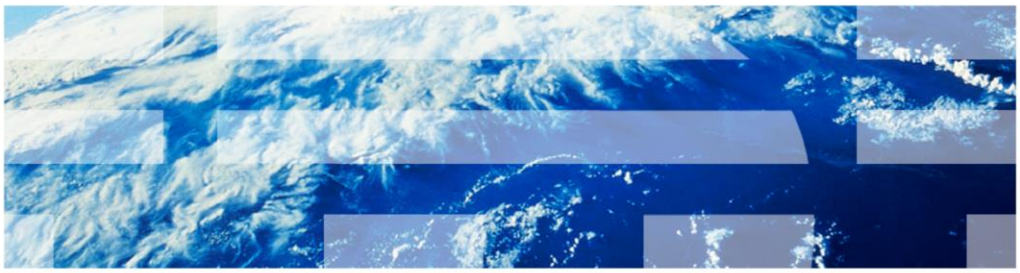
InfoSphere Information Server

Switching Information Server 8.5 and 8.7 to use federated repositories for LDAP authentication



This presentation will discuss how to switch Information Server version 8.5 and 8.7 and WebSphere to use federated repositories for LDAP authentication.

Objectives

- Benefits of federated repositories compared to Standalone LDAP
- Create realm definition
- Add new repositories
- Verify user and group filters
- Verify group member ID map
- Set current realm definition

The objectives of this presentation are to briefly discuss some of the benefits that federated repositories provide over Standalone LDAP. Also, how to create the initial realm definition, how to add a new repository, and how to verify user and group filters. It also discusses the group member ID map and how to set the federated repository to be the current realm definition.

Benefits of federated repositories

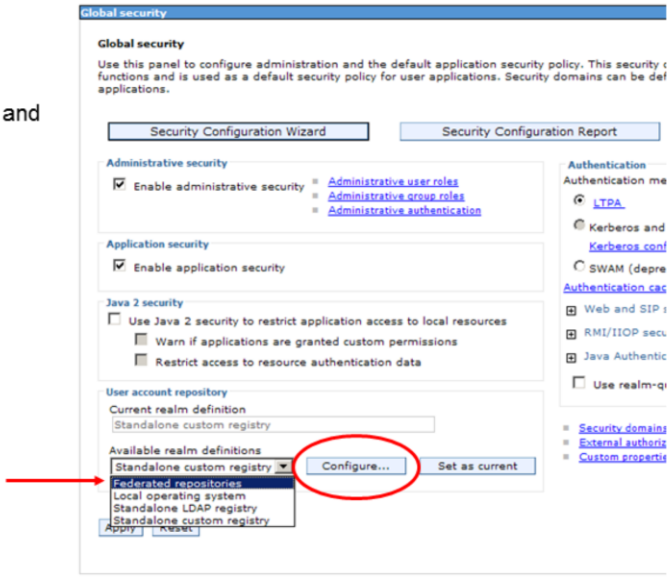
- Includes an internal file repository
  - Service users no longer need to be in LDAP
- Can configure multiple LDAP or Active Directory Domains or both
- Can have mixture of both LDAP, AD, and internal file repository
- Can define multiple search bases (optional)
- New filtering options (optional)

Information Server 8.5 and 8.7 is shipped with WebSphere 7.0 which now has an option to use federated repositories for LDAP authentication. There are several benefits to using federated repositories. One new feature is the internal file repository which is automatically created with federated repositories. This is an internal repository that is stored in WebSphere. The primary administrator user and password is kept in the internal registry and you can add other users. The benefit to this feature is that the service users such as wasadmin and isadmin no longer need to be created on the LDAP server, they can now all be stored in the internal repository.

With federated repositories, you can now specify multiple LDAP or Active Directory domains to authenticate against. It is also possible to mix the types of repositories. For example, you can configure the federated repository to authenticate against an OpenLDAP server and an Active Directory server in addition to the internal file repository. Another great feature with federated repositories is the ability to define multiple search bases for each repository. This will greatly help performance especially when multiple LDAP or Active Directory domains are specified. Federated repositories also have some new filtering capabilities that make setting up filters easier than in the 6.0 release.

