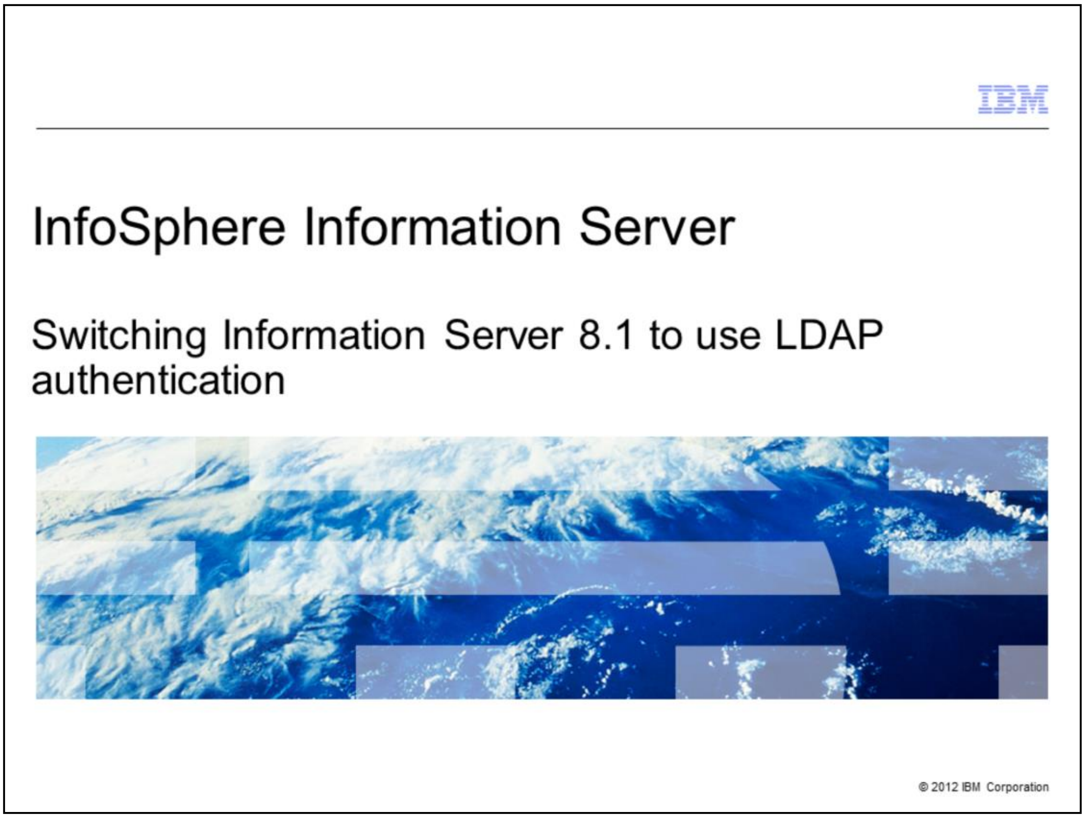
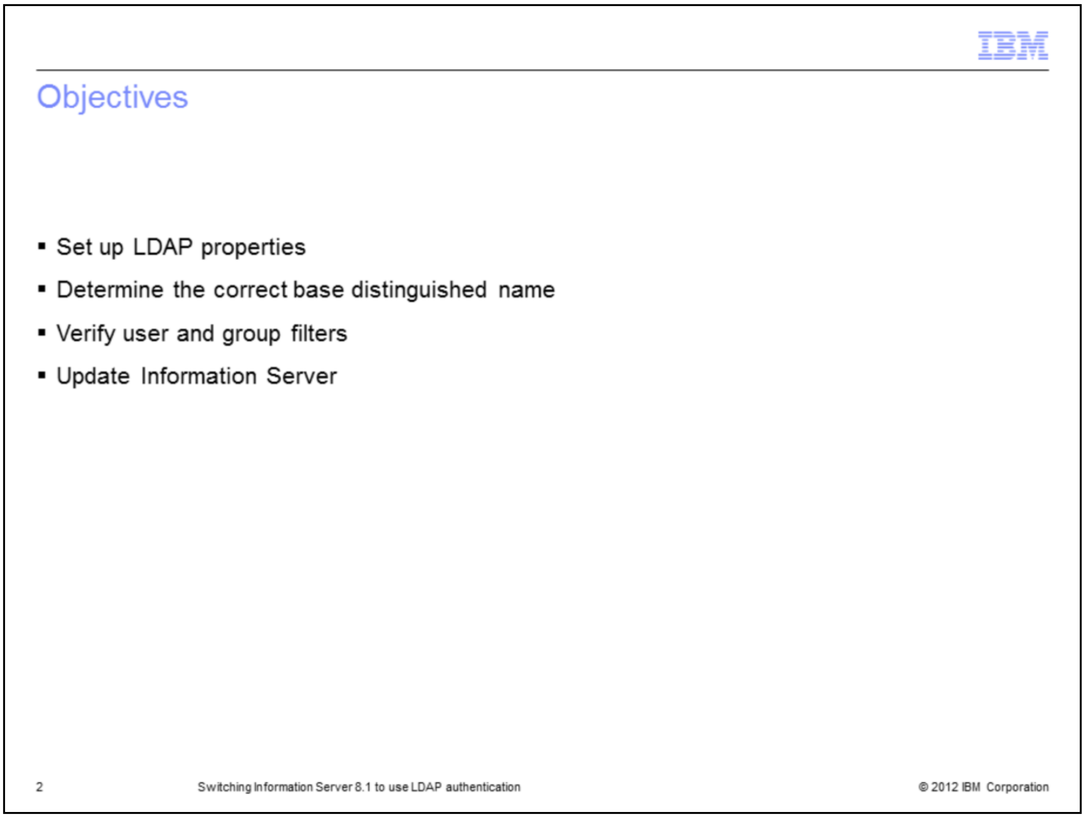


