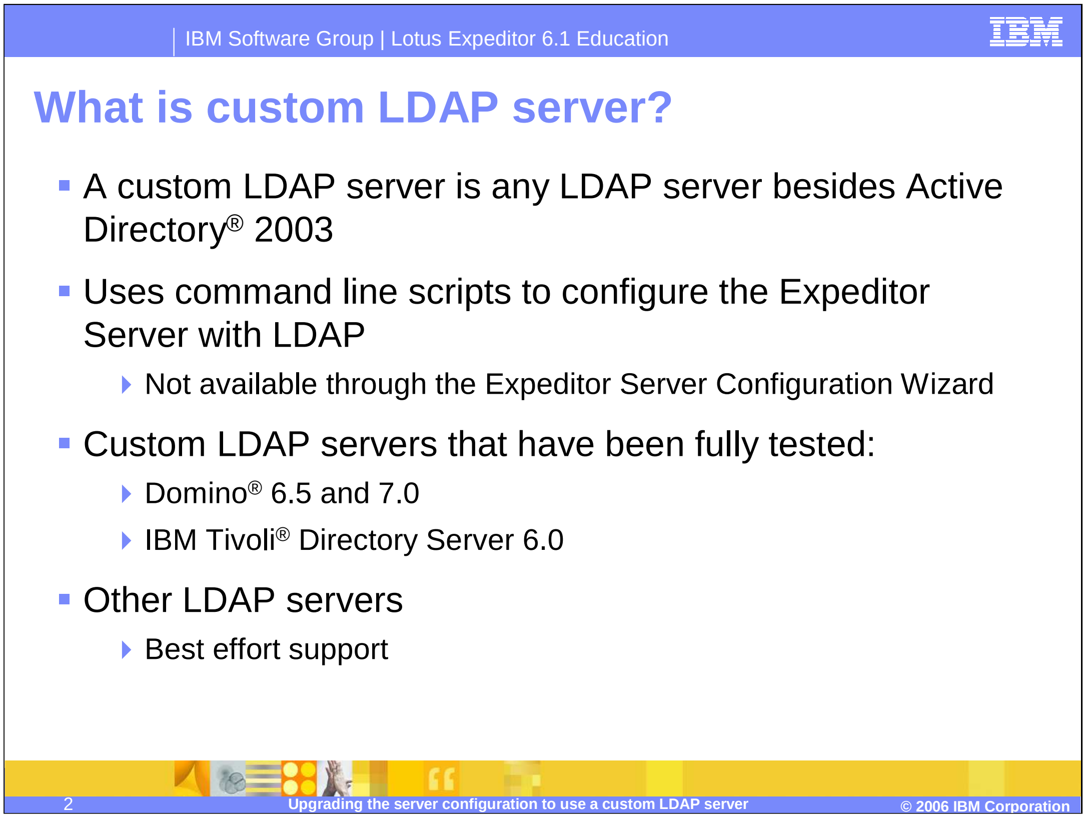
IBM® Lotus® Expeditor 6.1 Server

Upgrading the server configuration to use a custom LDAP server

Lotus software

business on demand software

Hello, and welcome to this presentation on upgrading the Lotus Expeditor 6.1 Server configuration to a custom LDAP.



IBM Software Group | Lotus Expeditor 6.1 Education

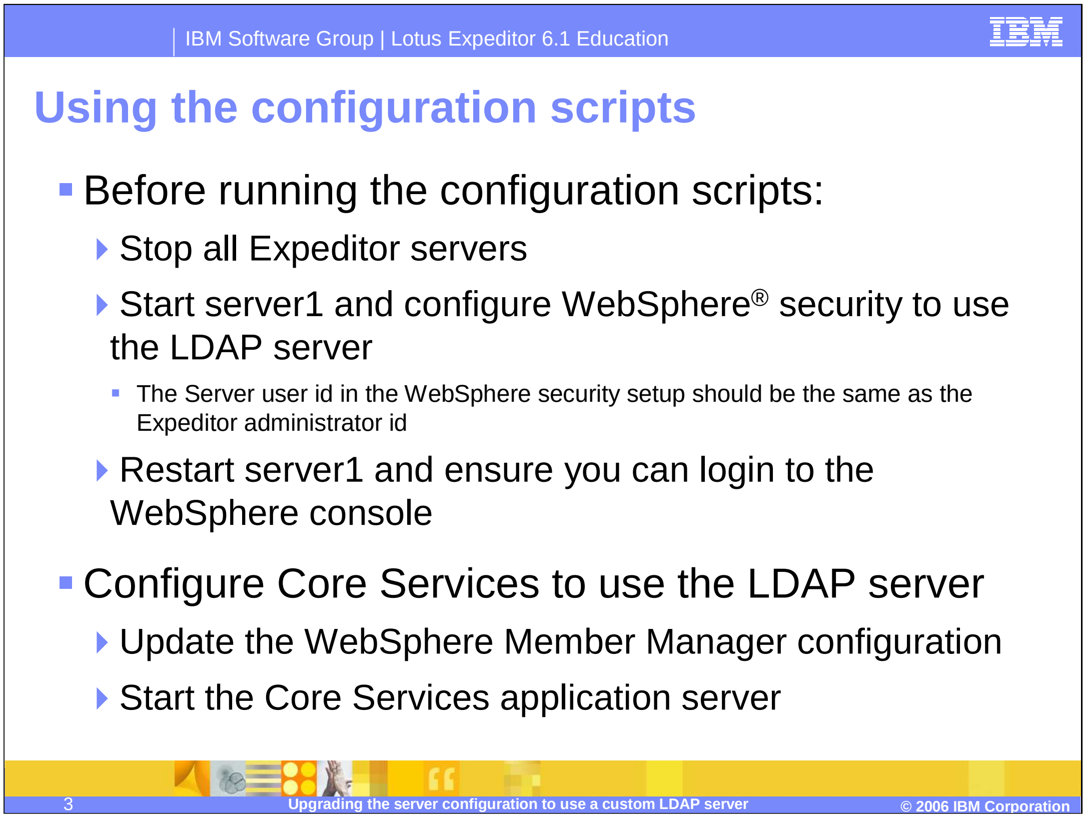
What is custom LDAP server?

- A custom LDAP server is any LDAP server besides Active Directory® 2003
- Uses command line scripts to configure the Expeditor Server with LDAP
  - Not available through the Expeditor Server Configuration Wizard
- Custom LDAP servers that have been fully tested:
  - Domino® 6.5 and 7.0
  - IBM Tivoli® Directory Server 6.0
- Other LDAP servers
  - Best effort support

2 Upgrading the server configuration to use a custom LDAP server

We use the term custom LDAP to refer to any LDAP besides Active Directory 2003. Active Directory 2003 is configured using the Expeditor Server configuration wizard. Custom LDAPs are configured using command line scripts and cannot be configured using the configuration wizard.

