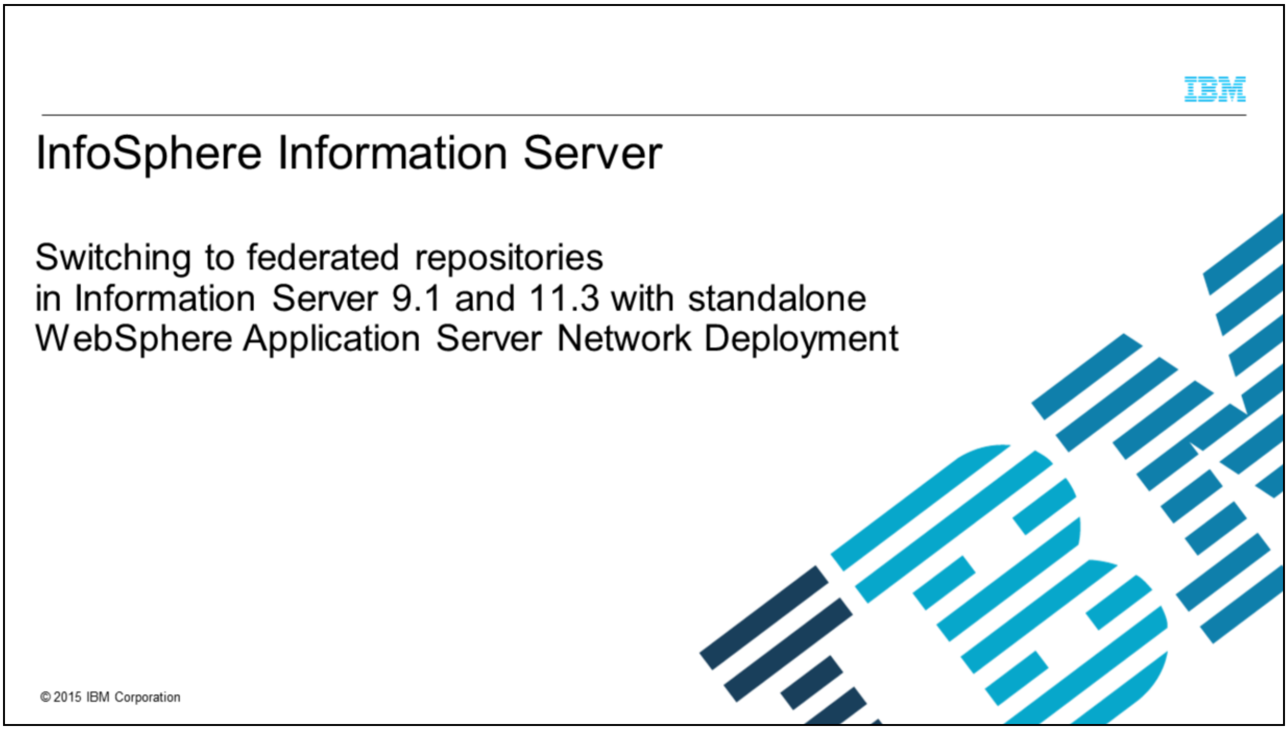
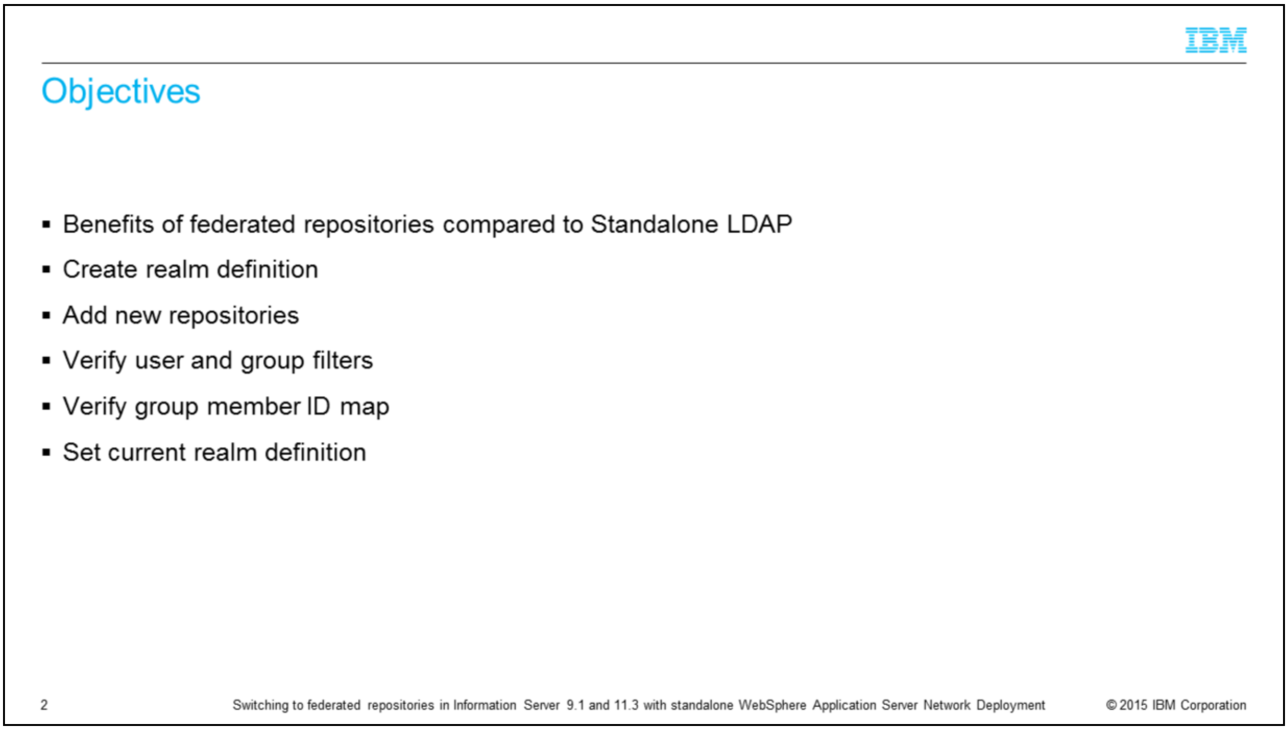


