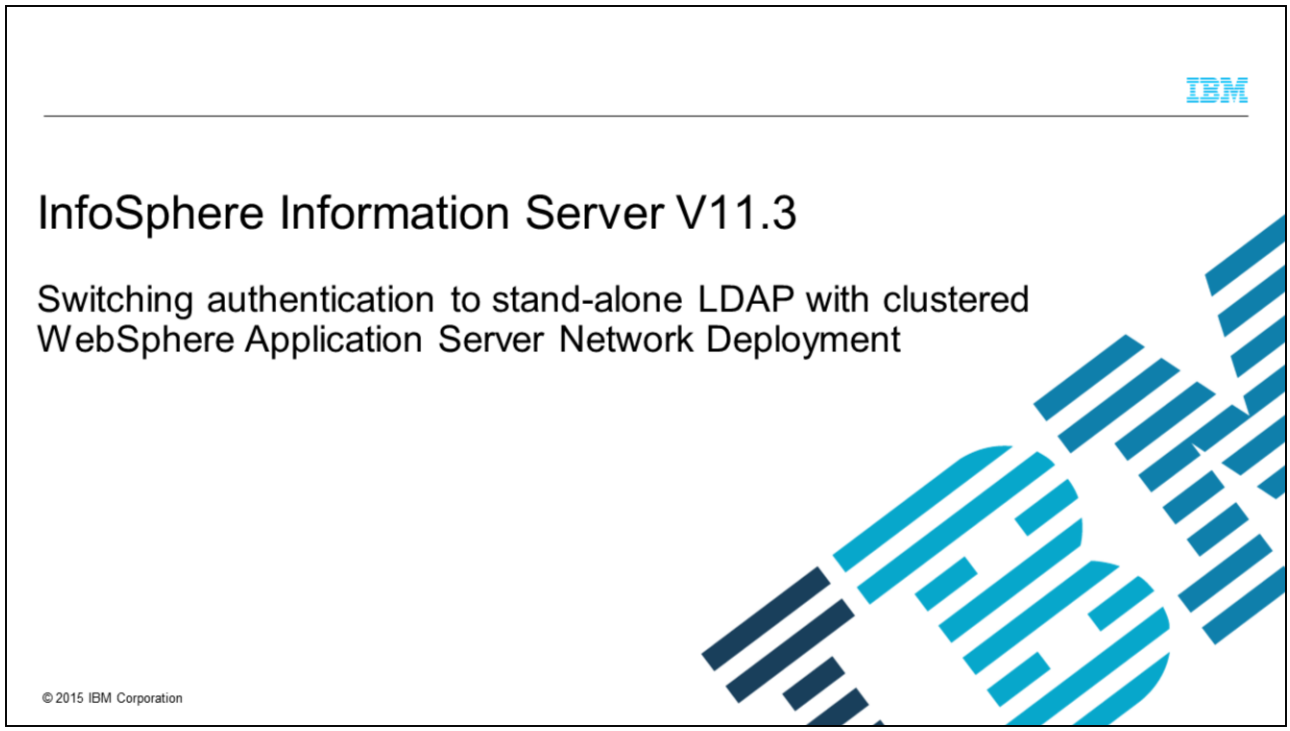


This presentation will discuss how to switch InfoSphere® Information Server 11.3 to use the stand-alone LDAP repository for authentication when WebSphere® is installed as a cluster. If you installed Information Server 11.3 with non-clustered WebSphere, refer to the IEA module Switching Information Server 9.1 - 11.3 to stand-alone LDAP with non-clustered WebSphere Application Server.

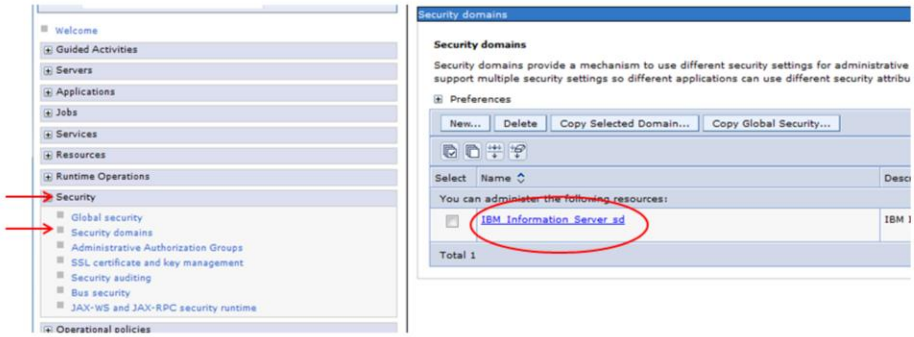
Objectives

- Set up stand-alone LDAP properties
- Verify user and group filters
- Finding proper case for base distinguished name
- Add Information Server admin user