IBM has fully tested Domino 6.5 and 7.0, as well as Tivoli Directory Server 6.0. Other LDAP servers should work with the custom LDAP configuration process as long as they comply with standard LDAP protocol. These LDAP servers are supported on a best effort basis. See the Supported hardware and software section of the Expeditor Server Information Center for the support statement on LDAP servers.



IBM Software Group | Lotus Expeditor 6.1 Education

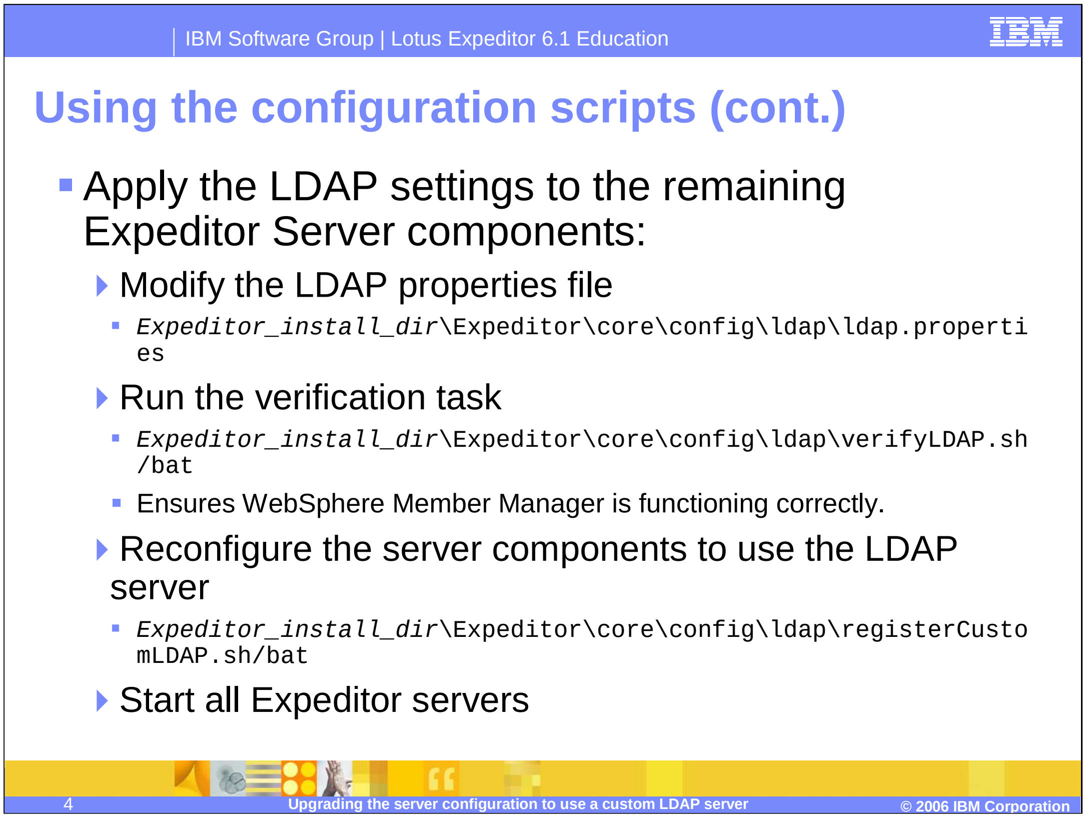
Using the configuration scripts

- Before running the configuration scripts:
  - Stop all Expeditor servers
  - Start server1 and configure WebSphere® security to use the LDAP server
    - The Server user id in the WebSphere security setup should be the same as the Expeditor administrator id
  - Restart server1 and ensure you can login to the WebSphere console
- Configure Core Services to use the LDAP server
  - Update the WebSphere Member Manager configuration
  - Start the Core Services application server

3 Upgrading the server configuration to use a custom LDAP server © 2006 IBM Corporation

Before running the configuration scripts, perform the following steps: Step 1, stop all Expeditor servers. Step 2, start server1 and configure WebSphere security to use the LDAP server. Make sure to set the server user id in the WebSphere security setup to the Expeditor Server administrator id. Step 3, restart server1 and make sure you can log in to the WebSphere console.

Next, configure core services to use the LDAP server by updating the WebSphere Member Manager configuration file. Start the core services application server before continuing.

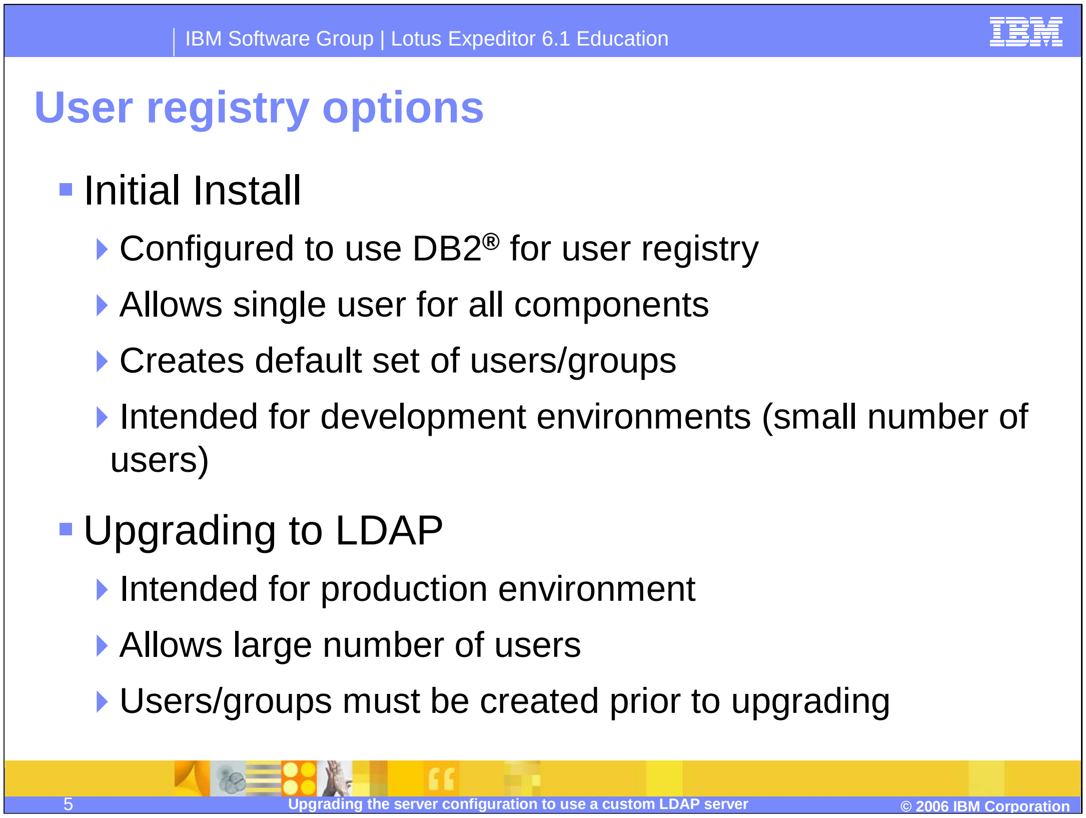


Using the configuration scripts (cont.)