InfoSphere Information Server

Switching Information Server 8.1 to use LDAP authentication

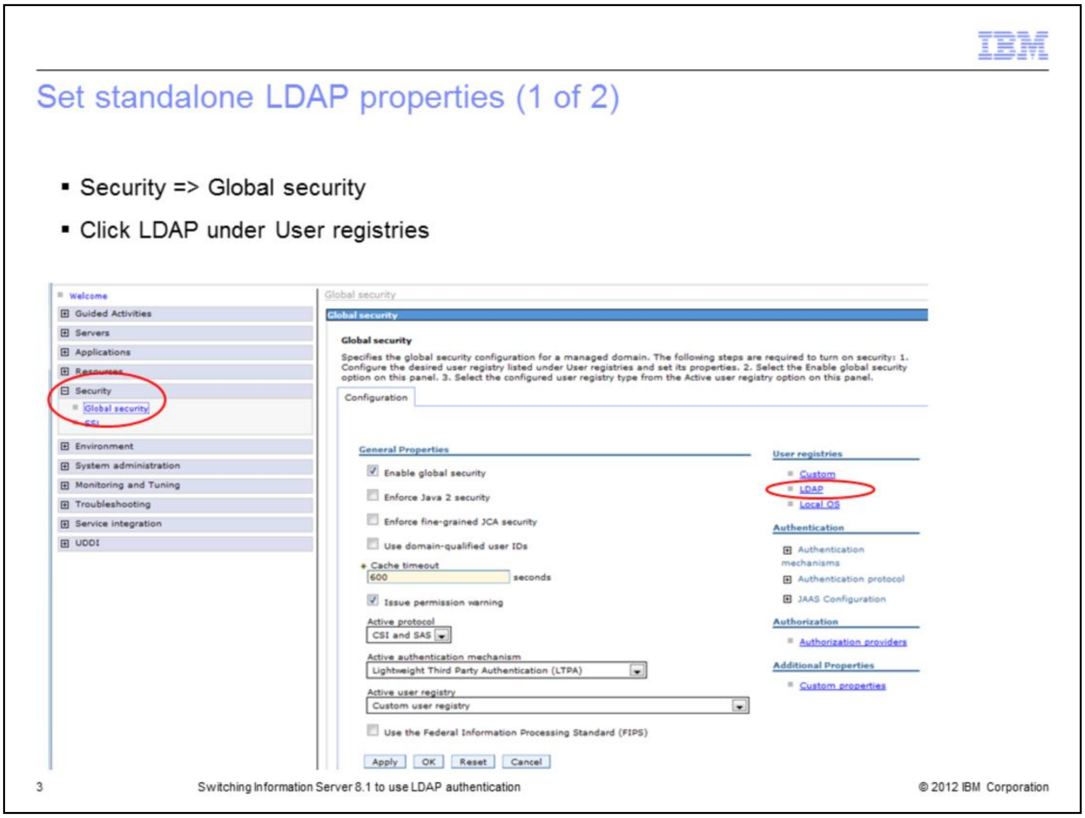
This presentation will discuss how to switch InfoSphere® Information Server 8.1 and WebSphere® 6.0 to use the LDAP repository for authentication.



Objectives

- Set up LDAP properties
- Determine the correct base distinguished name
- Verify user and group filters
- Update Information Server

The objectives of this presentation are to show how to set up the LDAP properties, how to determine the best base distinguished name to use and how to verify the user and group filters. The presentation will also show how to set LDAP as your current active user registry and how to update Information Server with the new WebSphere Administrative ID.



Set standalone LDAP properties (1 of 2)

- Security => Global security
- Click LDAP under User registries

Global security

Specifies the global security configuration for a managed domain. The following steps are required to turn on security: 1. Configure the desired user registry listed under User registries and set its properties. 2. Select the Enable global security option on this panel. 3. Select the configured user registry type from the Active user registry option on this panel.

General Properties

☑ Enable global security

□ Enforce Java 2 security

□ Enforce fine-grained JCA security

□ Use domain-qualified user IDs

* Cache timeout: 600 seconds

☑ Issue permission warning

Active protocol: CSI and SAS

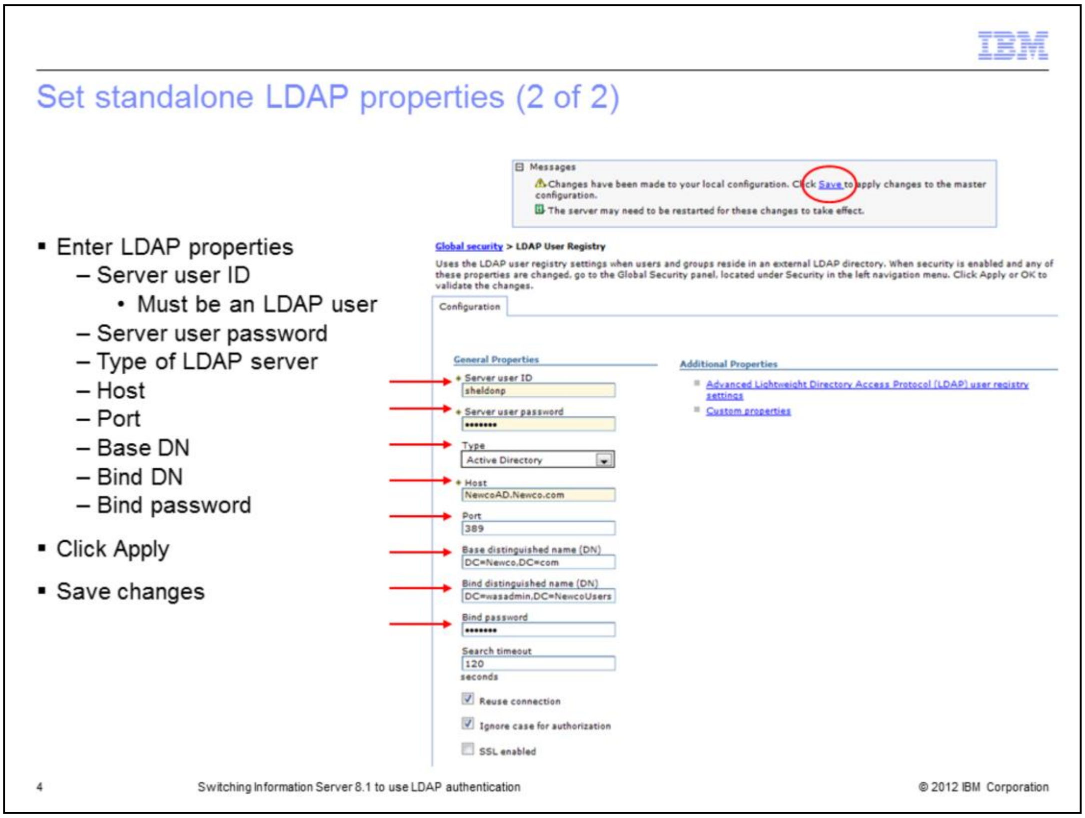
Active authentication mechanism: Lightweight Third Party Authentication (LTPA)

