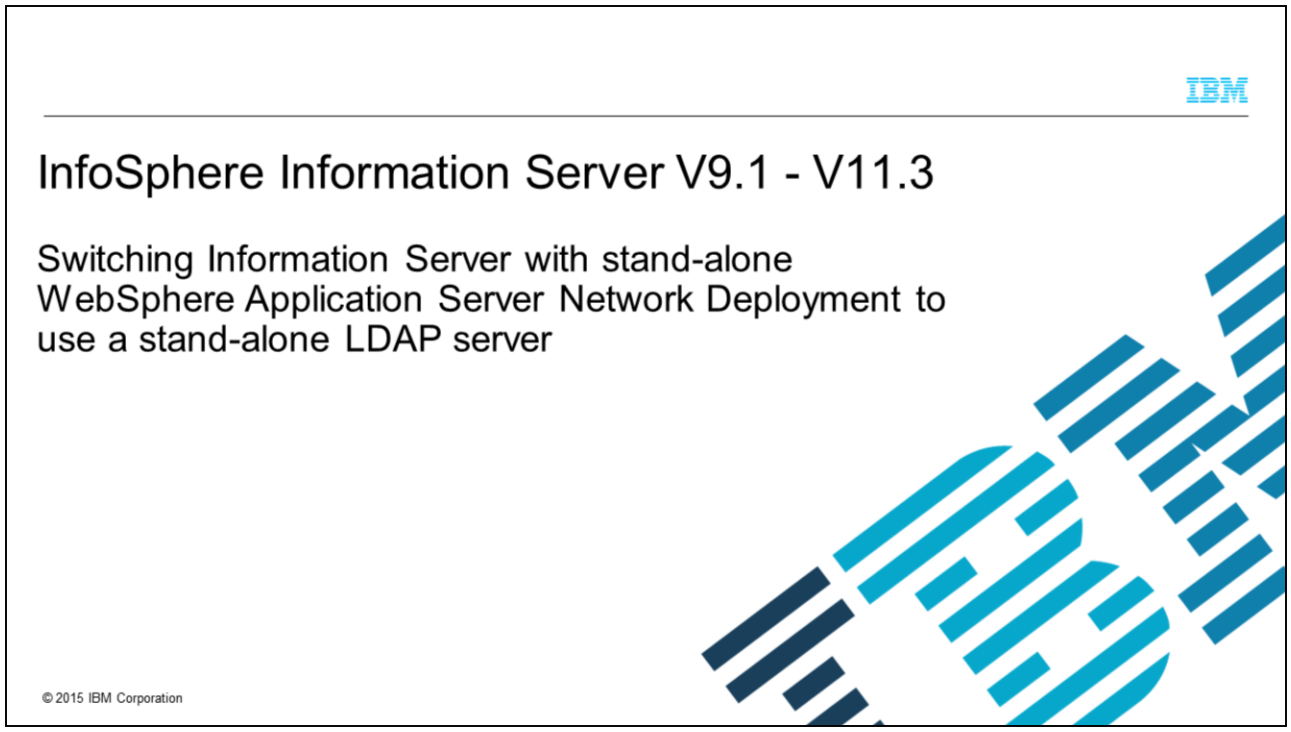


This presentation discusses how to switch InfoSphere® Information Server 9.1 and 11.3 to use the stand-alone Lightweight Directory Access Protocol, or LDAP, repository for authentication. This presentation is only applicable for installations using WebSphere® Application Server Network Deployment. If you installed version 11.3 with WebSphere Liberty, see the IBM Education Assistant module on Configuring LDAP with Information Server 11.3 with WebSphere Liberty. This presentation is not valid for InfoSphere Information Server 11.3 with clustered WebSphere Application Server Network Deployment.