- Apply the LDAP settings to the remaining Expeditor Server components:
  - Modify the LDAP properties file
    - *Expeditor_install_dir*\Expeditor\core\config\ldap\ldap.properties
  - Run the verification task
    - *Expeditor_install_dir*\Expeditor\core\config\ldap\verifyLDAP.sh/bat
    - Ensures WebSphere Member Manager is functioning correctly.
  - Reconfigure the server components to use the LDAP server
    - *Expeditor_install_dir*\Expeditor\core\config\ldap\registerCustomLDAP.sh/bat
  - Start all Expeditor servers

To apply the LDAP setting to all the Expeditor Server components, modify the LDAP properties file with the Expeditor Server administrator id and password and the administrator group and synchronization group. Then run the verifyLDAP command to ensure WebSphere Member Manager is functioning properly and the required users and groups can be accessed.

Finally, run the registerCustomLDAP command to configure all Expeditor Server components to use the LDAP server. This step updates the component configuration with the new LDAP information. Start all the servers when this command completes.



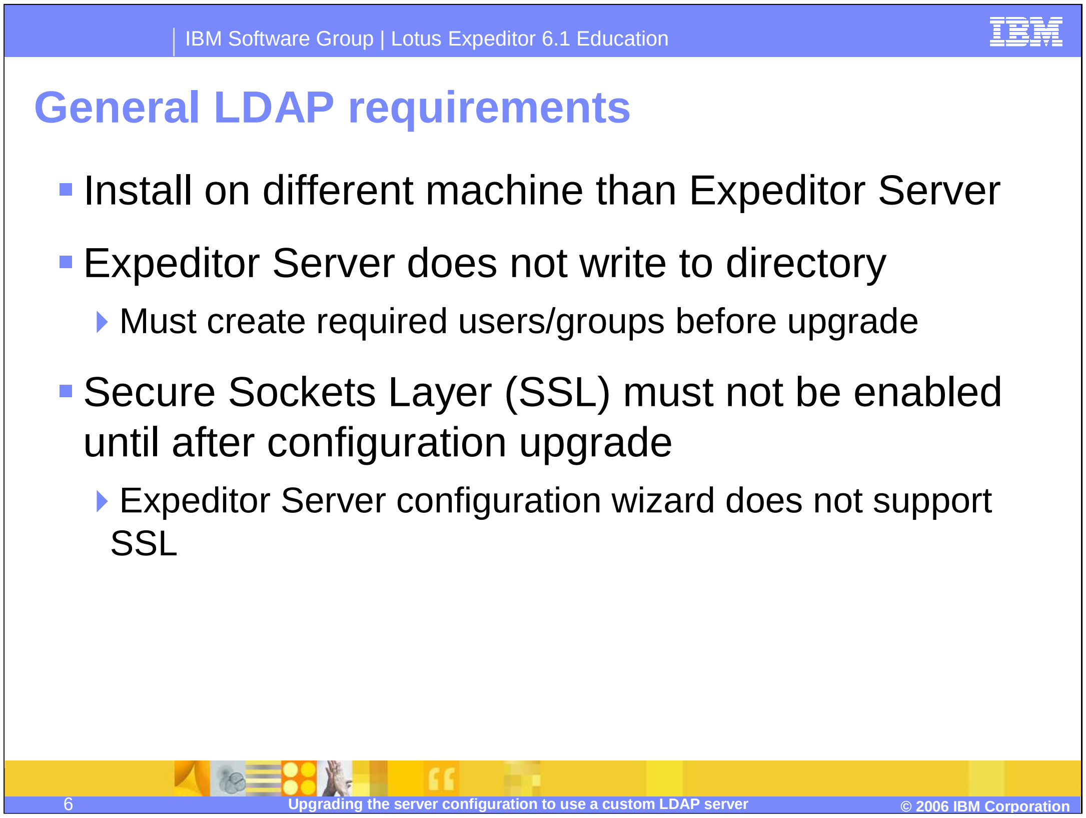
User registry options

- Initial Install
  - Configured to use DB2® for user registry
  - Allows single user for all components
  - Creates default set of users/groups
  - Intended for development environments (small number of users)
- Upgrading to LDAP
  - Intended for production environment
  - Allows large number of users
  - Users/groups must be created prior to upgrading

During the initial install of the Expeditor server, a DB2 database will be configured to hold the user registry information used by Expeditor Server components. Also a default set of users and groups will be created in the database registry. The database registry is intended for development environments with a small number of users. It is not intended to be used in production.

Upgrade to LDAP if you intend to use the server in a production environment with a large number of users. Required users and groups must be created in the LDAP server before upgrading the server configuration.

Note that Active Directory 2003 is supported using the configuration wizard. More information about using the configuration wizard to upgrade to Active Directory 2003 can be found on the IBM Education Assistant site under Active Directory 2003 configuration.