Active user registry: Custom user registry

□ Use the Federal Information Processing Standard (FIPS)

3 Switching Information Server 8.1 to use LDAP authentication © 2012 IBM Corporation

The first step in setting up the LDAP registry is to open the WebSphere Administrative console and on the left side of the screen, click Security and then Global security. Next, click LDAP under User registries.



Set standalone LDAP properties (2 of 2)

- Enter LDAP properties
  - Server user ID
    - Must be an LDAP user
  - Server user password
  - Type of LDAP server
  - Host
  - Port
  - Base DN
  - Bind DN
  - Bind password
- Click Apply
- Save changes

⊟ Messages

⚠ Changes have been made to your local configuration. Click Save to apply changes to the master configuration.

The server may need to be restarted for these changes to take effect.

Global security > LDAP User Registry

Uses the LDAP user registry settings when users and groups reside in an external LDAP directory. When security is enabled and any of these properties are changed, go to the Global Security panel, located under Security in the left navigation menu. Click Apply or OK to validate the changes.

Configuration

General Properties

* Server user ID: sheldonp

* Server user password: •••••••

Type: Active Directory

* Host: NewcoAD.Newco.com

Port: 389

Base distinguished name (DN): DC=Newco,DC=com

Bind distinguished name (DN): DC=wasadmin,DC=NewcoUsers

Bind password: •••••••

Search timeout: 120 seconds

☑ Reuse connection

☑ Ignore case for authorization

☐ SSL enabled

Additional Properties

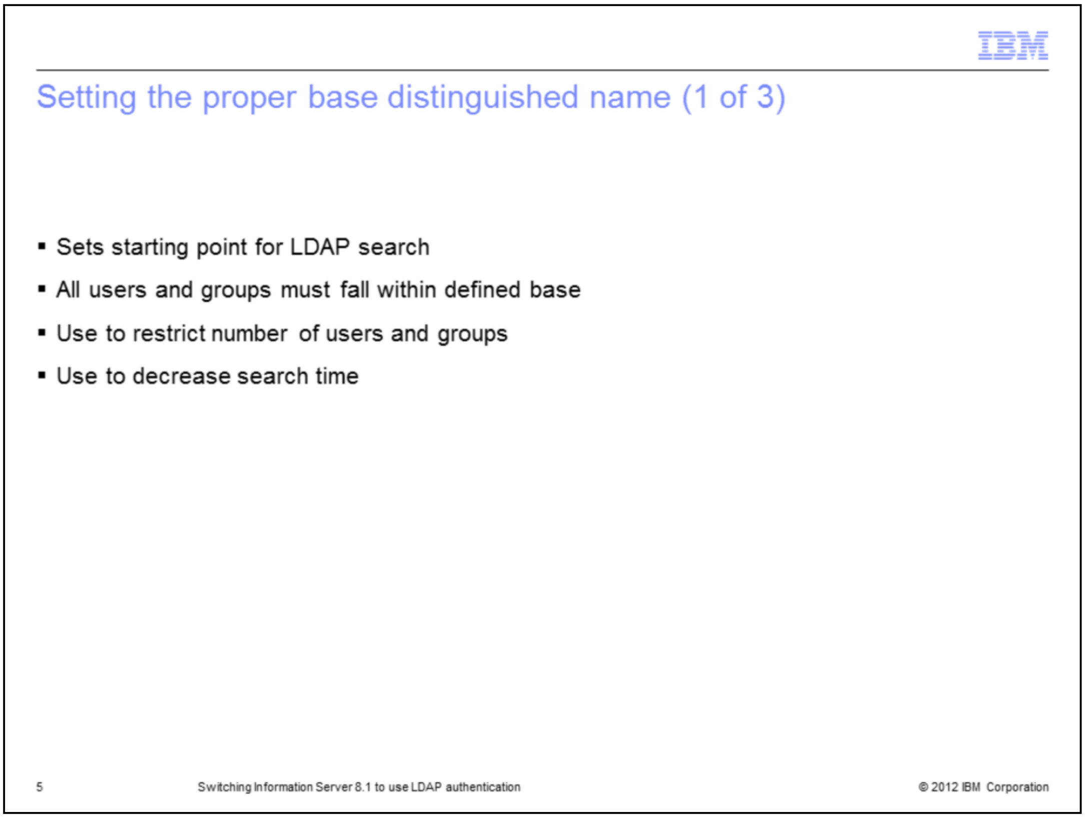
- Advanced Lightweight Directory Access Protocol (LDAP) user registry settings
- Custom properties

4 Switching Information Server 8.1 to use LDAP authentication © 2012 IBM Corporation

Under the General properties page, enter in the name and password of your WebSphere administrative user in the Server user ID field. Choose the type of LDAP server you are authenticating against. Next, enter the LDAP server name, Port, and Base distinguished name. The base distinguished name defines the starting point for LDAP searches. Making this value more restrictive will limit the number of users and groups returned to Information Server. Just be sure that all the users and groups fall within the defined base. The next slide will discuss the base DN in more detail.

Next, enter your bind distinguished name and password. This is the distinguished name of the user that is used to bind to the directory service. It does not have to be the same user as the primary administrative user. If your directory service supports anonymous bind, you can leave these fields blank.

When the information has been entered, click Apply at the bottom of the screen and then click Save in the message box at the top and Save on the next screen to save to the master configuration.