InfoSphere Information Server

Switching to federated repositories in Information Server 9.1 and 11.3 with standalone WebSphere Application Server Network Deployment

This presentation discusses how to switch Information Server version 9.1 and 11.3 and WebSphere® Application Server to use federated repositories for LDAP authentication. For version 11.3, this presentation is only applicable for WebSphere Application Server Network Deployment installations. If you are using 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 Information Server 11.3 with clustered WebSphere Application Server Network Deployment.



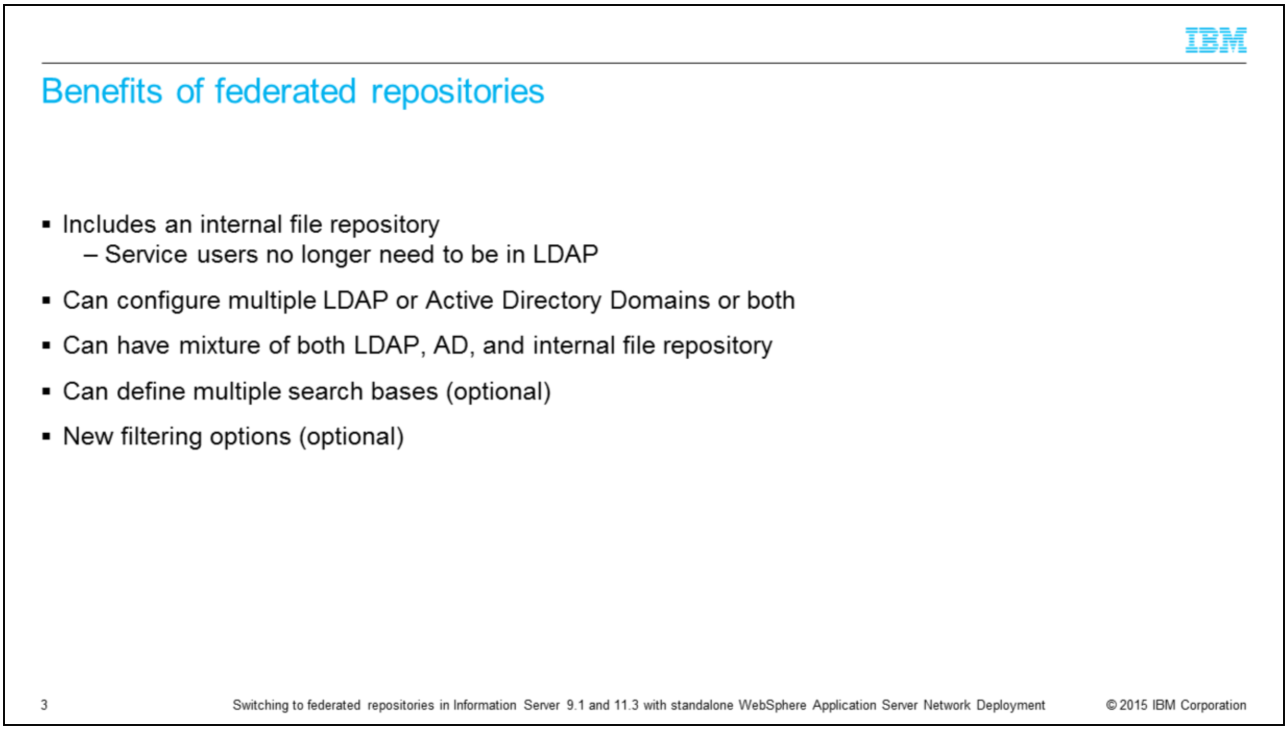
IBM

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

2 Switching to federated repositories in Information Server 9.1 and 11.3 with standalone WebSphere Application Server Network Deployment

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

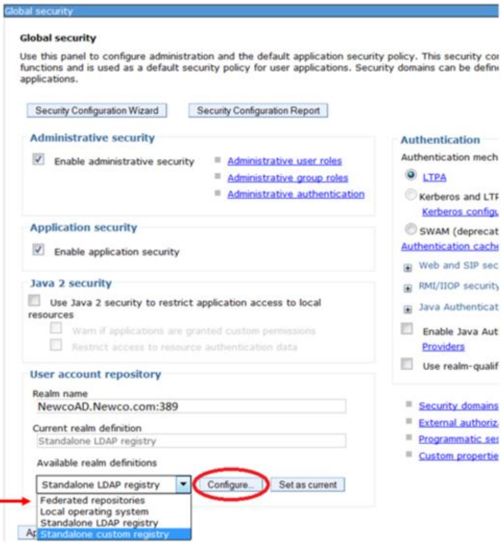
- Includes an internal file repository
  - Service users no longer need to be in LDAP
- Can configure multiple LDAP or Active Directory Domains or both
- Can have mixture of both LDAP, AD, and internal file repository
- Can define multiple search bases (optional)
- New filtering options (optional)