IBM Software Group | Lotus Expeditor 6.1 Education

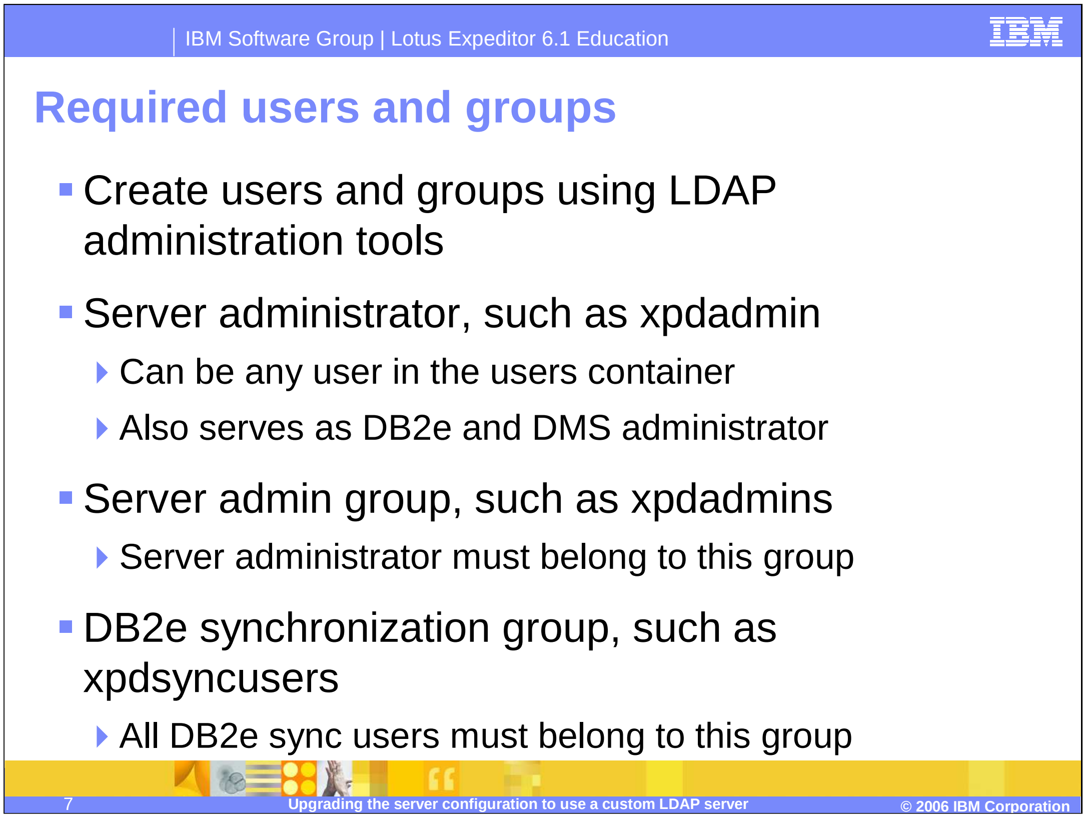
General LDAP requirements

- Install on different machine than Expeditor Server
- Expeditor Server does not write to directory
  - Must create required users/groups before upgrade
- Secure Sockets Layer (SSL) must not be enabled until after configuration upgrade
  - Expeditor Server configuration wizard does not support SSL

6 Upgrading the server configuration to use a custom LDAP server © 2006 IBM Corporation

The LDAP server must be installed on a different machine than the Expeditor Server. Since the Expeditor Server does not attempt to write to the directory, you must create the required users and groups before upgrading to the LDAP server.

Make sure that SSL is not enabled until after the upgrade. The Expeditor Server configuration scripts do not support SSL. A non-SSL port must be accessible by the configuration scripts.



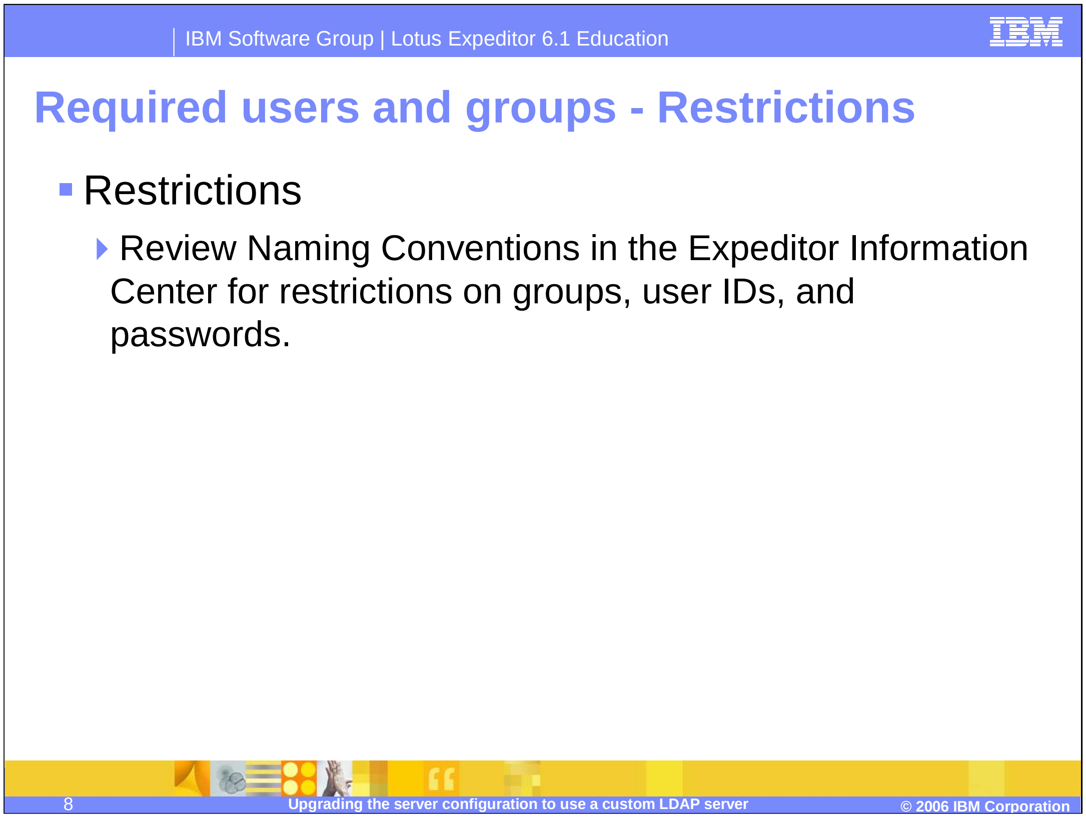
IBM Software Group | Lotus Expeditor 6.1 Education

Required users and groups

- Create users and groups using LDAP administration tools
- Server administrator, such as xpdadmin
  - Can be any user in the users container
  - Also serves as DB2e and DMS administrator
- Server admin group, such as xpdadmins
  - Server administrator must belong to this group
- DB2e synchronization group, such as xpdsyncusers
  - All DB2e sync users must belong to this group