The objectives of this presentation are to show how to set up the LDAP properties for stand-alone LDAP configured with Information Server 11.3 on a WAS cluster. It will also describe how to verify the user and group filters and how to determine the case of the base distinguished name. This presentation will also show how to add the Information Server administrative user.

Set stand-alone LDAP properties (1 of 4)

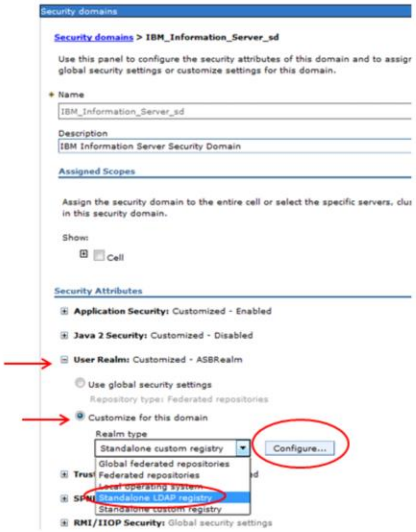
- Security => Security domains
- Click IBM_Information_Server_sd



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 Security domains. Next, click the Security domain name IBM_Information_Server_sd.

Set stand-alone LDAP properties (2 of 4)

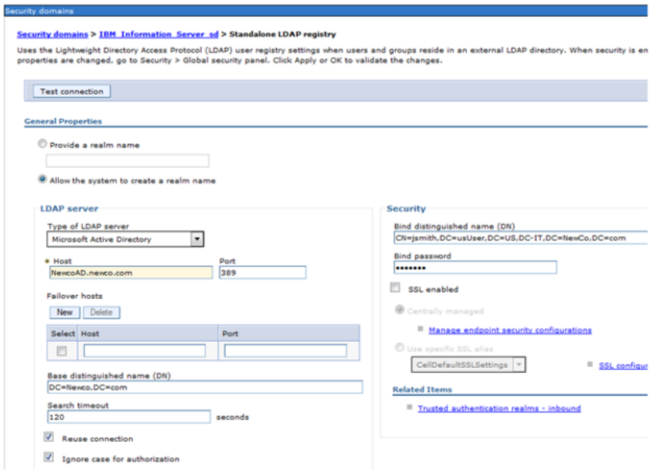
- Open User Realm
- Customize for this domain
  - Click Standalone LDAP registry
- Click configure



Next, click User Realm. Click the drop-down for the Realm type under “Customize for this domain” and pick Standalone LDAP registry. Click Configure.

Set stand-alone LDAP properties (3 of 4)

- Enter LDAP properties
  - Type of LDAP server
  - Host
  - Port
  - Base DN
    - Case needs to be exact
  - Bind DN
  - Bind password
- Click Apply
- Click Save



Under the General properties page, 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 that are returned to Information Server. Be sure that all the users and groups fall within the defined base. While WebSphere and LDAP are not case-sensitive, Information Server is. You must make sure that the case of the base DN you choose matches the case that is returned by LDAP. The next slide will discuss how to find the correct case.

Next, enter your bind distinguished name and password. The bind DN is the distinguished name of the user that is used to bind to the directory service. If your directory service supports an anonymous bind, you can leave these fields blank.

Once all the information has been entered, click Apply at the bottom of the screen and then click Save in the messages box at the top. Click Test connection to make sure that your connection to your LDAP server is working properly.