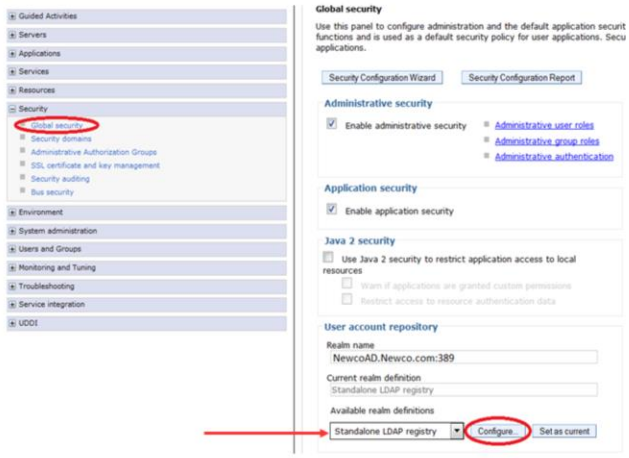
Objectives

- Set up stand-alone LDAP properties
- Verify user and group filters
- Setting proper base distinguished name
- Set stand-alone LDAP as current realm definition
- Update Information Server

The objectives of this presentation are to show how to set up the LDAP properties for stand-alone LDAP, how to verify the user and group filters and how to determine the best base distinguished name. This presentation also shows how to set stand-alone LDAP as your current realm definition and how to update Information Server with the new WebSphere Administrative ID.

Set stand-alone LDAP properties (1 of 2)

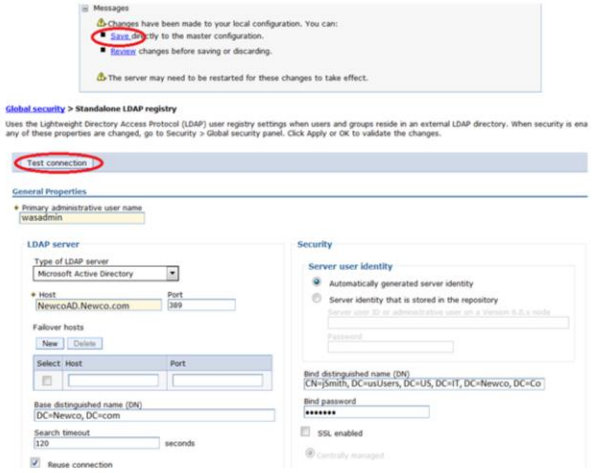
- Security => Global security
- Available realm definitions
  - Standalone LDAP
- Click Configure



The first step in setting up the stand-alone LDAP registry is to open the WebSphere administrative console. On the left side of the screen, click Security and then Global security. Next, click the drop-down for the Available realm definitions and choose Standalone LDAP registry. Click Configure.

Set stand-alone LDAP properties (2 of 2)

- Enter LDAP properties
  - Primary administrative user
    - Must be LDAP user
  - Server user identity
    - Automatically generated server identity
  - Type of LDAP server
  - Host
  - Port
  - Base DN
  - Bind DN
  - Bind password
- Click Apply
- Click Save



Under the General properties page, enter the name of your primary administrative user. This user must be a valid LDAP user. Next, ensure that the Server user identity is set to Automatically generated server identity. 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, limits the number of users and groups that are returned to Information Server. Be sure that all the users and groups fall within the defined base. The next slide discusses the base distinguished name 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 support is an 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. Click Test Connection to ensure that your connection to your LDAP server is working properly.

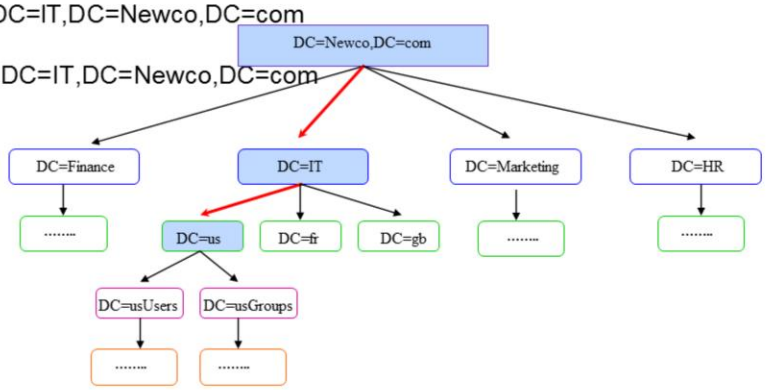
Setting proper base distinguished name (1 of 3)

- 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

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 limit the number of users and groups that are returned to Information Server and decrease the search time. The appropriate value for this field depends on the layout of your directory service.