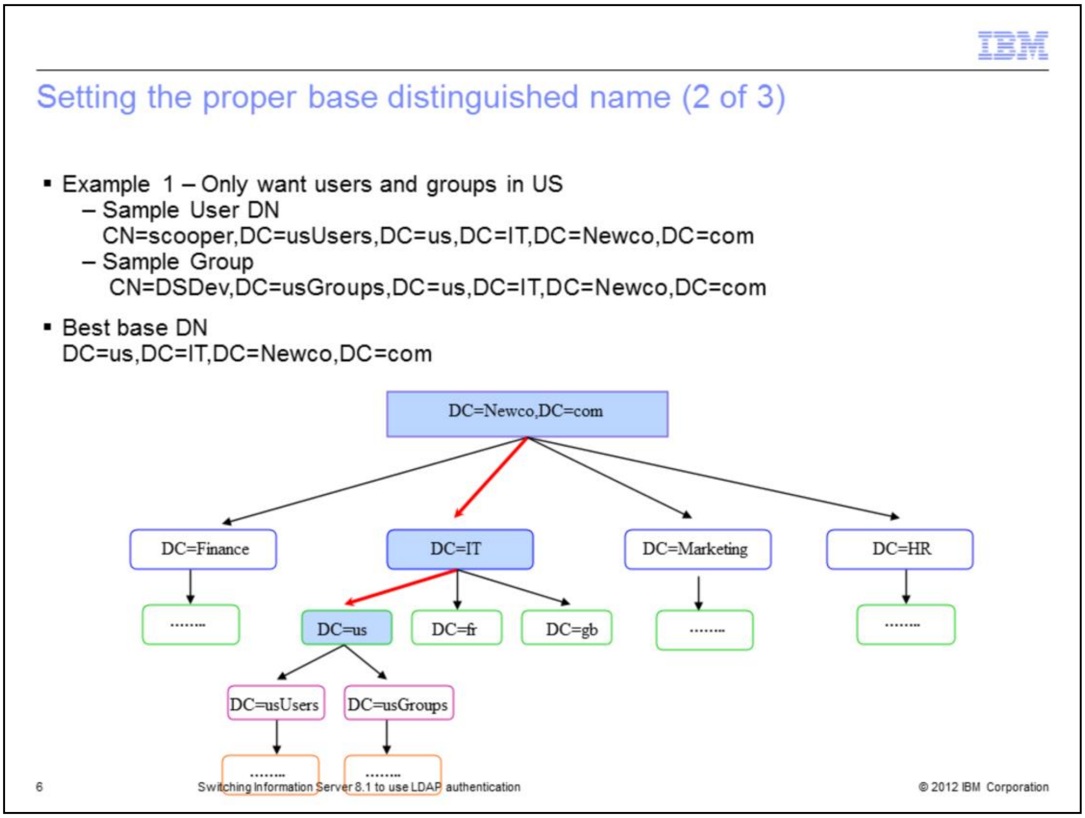
IBM

Setting the proper base distinguished name (1 of 3)

- Sets starting point for LDAP search
- All users and groups must fall within defined base
- Use to restrict number of users and groups
- Use to decrease search time

5 Switching Information Server 8.1 to use LDAP authentication © 2012 IBM Corporation

The base distinguished name sets the starting point for LDAP searches in the directory service. Setting this appropriately for your user and group search can help to limit the number of users and groups returned to Information Server and decrease the search time. The appropriate value for this field depends on the layout of your directory service.



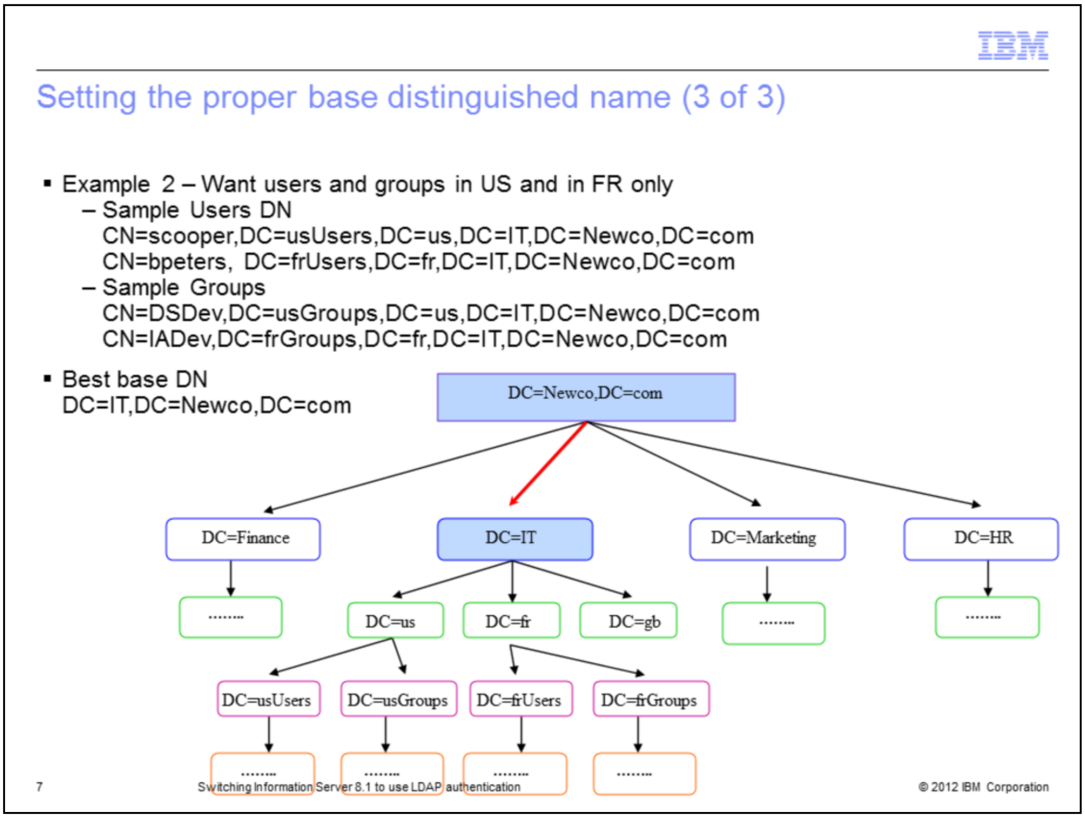
Setting the proper base distinguished name (2 of 3)