Information Server 9.1 and 11.3 is shipped with WebSphere 8.5 with the 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 administrative user and password may be kept in the internal registry and you can add other users to it as well. 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 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 greatly helps 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



Global security

Global security

Use this panel to configure administration and the default application security policy. This security co functions and is used as a default security policy for user applications. Security domains can be defin applications.

Administrative security

☑ Enable administrative security

Application security

☑ Enable application security

Java 2 security

□ Use Java 2 security to restrict application access to local resources

□ Warn if applications are granted custom permissions

□ Restrict access to resource authentication data

User account repository

Realm name: NewcoAD.Newco.com:389

Current realm definition: Standalone LDAP registry

Available realm definitions: Standalone LDAP registry

Authentication

Authentication mech

● LTPA

○ Kerberos and LTF

○ SWAM (deprecat

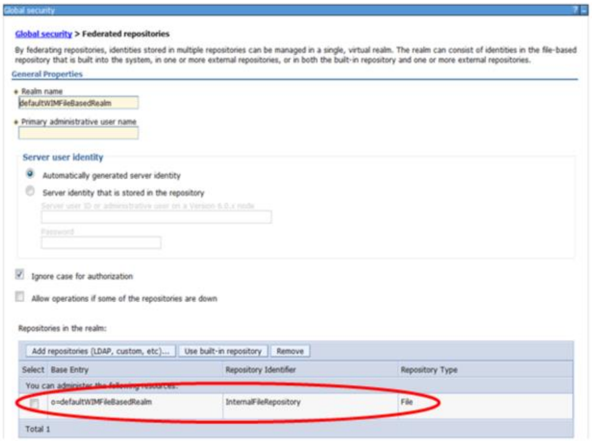
□ Enable Java Aut

□ Use realm-qualif

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



Global security > Federated repositories

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm can consist of identities in the file-based repository that is built into the system, in one or more external repositories, or in both the built-in repository and one or more external repositories.