7 Upgrading the server configuration to use a custom LDAP server © 2006 IBM Corporation

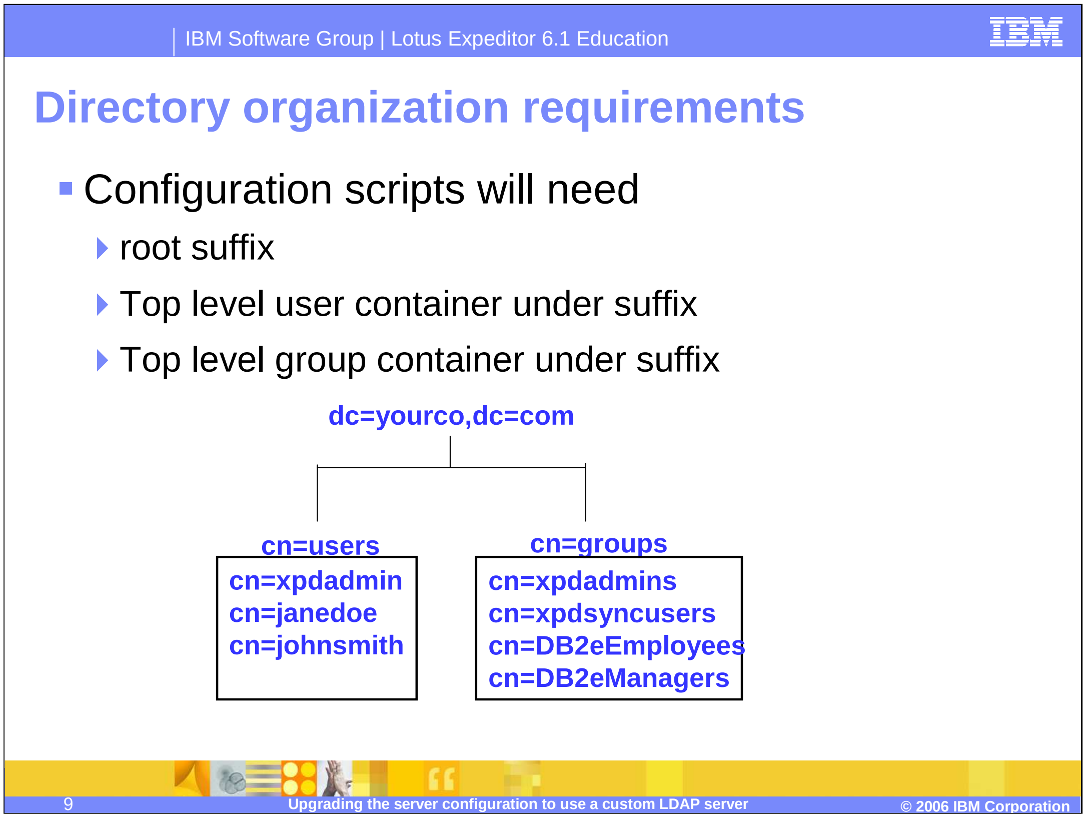
Before running the configuration wizard, you will need to create some required users and groups. For users, the Expeditor Server administrator user must be created. For groups, the Expeditor Server administrators group and the DB2e synchronization group must be created. All server administrator users must belong to the administrators group and all DB2e synchronization users must belong to the DB2e synchronization group.



Required users and groups - Restrictions

- Restrictions
  - Review Naming Conventions in the Expeditor Information Center for restrictions on groups, user IDs, and passwords.

The Expeditor Server has restrictions on the characters which may appear in groups, users and passwords. Review the Expeditor Server Information Center for information on the supported naming conventions before upgrading to LDAP.



Directory organization requirements

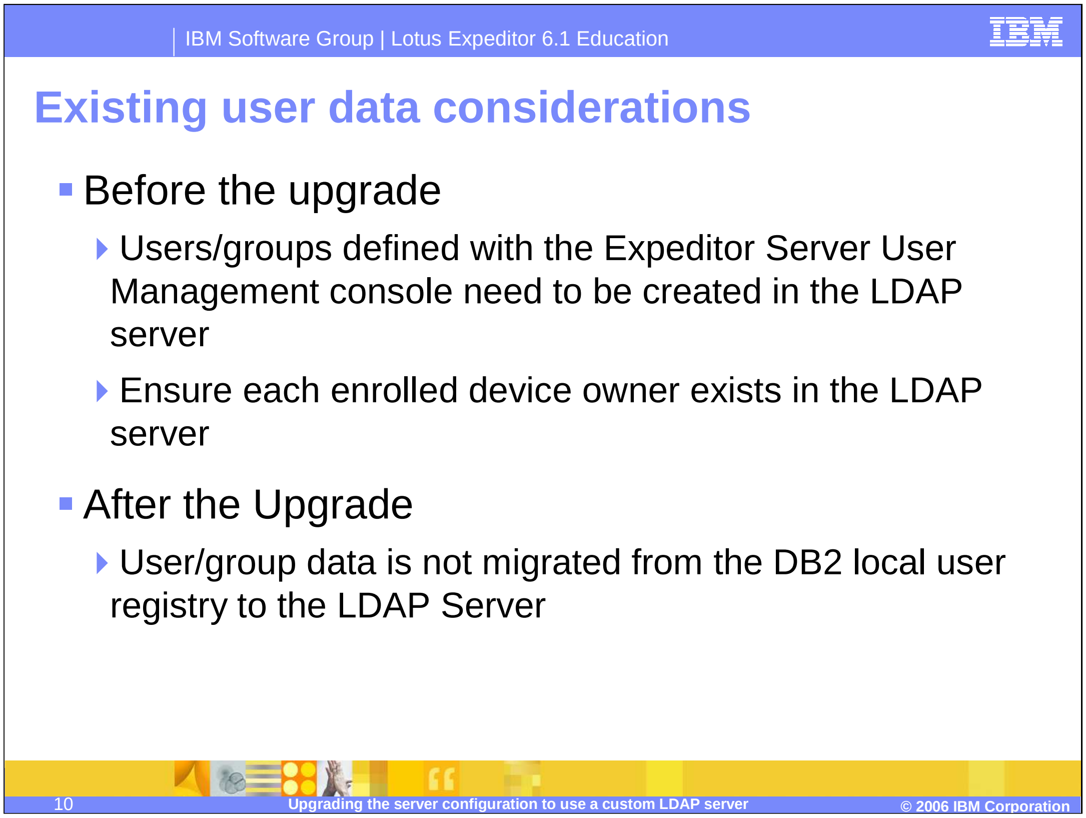
- Configuration scripts will need
  - root suffix
  - Top level user container under suffix
  - Top level group container under suffix