- Example 1 – Only want users and groups in US
  - Sample User DN
    CN=scooper,DC=usUsers,DC=us,DC=IT,DC=Newco,DC=com
  - Sample Group
    CN=DSDev,DC=usGroups,DC=us,DC=IT,DC=Newco,DC=com
- Best base DN
  DC=us,DC=IT,DC=Newco,DC=com

DC=Newco,DC=com
DC=Finance
DC=IT
DC=Marketing
DC=HR
……..
DC=us
DC=fr
DC=gb
……..
……..
DC=usUsers
DC=usGroups
……..
……..

6 Switching Information Server 8.1 to use LDAP authentication © 2012 IBM Corporation

In this example, the company Newco only wants their US users and groups to appear in Information Server. This slide displays an example distinguished name for user scooper and group DSDev. If Newco uses DC=Newco,DC=com for their base DN, whenever they do an LDAP lookup or attempt to get a list of users and groups, LDAP will have to search all four branches. Searching all four branches, Finance, IT, Marketing, and HR, can be time consuming in a large directory service and will return thousands of unwanted users and groups. Since all of the users and groups are under the DC=us branch, it is much more efficient to make the base DN DC=us,DC=IT,DC=Newco,DC=com. In this case, if an LDAP search, user list, or group list is requested, the search will begin at the DC=us branch making the search much more efficient.

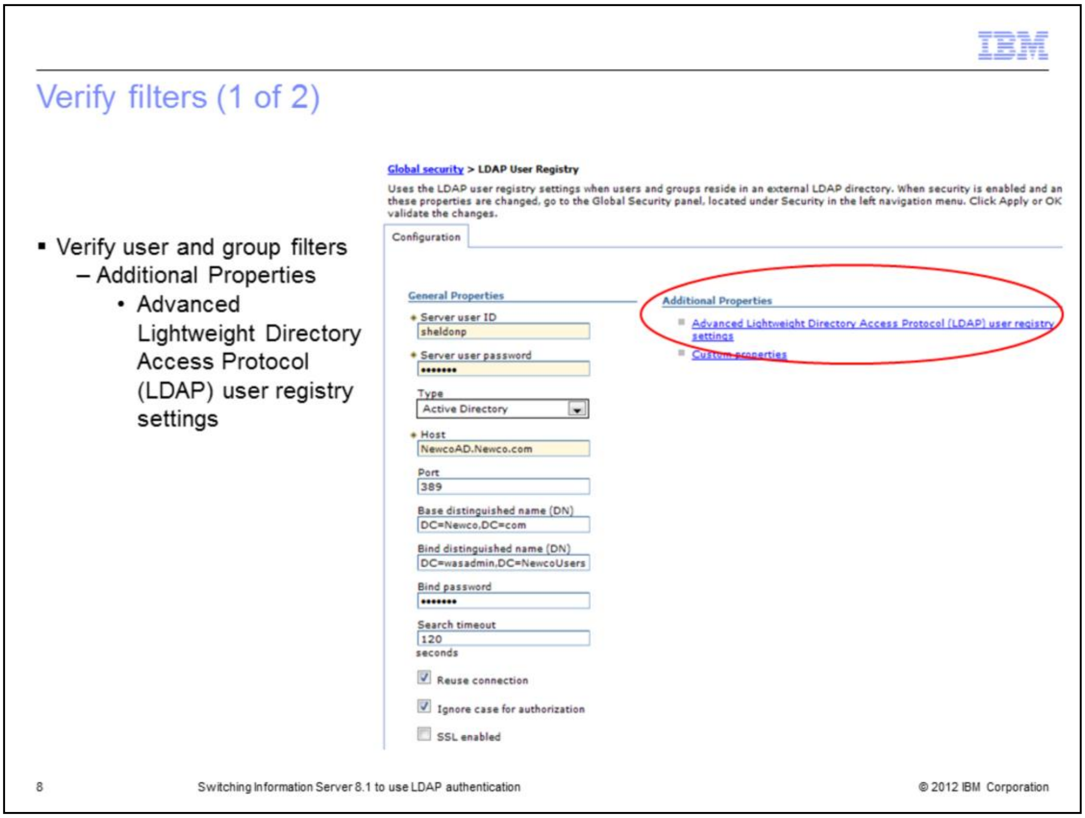


Setting the proper base distinguished name (3 of 3)

- Example 2 – Want users and groups in US and in FR only
  - Sample Users DN
    CN=scooper,DC=usUsers,DC=us,DC=IT,DC=Newco,DC=com
    CN=bpeters, DC=frUsers,DC=fr,DC=IT,DC=Newco,DC=com
  - Sample Groups
    CN=DSDev,DC=usGroups,DC=us,DC=IT,DC=Newco,DC=com
    CN=IADev,DC=frGroups,DC=fr,DC=IT,DC=Newco,DC=com
- Best base DN
  DC=IT,DC=Newco,DC=com

DC=Newco,DC=com
DC=Finance
DC=IT
DC=Marketing
DC=HR
....
DC=us
DC=fr
DC=gb
....
....
DC=usUsers
DC=usGroups
DC=frUsers
DC=frGroups
....
....
....
....

In this example, Newco wants both their US and France users. The base DN will have to be less restrictive and use DC=IT,DC=Newco,DC=com so that it will include both the users and groups from the US and France. Since the Great Britain users are also under the IT branch, DC=gb will always be searched as well. Even with this being the case, the search is more efficient than searching the entire Newco domain.



Verify filters (1 of 2)

- Verify user and group filters
  - Additional Properties
    - Advanced Lightweight Directory Access Protocol (LDAP) user registry settings

Global security > LDAP User Registry

Uses the LDAP user registry settings when users and groups reside in an external LDAP directory. When security is enabled and an these properties are changed, go to the Global Security panel, located under Security in the left navigation menu. Click Apply or OK validate the changes.