General Properties

* Realm name
defaultWIMFileBasedRealm

* Primary administrative user name

Server user identity

● Automatically generated server identity

○ Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node

Password

☑ Ignore case for authorization

☐ Allow operations if some of the repositories are down

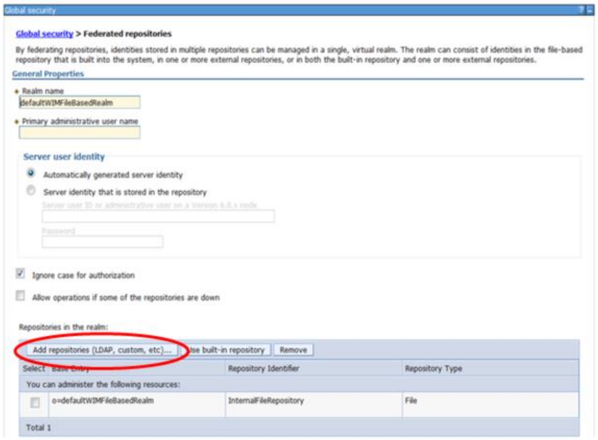
Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
☐	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 1			

On the Federated repositories screen, you will see that the internal file repository is created automatically. This repository can be used to store the wasadmin user and password if you do not want to use an LDAP user as the administrator. You can 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 repositories
  - Create new repositories
  - Add multiple search bases to existing repository



Global security

Global security > Federated repositories

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm can consist of identities in the file-based repository that is built into the system, in one or more external repositories, or in both the built-in repository and one or more external repositories.

General Properties

* Realm name: defaultWIMFileBasedRealm
* Primary administrative user name:

Server user identity

● Automatically generated server identity
○ Server identity that is stored in the repository

Password

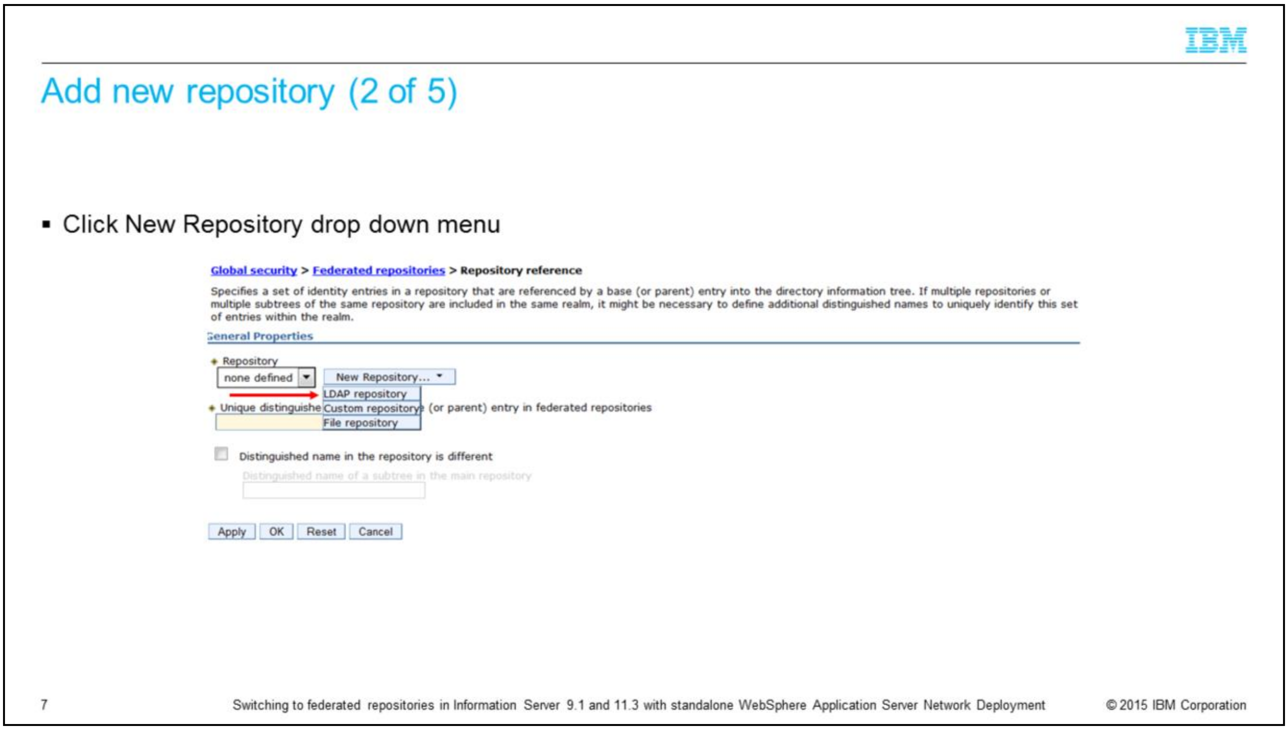
☑ Ignore case for authorization

☐ Allow operations if some of the repositories are down

Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
☐	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 1			

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 New Repository drop down menu

Global security > Federated repositories > Repository reference

Specifies a set of identity entries in a repository that are referenced by a base (or parent) entry into the directory information tree. If multiple repositories or multiple subtrees of the same repository are included in the same realm, it might be necessary to define additional distinguished names to uniquely identify this set of entries within the realm.