dc=yourco,dc=com

cn=users
cn=xpdadmin
cn=janedoe
cn=johnsmith

cn=groups
cn=xpdadmins
cn=xpdsyncusers
cn=DB2eEmployees
cn=DB2eManagers

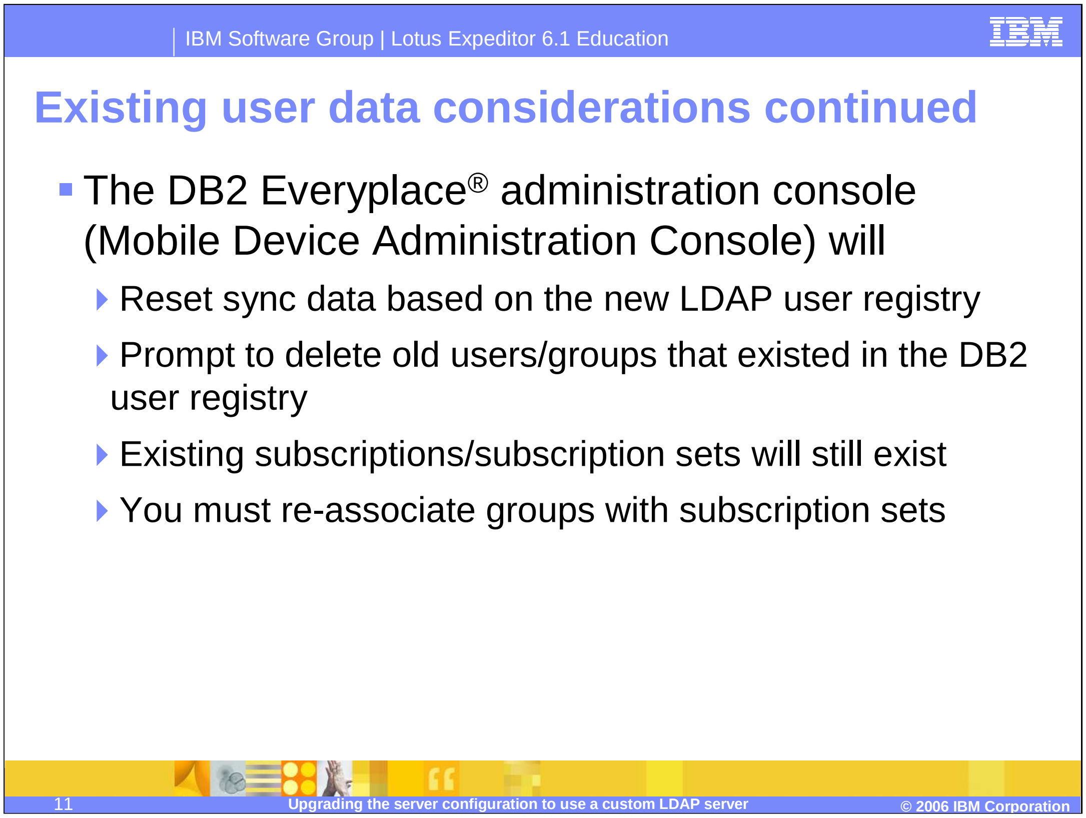
Before running the configuration, you will need to gather some information about your directory structure. You will need the root suffix for your users and groups and the top level containers for users and the top level containers for groups.



Existing user data considerations

- Before the upgrade
  - Users/groups defined with the Expeditor Server User Management console need to be created in the LDAP server
  - Ensure each enrolled device owner exists in the LDAP server
- After the Upgrade
  - User/group data is not migrated from the DB2 local user registry to the LDAP Server

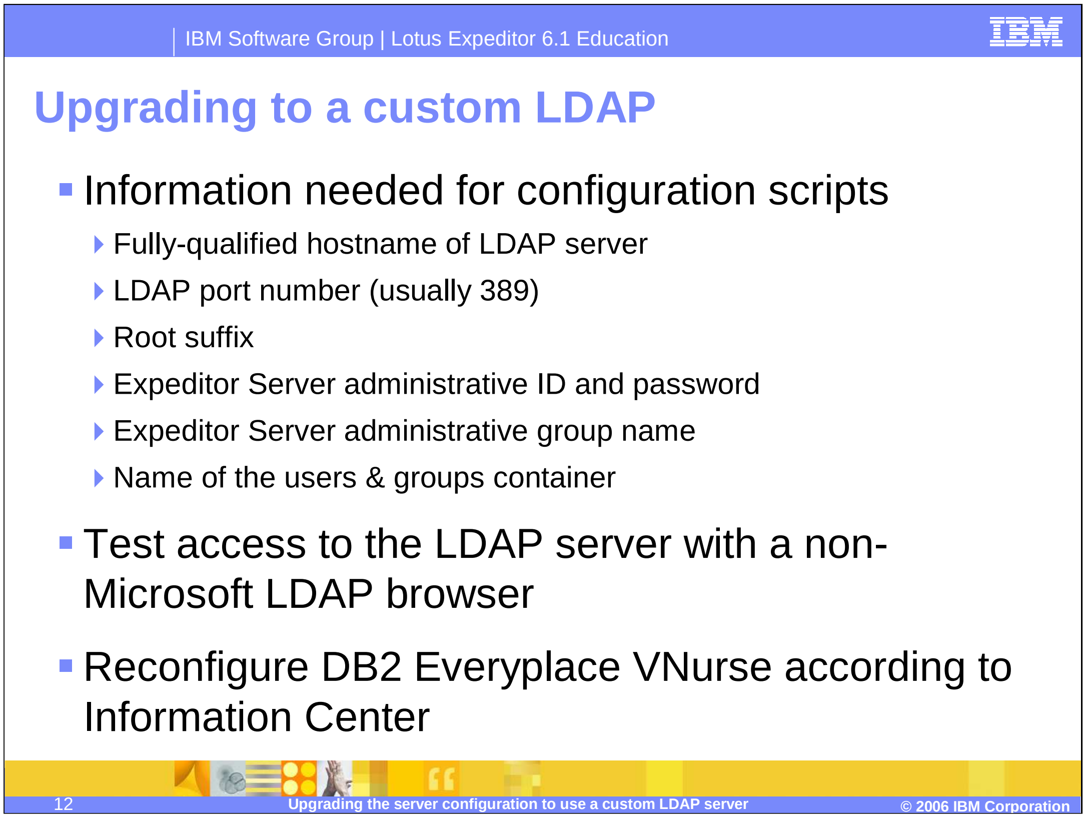
Before you upgrade to LDAP, any users or groups defined with the Expeditor Server User Management console will need to be created in the LDAP server. Device owners for devices enrolled with Device Management will need to be created in the LDAP server. Note that the upgrade process will not migrate any data form the local user registry to the LDAP server because the configuration scripts do not modify the LDAP server.



Existing user data considerations continued

- The DB2 Everyplace® administration console (Mobile Device Administration Console) will
  - Reset sync data based on the new LDAP user registry
  - Prompt to delete old users/groups that existed in the DB2 user registry
  - Existing subscriptions/subscription sets will still exist
  - You must re-associate groups with subscription sets

After the upgrade is complete, DB2 Everyplace data will need to be reset for the users and groups in the LDAP server. When you start the Mobile Device Administration Console after the upgrade, you will be prompted to delete users and groups associated with the DB2 user registry. You can then refresh the user and group data from the LDAP server. Note that subscriptions and subscription sets will still exist. However, the associations between DB2 Everyplace subscriptions and groups will be lost. You will need to edit the DB2 Everyplace subscriptions and re-associate them with the groups.