Configure realm definition (1 of 2)

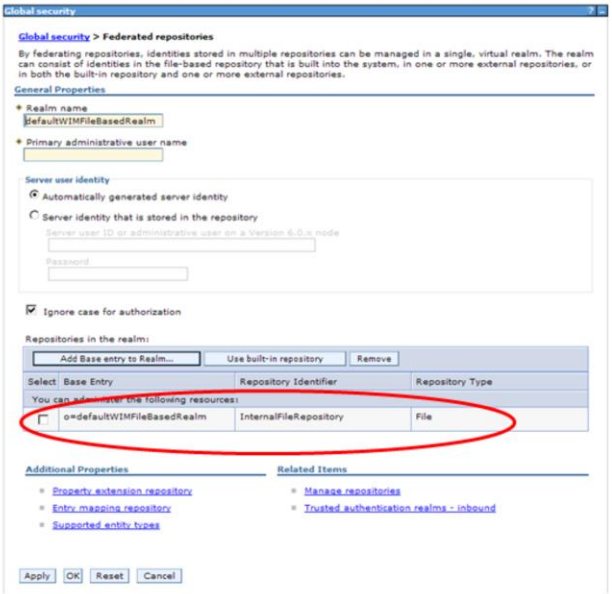
- WebSphere and federated repositories support both LDAP and Active Directory
- Select Federated repositories
- Click Configure



To set up your federated repositories, open the WebSphere Administrative console, click Security and then Global security. Click the drop down for Available realm definitions and select Federated repositories. Next, click the Configure button.

Configure realm definition (2 of 2)

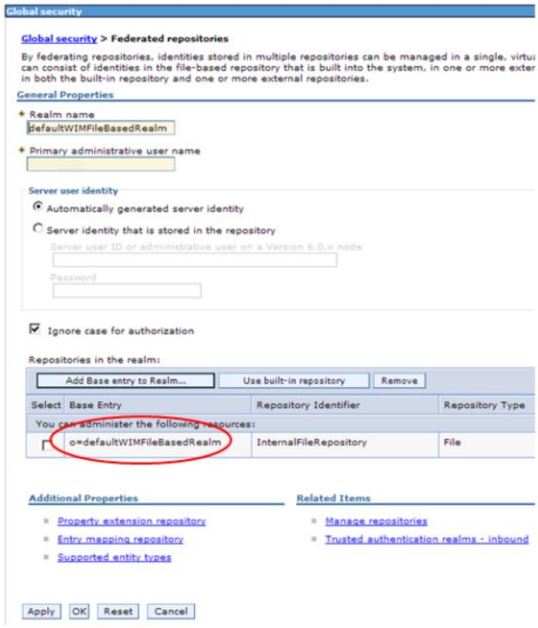
- InternalFileRepository exists by default
  - Internal to WebSphere
  - May add service users such as wasadmin and isadmin



On the Federated repositories screen, you will see that the internal file repository is created automatically. This repository may be used to store the wasadmin user and password if you do not want to use an LDAP user as the administrator. You may add other users to it as well if you have service accounts, for example, that you do not want to add to your LDAP directory .

Add new repository (1 of 5)

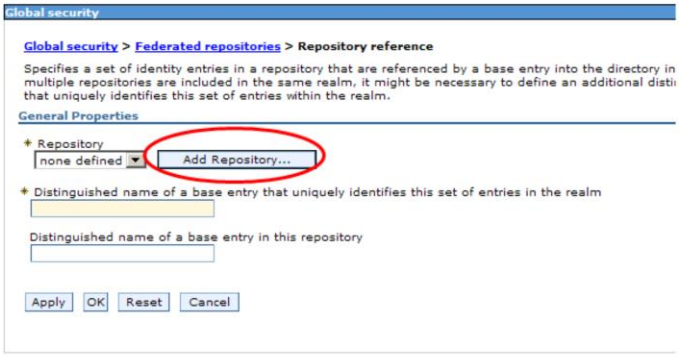
- Click Add Base entry to Realm
  - Create new repositories
  - Add multiple search bases to existing repository



Next, add the first LDAP repository. Click the Add Base entry to realm button. This can be used to create new repositories or to add another search base to an existing repository. This example shows a new repository being added.