Configuration

General Properties

* Server user ID: sheldonp
* Server user password: •••••••
* Type: Active Directory
* Host: NewcoAD.Newco.com
* Port: 389
* Base distinguished name (DN): DC=Newco,DC=com
* Bind distinguished name (DN): DC=wasadmin,DC=NewcoUsers
* Bind password: •••••••
* Search timeout: 120 seconds

☑ Reuse connection

☑ Ignore case for authorization

□ SSL enabled

Additional Properties

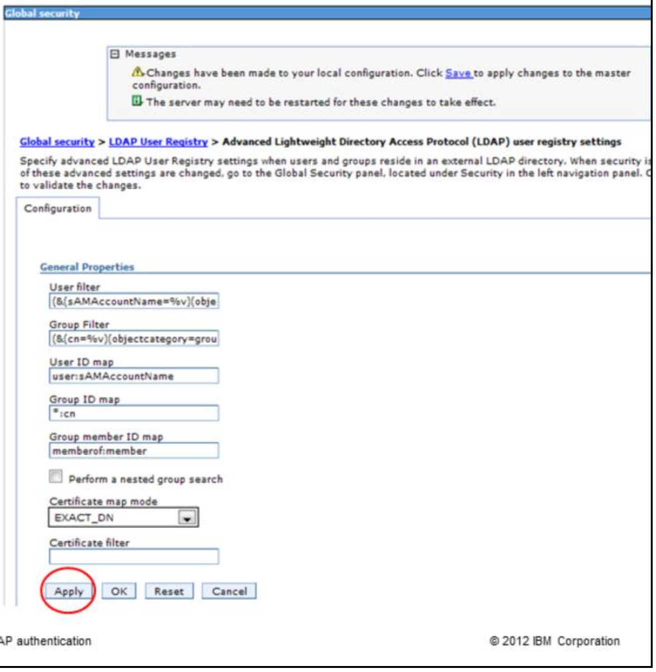
- Advanced Lightweight Directory Access Protocol (LDAP) user registry settings
- Custom properties

8 Switching Information Server 8.1 to use LDAP authentication

The next step in setting up the LDAP repository is to verify that the default user and group filters are correct. While in the General Properties screen for the LDAP repository, click Advanced Lightweight Directory Access Protocol user registry settings under Additional Properties.

Verify filters (1 of 2)

- Verify/update user and group filters
- Click Apply and Save changes


Global security

⊟ Messages

⚠ Changes have been made to your local configuration. Click Save to apply changes to the master configuration.

The server may need to be restarted for these changes to take effect.

Global security > LDAP User Registry > Advanced Lightweight Directory Access Protocol (LDAP) user registry settings

Specify advanced LDAP User Registry settings when users and groups reside in an external LDAP directory. When security is
of these advanced settings are changed, go to the Global Security panel, located under Security in the left navigation panel. C
to validate the changes.

Configuration

General Properties

User filter
(&(sAMAccountName=%v)(obje

Group Filter
(&(cn=%v)(objectcategory=grou

User ID map
user:sAMAccountName

Group ID map
*:cn

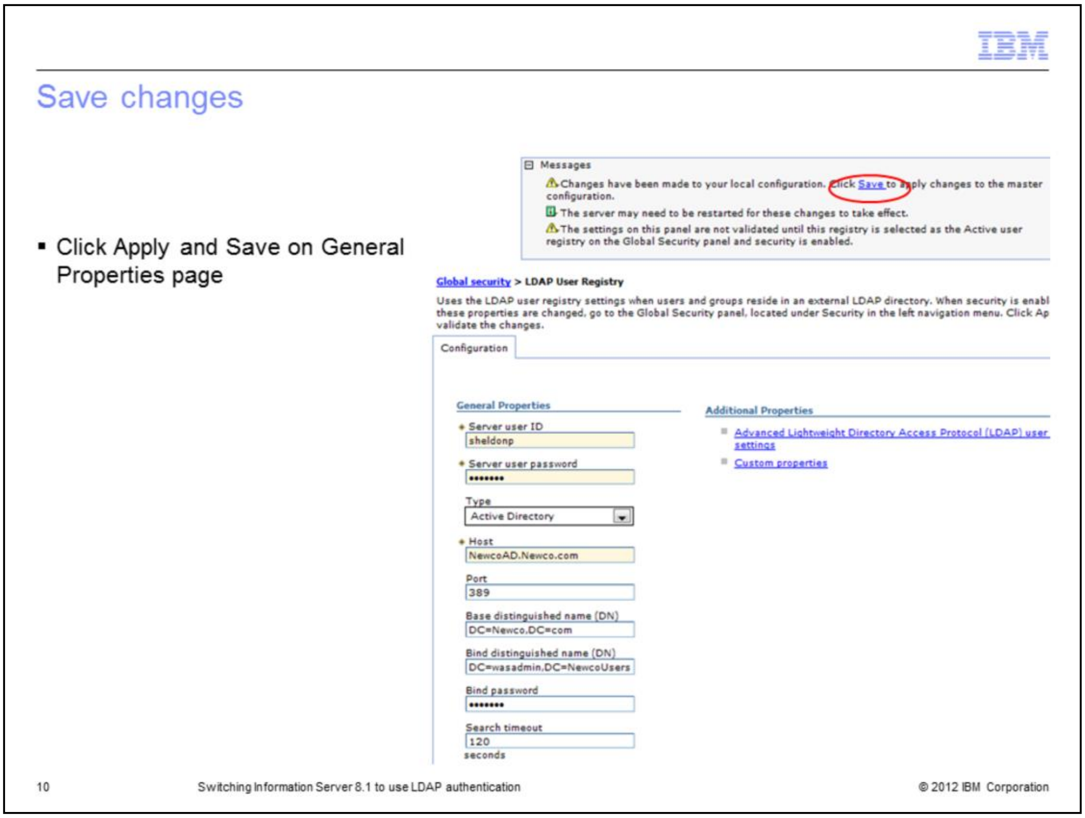
Group member ID map
memberof:member

□ Perform a nested group search

Certificate map mode
EXACT_DN

Certificate filter

Verify that the filters match what was supplied to you by your LDAP administrator. If the values do not match, make the appropriate changes and click Apply at the bottom of the screen. Then click Save in the message box at the top and Save on the next screen to save to the master configuration.