IBM Software Group | Lotus Expeditor 6.1 Education

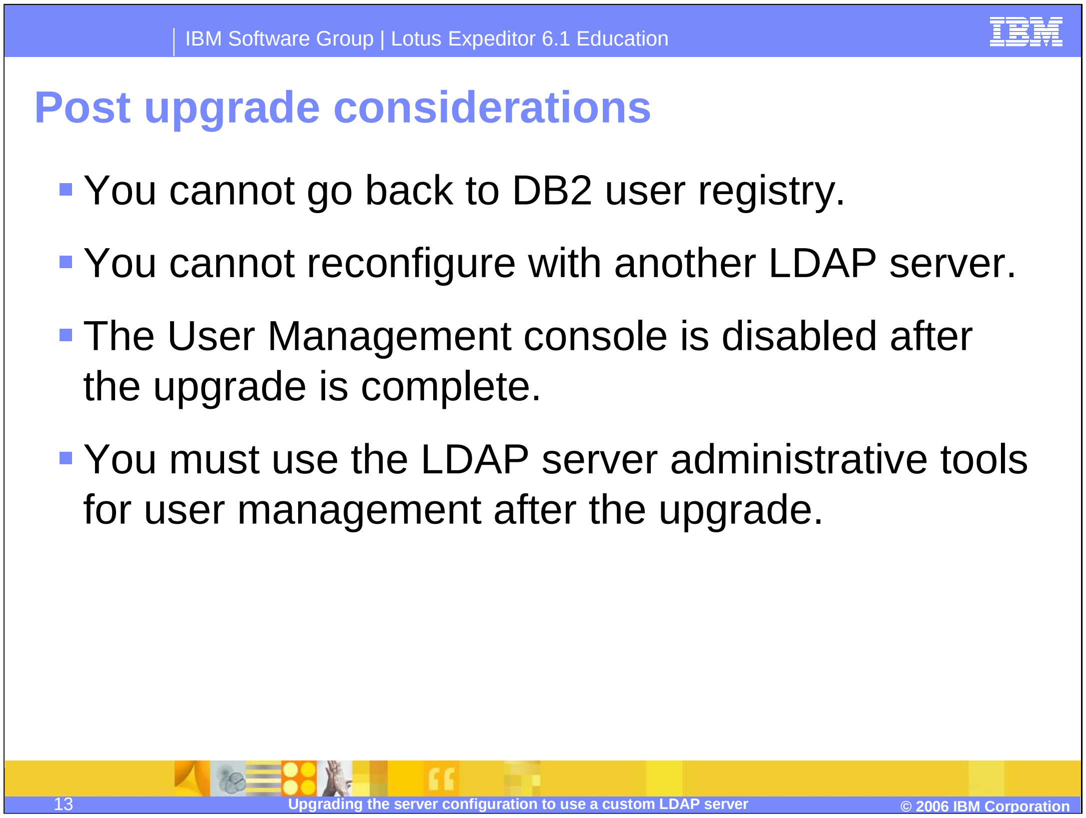
Upgrading to a custom LDAP

- Information needed for configuration scripts
  - Fully-qualified hostname of LDAP server
  - LDAP port number (usually 389)
  - Root suffix
  - Expeditor Server administrative ID and password
  - Expeditor Server administrative group name
  - Name of the users & groups container
- Test access to the LDAP server with a non-Microsoft LDAP browser
- Reconfigure DB2 Everyplace VNurse according to Information Center

12 Upgrading the server configuration to use a custom LDAP server © 2006 IBM Corporation

The following information will be required to complete the configuration to a custom LDAP: fully-qualified hostname for the LDAP server; LDAP port number (usually 389); root suffix; Expeditor Server administrator ID and password defined in the LDAP server; the Expeditor Server administrative group name defined in the LDAP server and name of the users & groups container in the LDAP server. The Expeditor Server Information Center contains a checklist for LDAP configuration.

It is suggested that before you run the configuration scripts that you test access to the LDAP server from the Expeditor Server using a non-Microsoft LDAP browser. There are many freeware LDAP browser available to perform this task.



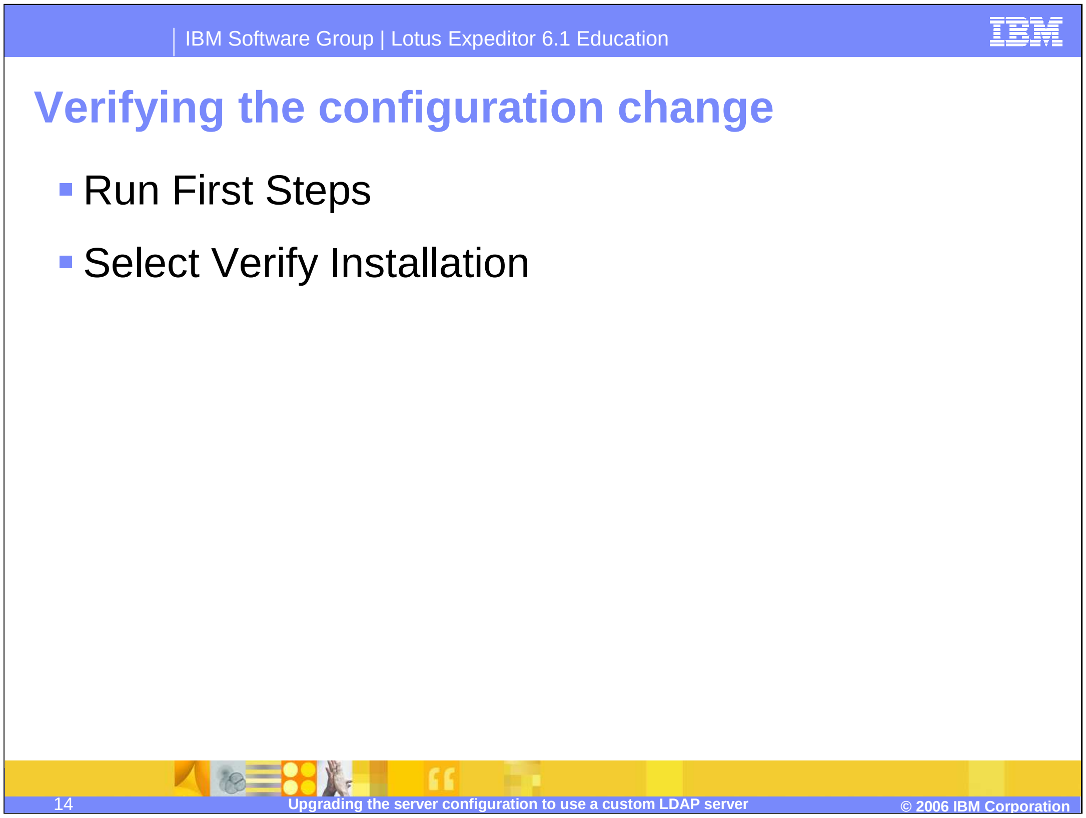
IBM Software Group | Lotus Expeditor 6.1 Education

Post upgrade considerations

- You cannot go back to DB2 user registry.
- You cannot reconfigure with another LDAP server.
- The User Management console is disabled after the upgrade is complete.
- You must use the LDAP server administrative tools for user management after the upgrade.