Add new repository (2 of 5)

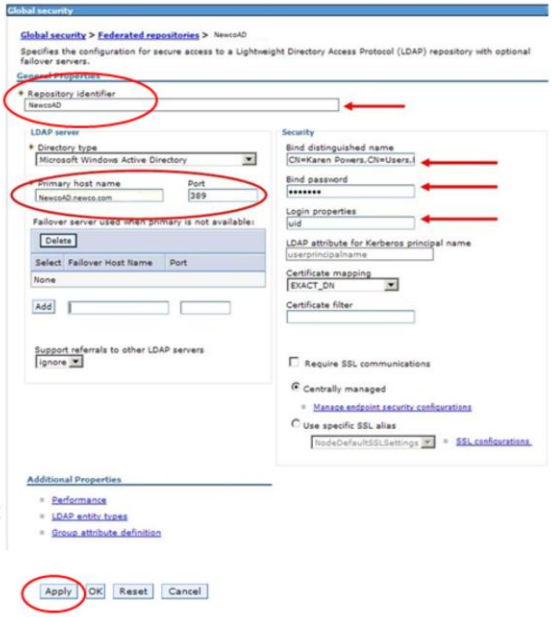
- Click Add Repository



On the next screen, click Add Repository.

Add new repository (3 of 5)

- Enter repository ID
- Select Directory type (this is important to make sure right default values are set based on server type)
- Enter Hostname, Port, Bind Distinguished name and Bind Password
- Enter Login property you want LDAP to search on
  - Add multiple login properties by separating with a ";"
  - Example: uid;mail
- Click Apply
  - Be sure message box at top does not display errors



8 Switching Information Server 8.5 and 8.7 to use federated repositories for LDAP authentication

On the General Properties screen for the new repository, enter the name of your new repository in the Repository Identifier field. Next, select the appropriate Directory type. It is important to ensure the correct directory type is selected as it will determine the default values for the LDAP entity types.

Next, enter the LDAP server name and port number. Then, enter your bind distinguished name and password if your system does not use anonymous bind. Be sure that the bind DN is the fully distinguished name for the user. There is also a Login Properties field on this screen. This field tells LDAP what user property you want to search on. In this example, it will do a search on uid. If you wanted to search for the users' mail address for example, enter mail into the Login Properties. You can also add multiple properties as well by separating the values with a semi-colon. For example, uid;mail. Click Apply and save your changes. Be sure the message box does not display any errors at this point.

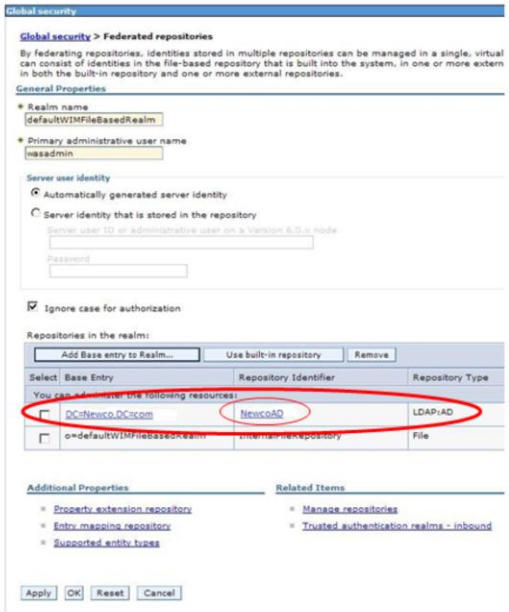
Add new repository (4 of 5)

- Add base distinguished name
  - Base DN for realm
  - Base DN for repository

The next step is to add the base distinguished name for the realm and for the repository. It is easiest to make these the same. Click Apply and Save.

Add new repository (5 of 5)

- New repository now listed
- Check user and group filters
  - Click Repository Identifier
    Example: NewcoAD



You will now see your new repository listed along with the internal file repository. The next step is to check to be sure the default user and group filters are correct. Click the repository identifier of the repository just created. In this example it is NewcoAD.

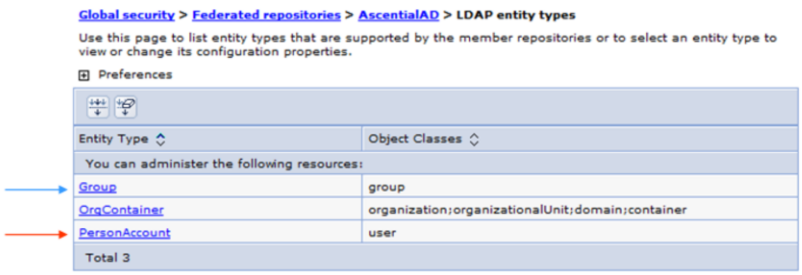
Verify default user and group filters (1 of 4)

- Check user and group filters
- Additional Properties => LDAP entity types

Federated repositories store the user and group filters under the LDAP entity types. Click LDAP entity types under Additional Properties.