Setting proper base distinguished name (2 of 3)

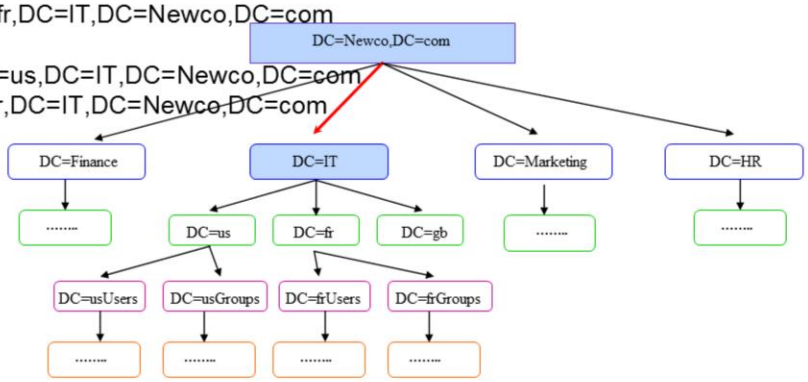
- Example 1 – Only want users and groups in US
  - Sample User DN
    CN=scooper,DC=usUsers,DC=us,DC=IT,DC=Newco,DC=com
  - Sample Group
    CN=DSDev,DC=usGroups,DC=us,DC=IT,DC=Newco,DC=com
- Best base DN
  DC=us,DC=IT,DC=Newco,DC=com



In the example that is displayed on this slide, 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 distinguished name, whenever they do an LDAP lookup or attempt to get a list of users and groups, LDAP has to search all four branches. Searching the four branches, Finance, IT, Marketing, and HR, can be time consuming in a large directory service and returns 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 distinguished name DC=us,DC=IT,DC=Newco,DC=com. In this case, if an LDAP search, user list, or group list is requested, the search begins at the DC=us branch making the search much more efficient.

Setting proper base distinguished name (3 of 3)

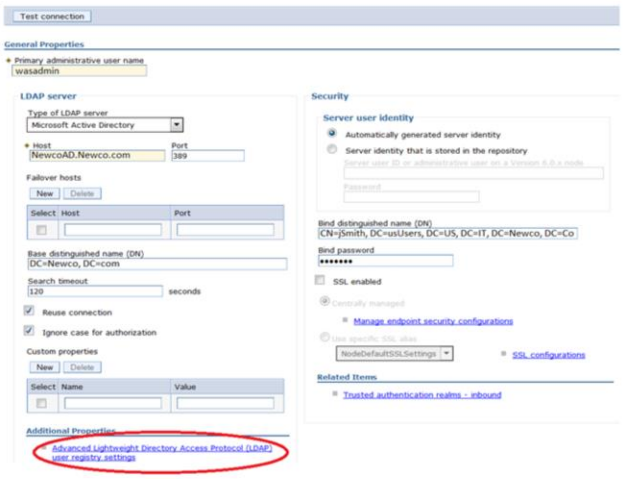
- Example 2 – Want users and groups in US and in FR only
  - Sample Users DN
    CN=scooper,DC=usUsers,DC=us,DC=IT,DC=Newco,DC=com
    CN=bpeters, DC=frUsers,DC=fr,DC=IT,DC=Newco,DC=com
  - Sample Groups
    CN=DSDev,DC=usGroups,DC=us,DC=IT,DC=Newco,DC=com
    CN=IADev,DC=frGroups,DC=fr,DC=IT,DC=Newco,DC=com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



In the example that is displayed on this slide, the company Newco, only wants both their US and France users. The base distinguished name has to be less restrictive and use DC=IT,DC=Newco,DC=com, so that it includes both the user 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 still more efficient than searching the entire Newco domain. If you want to use multiple base distinguished names for searching, set WebSphere up to use federated repositories.