13 Upgrading the server configuration to use a custom LDAP server © 2006 IBM Corporation

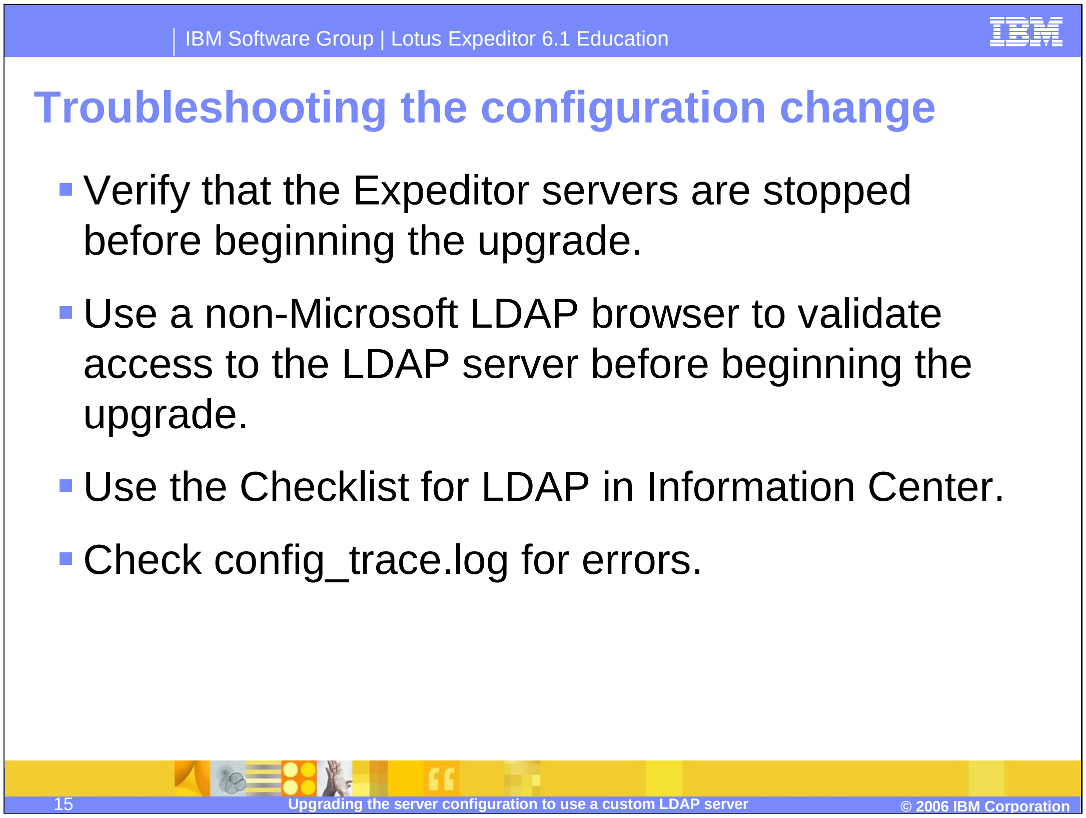
Before you upgrade to LDAP, be aware of the following considerations. Once you upgrade to LDAP you cannot go back to using the DB2 user registry and you cannot reconfigure with another LDAP server. The user management console is disabled since it can only be used with the DB2 user registry. Therefore, you must use the LDAP administrative tools for user management.



Verifying the configuration change

- Run First Steps
- Select Verify Installation

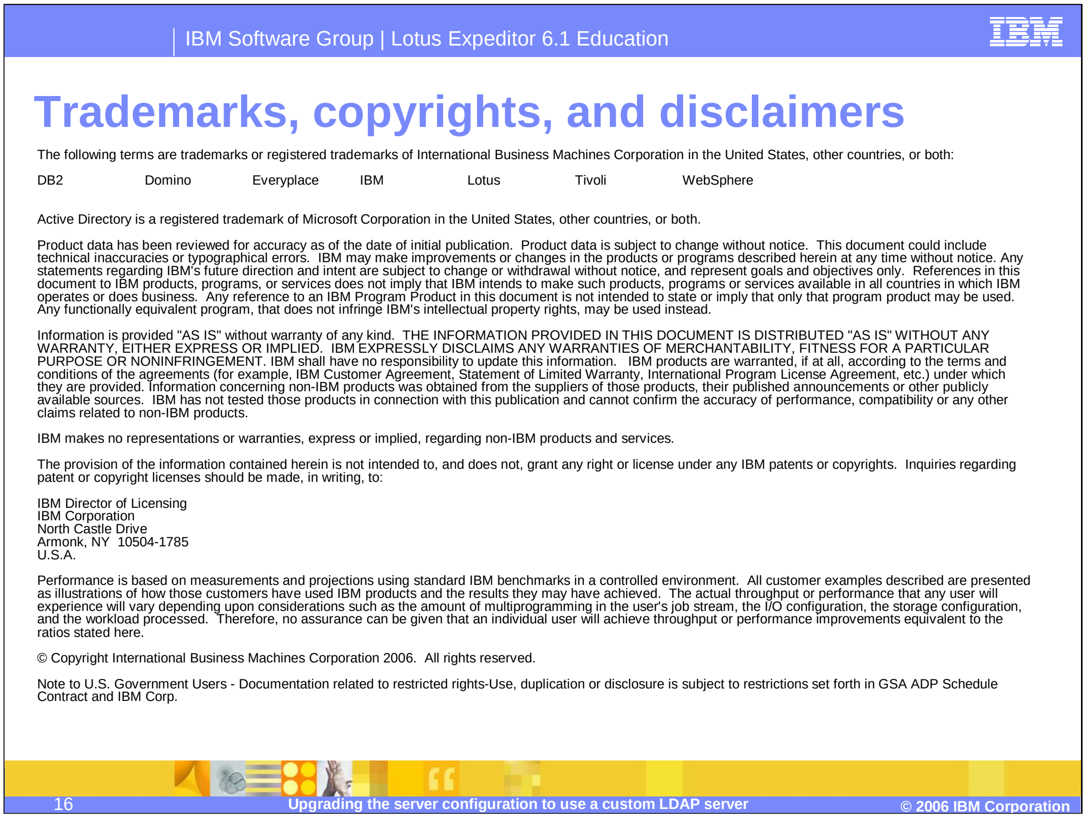
After you run the configuration scripts to upgrade to LDAP, run the verify installation task from the First Steps application to verify that the Expeditor Server is functioning properly.



Troubleshooting the configuration change

- Verify that the Expeditor servers are stopped before beginning the upgrade.
- Use a non-Microsoft LDAP browser to validate access to the LDAP server before beginning the upgrade.
- Use the Checklist for LDAP in Information Center.
- Check config_trace.log for errors.

To avoid problems during the upgrade, verify that all Expeditor Servers are stopped before you begin the upgrade. Verify you can access the LDAP server from the Expeditor Server using a non-Microsoft LDAP browser. Use the checklist for LDAP configuration in the Expeditor Server Information Center to ensure you have performed all the pre-upgrade steps. If you encounter problems during the LDAP upgrade, check the configuration trace log for errors.



Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

DB2 Domino Everyplace IBM Lotus Tivoli WebSphere

Active Directory is a registered trademark of Microsoft Corporation in the United States, other countries, or both.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.