Verify default user and group filters (2 of 4)

- Check that User and Group filters are correct
  - PersonAccount = User
  - Group = Group
- May need to "convert" standalone format to federated repository format
- Example 1:
  - Standalone
    LDAP User filter = (&(sAMAccountName=%v)(objectClass=user))
    LDAP Group filter = (&(cn=%v)(objectClass=group))
  - Federated repositories
    PersonAccount = user
    Group = group



The two entity types of interest are Group and PersonAccount. These are the equivalent of the Group and User filters. LDAP administrators provide the standalone LDAP syntax for the default user and group filters and it is necessary to understand how that syntax relates to the federated style of setting these filters. In this example, the user filter has an objectClass of user and the group filter has an object class of group. The screen capture displayed on this slide shows the federated repository format where the entity type for PersonAccount, which is equivalent to the User filter, has an object class of user. The entity type of Group has an object class of group.

Verify default user and group filters (3 of 4)

- Example 2
  - Standalone
    LDAP user filter = (&(uid=%v)(objectclass=inetOrgPerson))
    LDAP group filter = (&(cn=%v)(objectclass=posixGroup))
  - Federated repositories
    PersonAccount = inetOrgPerson
    Group = posixGroup

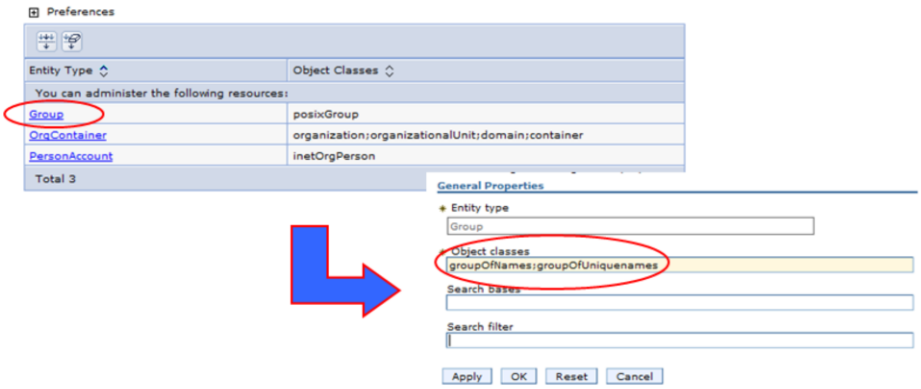
Preferences

Entity Type	Object Classes
You can administer the following resources:	
Group	posixGroup
OrgContainer	organization;organizationalUnit;domain;container
PersonAccount	inetOrgPerson
Total 3	

The next example shows a user filter with an object class of inetOrgPerson and a group filter with an object class of posixGroup. When the federated repositories entity types are displayed, you should see the entity type PersonAccount with an object class of inetOrgPerson and the group entity type with an object class of posixGroup.

Verify default user and group filters (4 of 4)

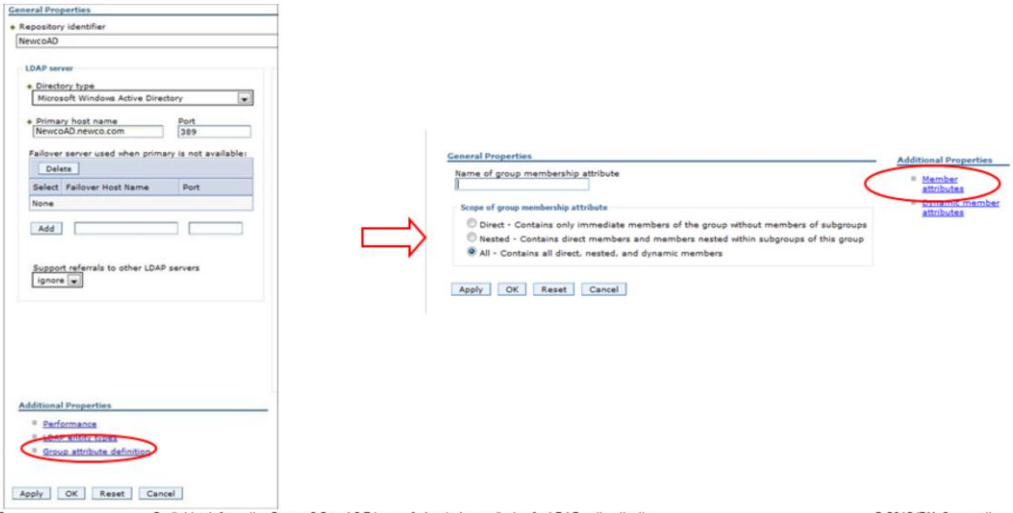
- Click Entity Type to edit
- Enter appropriate Object Class value
- Example: LDAP group filter contains multiple object classes
  (&(cn=%v)(objectClass=groupOfNames)(objectClass=groupOfUniqueNames))
- Separate multiple object classes with semi colon