Set stand-alone LDAP properties (4 of 4)

- Base DN must be in the correct case
- Verify with LDAP viewer or ldapsearch
  - Search with a user or group

    ldapsearch –h <ldapServer> -p <ldapPort> -b <Base DN> -D <bindDN> -w <bindPasswd> cn=<groupName>

    Example

    ldapsearch –h NewcoAD.newco.com -p 389 –b "DC=Newco,DC=com" -D "CN=BndUser,CN=User,DC=Newco,DC=com" -w Bpasswd cn=IPS_Support

    Output

    CN=IPS_Support,OU=Groups,DC=Newco,DC=com

    objectClass=group

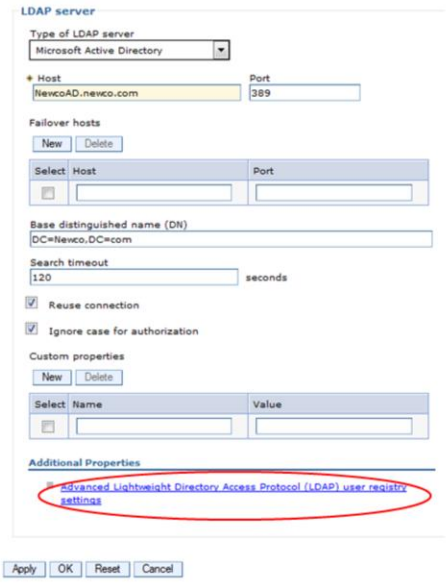
    ……

In order for Information Server to correctly create and find the user's proxy records in xmeta, you must insure that the base distinguished name configured in WebSphere is in the proper case. If you have an ldap browser, open the attributes for a user or group and look at the value of the distinguished name. If you don't have an LDAP browser, use a command-line utility like ldapsearch to retrieve the attributes.

This slide shows an example of an ldapsearch command to return the group attributes of group IPS_support. It does not matter if you use a group or user because you just need to see what the case is of the base part of the distinguished name.

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 stand-alone 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.

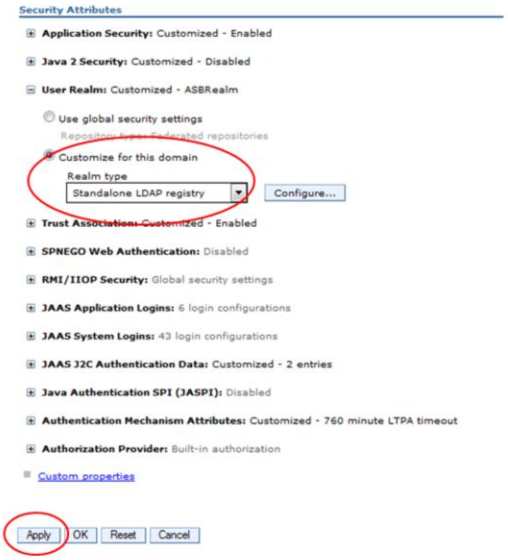
Verify filters (2 of 2)

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

Next, 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 realm type

- Security => Security domains => IBM_Information_Server_sd
- Set Realm type to Standalone LDAP
- Click Apply and Save
- Restart WebSphere Application Server cluster



Once the LDAP settings are saved, go back to the IBM_Information_Server_sd page under Security, Security domains. Be sure the Realm type under User Realm is set to Standalone LDAP registry and click apply and then save at the top of the screen. Restart the WebSphere cluster.

Update Information Server

- Login to Domain server
- Clear any internal user and group proxy records

```
cd /opt/IBM/InformationServer/ASBServer/bin
./DirectoryAdmin.sh -delete_users
./DirectoryAdmin.sh -delete_groups
```

- Add IS admin user with DirectoryAdmin.sh
  - User DN must be same case as returned by LDAP
  - UNIX® or Linux®

```
cd IBM/InformationServer/ASBServer/bin
./DirectoryAdmin.sh -admin -user -userid "CN=MyAdmin,OU=Users,DC=Newco,DC=com"
```

  - Windows®

```
cd IBM\InformationServer\ASBServer\bin
.\DirectoryAdmin.bat -admin -user -userid "CN=MyAdmin,OU=Users,DC=Newco,DC=com"
```

- Login to IS web console as MyAdmin
  - Set up roles
  - Add additional suite admins

The next step is to remove any users and groups that were created when Information Server was using the previous registry. Change directories to the ASBServer/bin directory and run the DirectoryAdmin command with both delete_users and delete_groups.

Next, run the DirectoryAdmin command as shown on this slide to add an Information Server administrative user. The user id needs to be the user's full distinguished name. Be sure the case is the same as seen with the ldap browser or the ldapsearch command.

Once that has completed successfully, you are ready to go into the Information Server web console. The first time you log into the Information Server web console, you need to use the IS administrative user you specified with the DirectoryAdmin command. Once you open the Information Server web console, you can set the user roles as needed.

Trademarks, disclaimer, and copyright information