Verify filters (1 of 2)

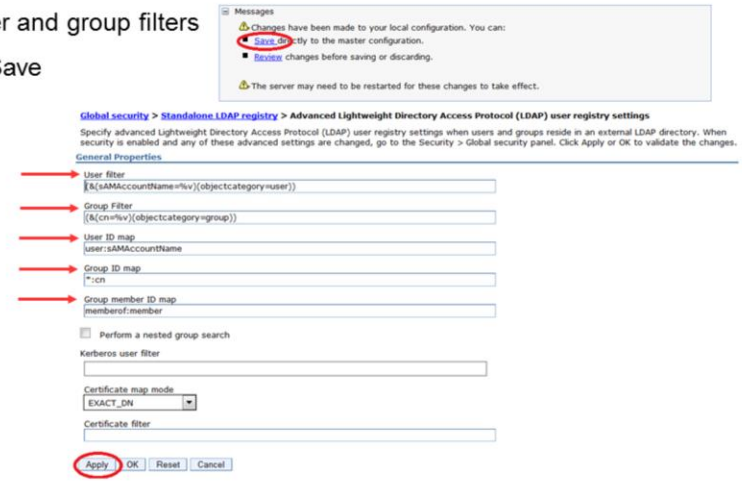
- Verify user and group filters
  - Additional Properties
    - Advanced Lightweight Directory Access Protocol (LDAP) user registry settings



The next step in setting up the standalone 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 (2 of 2)

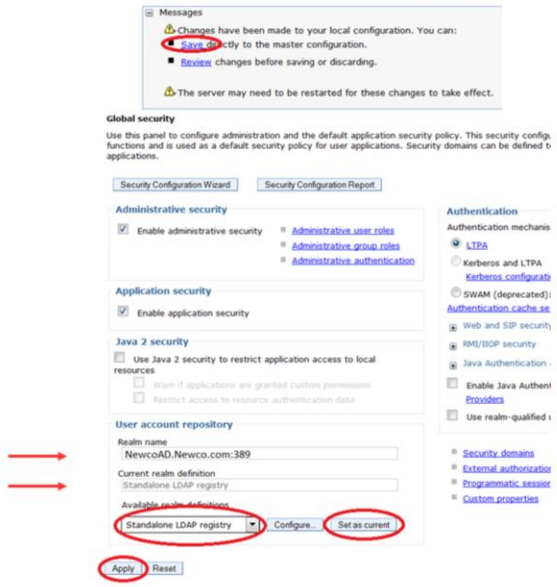
- Verify/update user and group filters
- Click Apply and Save



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 and Save.

Set current realm definition

- Set Available realm definitions
  - Standalone LDAP registry
- Click Set as current
- Click Apply
- Click Save
- Restart WebSphere



The last step in WebSphere is to set the standalone LDAP repository as the current realm definition. Be sure that Standalone LDAP registry is selected under Available realm definitions and click Set as current. The current realm definition should change to Standalone LDAP registry and the realm name should display your LDAP server name and port number. Next, click Apply. If no error appears in the message box at the top, click Save. If a message appears, you need to review your LDAP properties and filters. You also need to restart WebSphere for the changes to take effect.

Update Information Server

- Login to Domain server
- 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 IS Web Console as wasadmin
  - Set up roles
  - Add more suite administrators

On the Information Server side, you need to run the AppServerAdmin command-line utility 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 ready to go into the Information Server Web Console. The first time you login to the Information Server Web Console, you 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 administrators.

Additional information

- Advanced LDAP filtering information
  - Refer to IBM Education Assistant module
    - Information Server 8 Advanced LDAP filtering techniques to minimize Information Server user list
- Configuring Federated Repositories for LDAP authentication
  - Refer to IBM Education Assistant module
    - Switching Information Server 8.5 and 8.7 to use federated repositories for LDAP authentication

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”.

For more information on how to configure Information Server and WebSphere to use federated repositories, see the IBM Education Assistant module “Switching Information Server 8.5 and 8.7 to use federated repositories for LDAP authentication”.

Trademarks, disclaimer, and copyright information