If the default object class set by WebSphere is incorrect for your LDAP server, click the entity type you need to change. In this example click Group and then change the object classes as necessary. If there are multiple object classes for an entity type as in this example, you can specify all the object classes by separating them with a semi-colon.

Group member ID map (1 of 2)

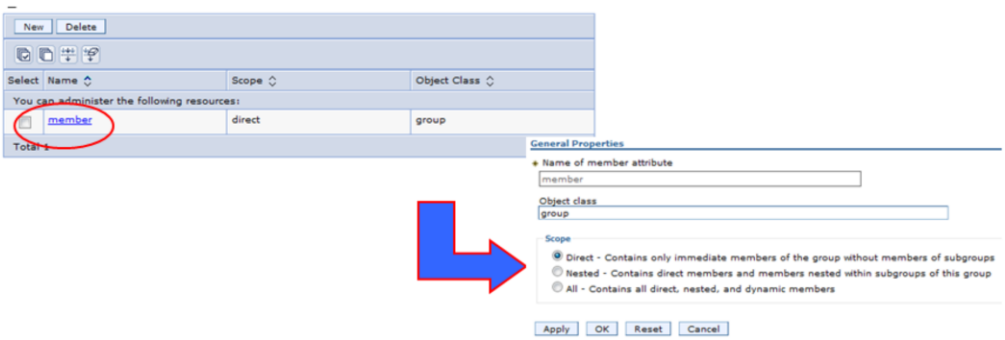
- Check Group member ID map
  - Additional Properties => Group attribute definitions
  - Additional Properties => Member attributes



The last thing that should be verified is the Group member ID map. In federated repositories with your repository properties open, click Group attribute definitions under Additional properties. On the next screen, click Member attributes under additional properties.

Group member ID map (2 of 2)

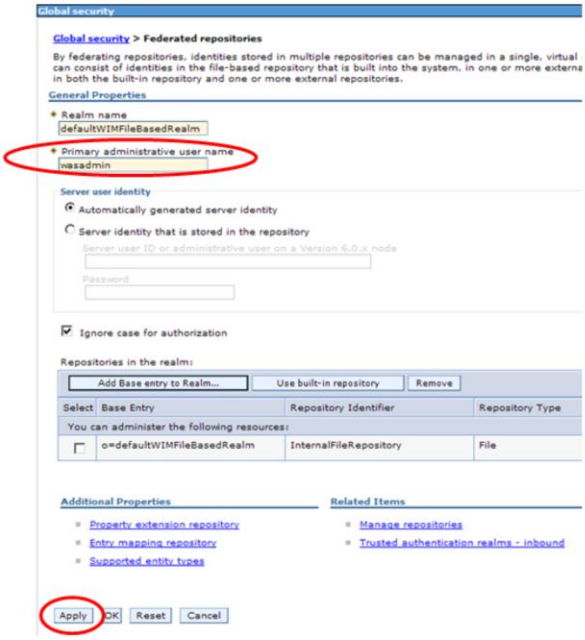
- Equivalent to Standalone LDAP group member ID map
  - Objectclass:property
  - Ex: group:member
- Click property name to change
- May add multiple properties
- Use Delete and New if default property name is incorrect



As with the entity types, the LDAP format for the group member ID map is objectClass and property name. This example shows the LDAP syntax of group:member so in the federated repository screen, the name is member and the object class is group. If the default member attribute is not the same as the LDAP filter supplied by the LDAP admin, delete the existing member attribute and click New to add a new one.