Save changes

- Click Apply and Save on General Properties page

⊟ Messages

⚠ Changes have been made to your local configuration. Click Save to apply changes to the master configuration.

The server may need to be restarted for these changes to take effect.

⚠ The settings on this panel are not validated until this registry is selected as the Active user registry on the Global Security panel and security is enabled.

Global security > LDAP User Registry

Uses the LDAP user registry settings when users and groups reside in an external LDAP directory. When security is enabl these properties are changed, go to the Global Security panel, located under Security in the left navigation menu. Click Ap validate the changes.

General Properties

* Server user ID: sheldonp
* Server user password: ••••••••
Type: Active Directory
* Host: NewcoAD.Newco.com
Port: 389
Base distinguished name (DN): DC=Newco,DC=com
Bind distinguished name (DN): DC=wasadmin,DC=NewcoUsers
Bind password: ••••••••
Search timeout: 120 seconds

Additional Properties

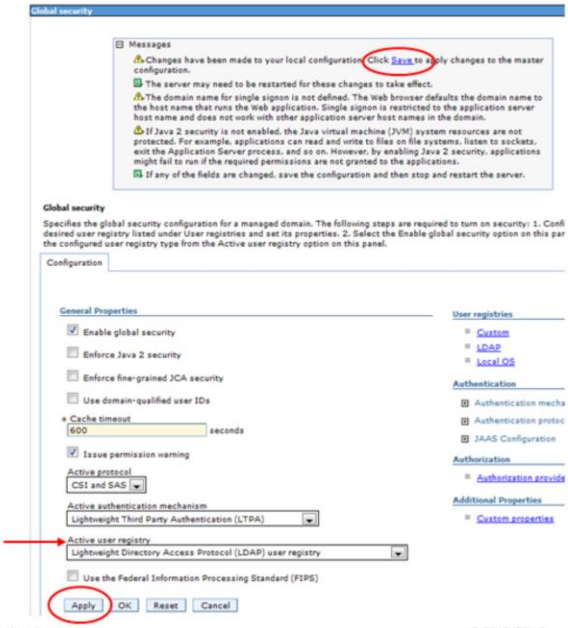
- Advanced Lightweight Directory Access Protocol (LDAP) user settings
- Custom properties

10 Switching Information Server 8.1 to use LDAP authentication © 2012 IBM Corporation

Click Apply and Save on the General Properties page.

Change Active user registry

- Global Security Page
  - Select Lightweight Directory Access Protocol (LDAP) user registry
  - Click Apply
    - WebSphere will attempt to authenticate
    - Messages box will show authentication errors
  - Save changes
- Restart WebSphere



Global security

⊟ Messages

⚠ Changes have been made to your local configuration. Click Save to apply changes to the master configuration.

The server may need to be restarted for these changes to take effect.

⚠ The domain name for single signon is not defined. The Web browser defaults the domain name to the host name that runs the Web application. Single signon is restricted to the application server host name and does not work with other application server host names in the domain.

⚠ If Java 2 security is not enabled, the Java virtual machine (JVM) system resources are not protected. For example, applications can read and write to files on file systems, listen to sockets, exit the Application Server process, and so on. However, by enabling Java 2 security, applications might fail to run if the required permissions are not granted to the applications.

If any of the fields are changed, save the configuration and then stop and restart the server.

Global security

Specifies the global security configuration for a managed domain. The following steps are required to turn on security: 1. Confi desired user registry listed under User registries and set its properties. 2. Select the Enable global security option on this par the configured user registry type from the Active user registry option on this panel.