Add Primary administrative user (1 of 2)

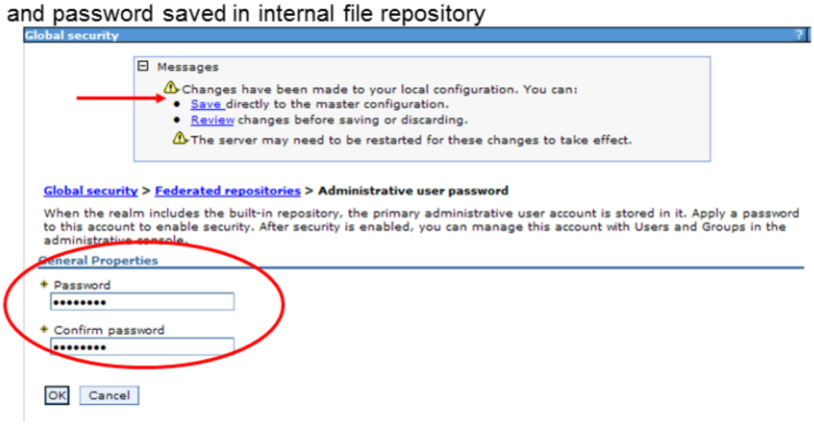
- Add wasadmin user
  - May be an LDAP user
  - May create a new WebSphere internal user
- Click Apply



The next step is to add the Primary administrative user name. This is the user that is used to login to the WebSphere Administrative console as an administrative user. This user may be an LDAP user or you may create an internal file repository user using a user name that does not exist in the LDAP registry. You can name this whatever you like. Click Apply.

Add Primary administrative user (2 of 2)

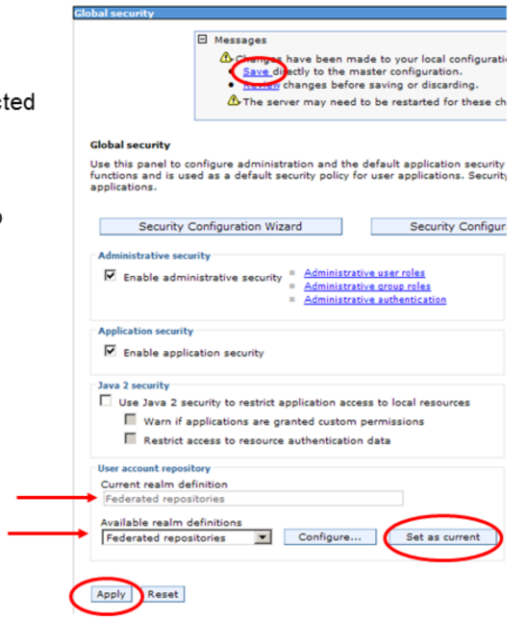
- Enter wasadmin password
- Click Save
- User and password saved in internal file repository



If the user name entered into the primary administrative user box does not exist in LDAP, WebSphere will automatically add this user to its internal file based repository. Since it is saved in the internal repository, you need to give it a password. This password can be anything you want. Enter the password, confirm the password and click Save.

Set current realm definition

- Ensure federated repositories is selected under Available realm definitions
- Click Set as current
- Current realm definition will change to federated repositories
- Click Apply
- Click Save
- Restart WebSphere



The last step is to set the federated repositories as your current realm definition. Ensure that Federated repositories is selected under the Available realm definitions and then click Set as current. You should see the Current realm definition change to Federated repositories. Click Apply and Save.

At this point, you have done the basic set up for federated repositories. You need to stop and restart WebSphere for the new settings to take effect.

Update Information Server

- Log in to Domain server as root or windows administrator
- Run AppServerAdmin
  - UNIX/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
- Log in to IS web console as wasadmin
  - Set up roles
  - Add more suite admins

On the Information Server side you need to run the AppServerAdmin command line utility as root or your 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 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 6. 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

- Additional IBM Education Assistant modules
  - Information Server 8 Advanced LDAP filtering techniques to minimize Information Server user list
  - Adding additional search bases to federated repositories

This presentation explained the basic steps to setting up a federated repository. Displayed on this slide are two additional IBM Education Assistant modules that cover more advanced topics on configuring federated repositories.

Trademarks, disclaimer, and copyright information