Configuration

General Properties

☑ Enable global security

□ Enforce Java 2 security

□ Enforce fine-grained JCA security

□ Use domain-qualified user IDs

* Cache timeout: 600 seconds

☑ Issue permission warning

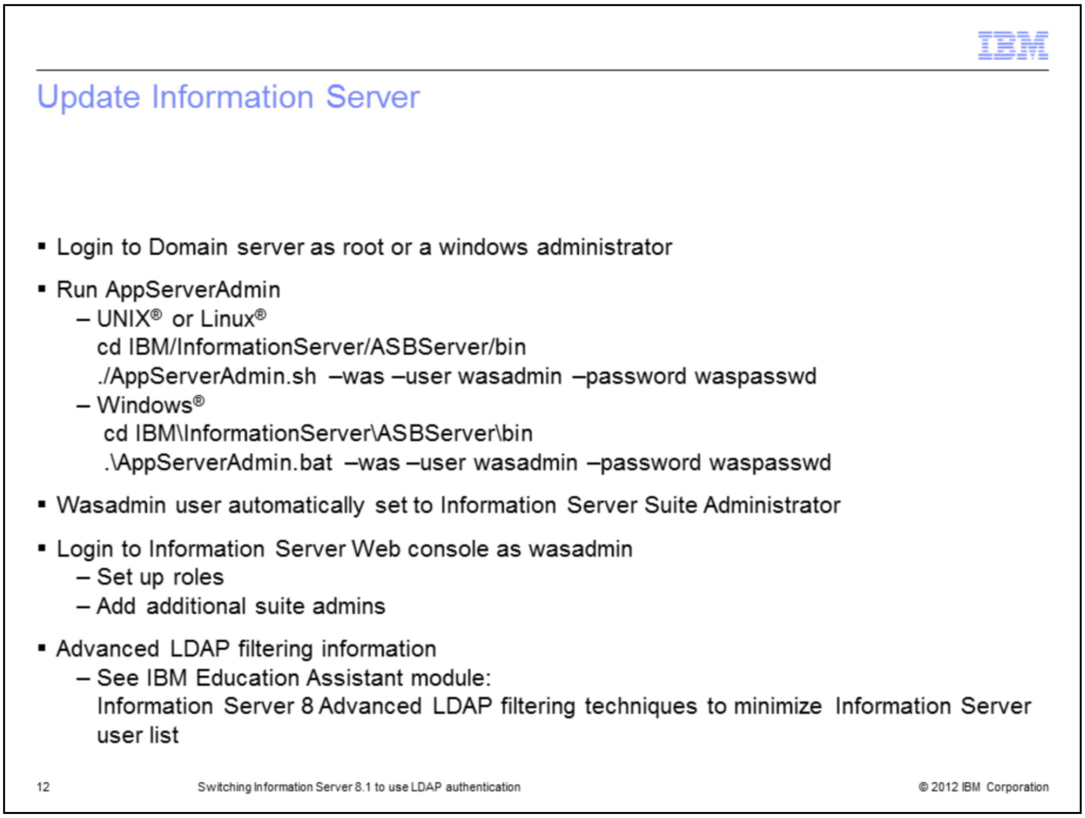
Active protocol: CSI and SAS

Active authentication mechanism: Lightweight Third Party Authentication (LTPA)

Active user registry: Lightweight Directory Access Protocol (LDAP) user registry

□ Use the Federal Information Processing Standard (FIPS)

On the Global security page, click the drop down for Active user registry and select Lightweight Directory Access Protocol (LDAP) user registry. Click Apply. At this point, WebSphere will try to authenticate the WebSphere administrative user against the LDAP directory service. If the authentication fails due to a configuration error, an error will appear in the message box at the top and the changes are not saved. If this is the case, go back and verify your LDAP properties and filters. If no errors appear in the message box, click Save. WebSphere must be restarted for these changes to take effect.



Update Information Server

- Login to Domain server as root or a windows administrator
- Run AppServerAdmin
  - UNIX® or Linux®

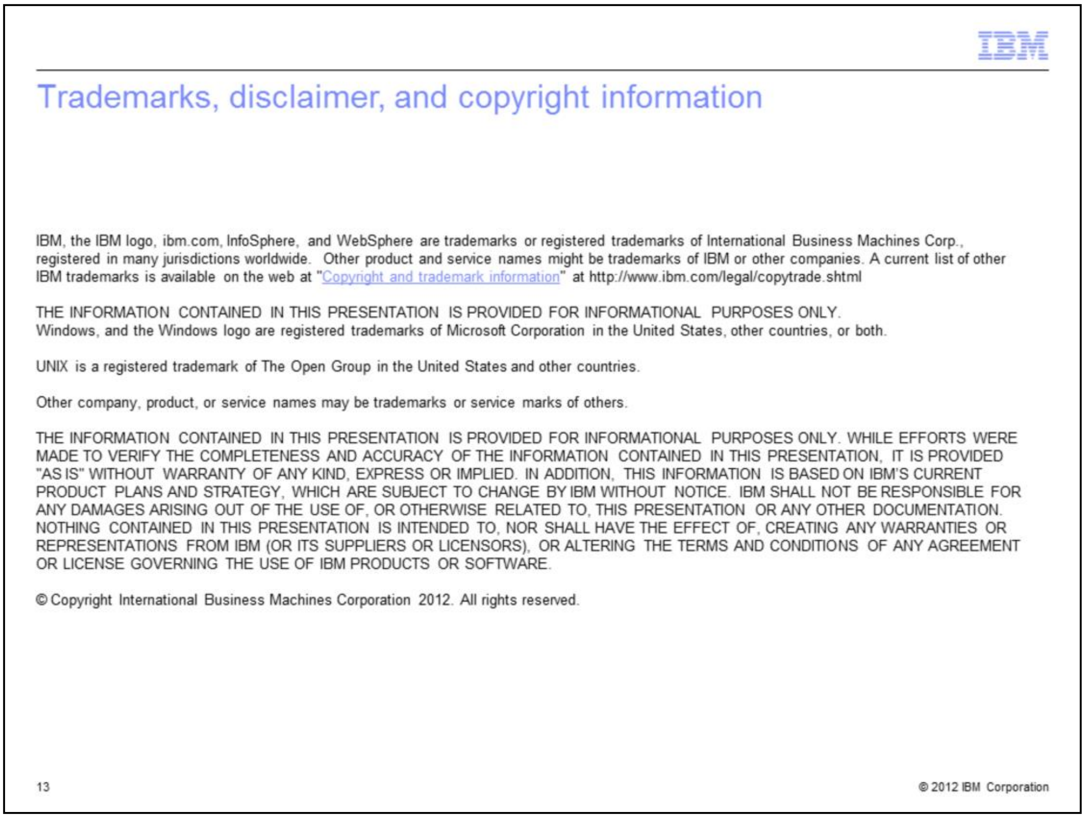
    ```
    cd IBM/InformationServer/ASBServer/bin
    ./AppServerAdmin.sh  –was –user wasadmin –password waspasswd
    ```
  - Windows®

    ```
    cd IBM\InformationServer\ASBServer\bin
    .\AppServerAdmin.bat  –was –user wasadmin –password waspasswd
    ```
- Wasadmin user automatically set to Information Server Suite Administrator
- Login to Information Server Web console as wasadmin
  - Set up roles
  - Add additional suite admins
- Advanced LDAP filtering information
  - See IBM Education Assistant module: Information Server 8 Advanced LDAP filtering techniques to minimize Information Server user list

On the Information Server side, you will need to run the AppServerAdmin command line utility as root or a Windows administrator to update Information Server with your new wasadmin user and password. cd into the InformationServer/ASBServer/bin directory and run the AppServerAdmin command as displayed on this slide.

Once that has completed successfully, you are now ready to go into the Information Server Web console. The first time you login to the Information Server Web console, you will need to use the primary administrative user you specified on slide four. This user will automatically be an Information Server suite administrator. Once you open the Information Server Web console, you can then go in and set the user roles and add any additional users as suite admins.

For information on more advanced LDAP filtering techniques, see the IBM Education Assistant module “Information Server 8 Advanced LDAP filtering techniques to minimize Information Server user list”.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, InfoSphere, 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.
Windows, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

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.