General Properties

* Repository: none defined

* Unique distinguishe… (or parent) entry in federated repositories

□ Distinguished name in the repository is different

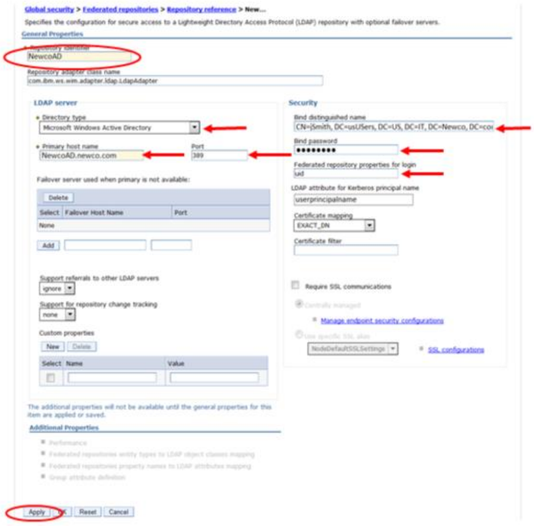
Distinguished name of a subtree in the main repository

7 Switching to federated repositories in Information Server 9.1 and 11.3 with standalone WebSphere Application Server Network Deployment © 2015 IBM Corporation

On the next screen, click the New Repository drop down menu for available repositories and select LDAP repository.

Add new repository (3 of 5)

- Enter repository ID
- Select Directory 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



Global security > Federated repositories > Repository reference > New...

Specifies the configuration for secure access to a Lightweight Directory Access Protocol (LDAP) repository with optional failover servers.

General Properties

* Repository identifier: NewcoAD

Repository adapter class name: com.ibm.ws.wim.adapter.ldap.LdapAdapter

LDAP server

* Directory type: Microsoft Windows Active Directory

* Primary host name: NewcoAD.newco.com

Port: 389

Failover server used when primary is not available:

Select	Failover Host Name	Port
None		

Support referrals to other LDAP servers: ignore

Support for repository change tracking: none

Custom properties

Select	Name	Value
□		

Security

Bind distinguished name: CN=jSmith, DC=usUSers, DC=US, DC=IT, DC=Newco, DC=co

Bind password: ●●●●●●●●●

Federated repository properties for login: uid

LDAP attribute for Kerberos principal name: userprincipalname

Certificate mapping: EXACT_DN

Certificate filter:

□ Require SSL communications

● Centrally managed

○ Use specific SSL alias: NodeDefaultSSLSettings

The additional properties will not be available until the general properties for this item are applied or saved.

Additional Properties

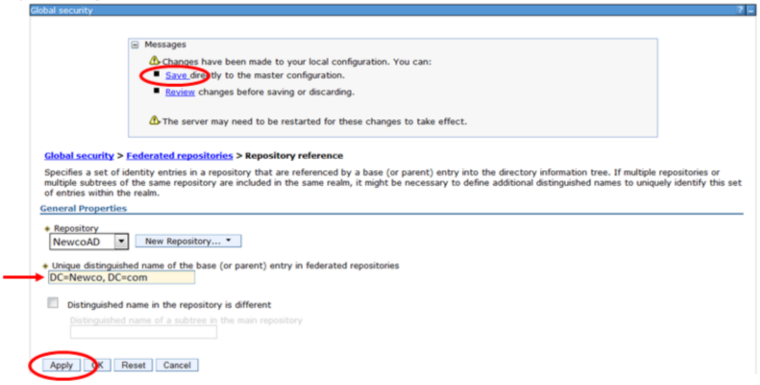
- Performance
- Federated repositories entity types to LDAP object classes mapping
- Federated repositories property names to LDAP attributes mapping
- Group attribute definition

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 distinguished name 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. In this example, it is doing 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 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



Global security

⊟ Messages

⚠ Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

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

Global security > Federated repositories > Repository reference

Specifies a set of identity entries in a repository that are referenced by a base (or parent) entry into the directory information tree. If multiple repositories or multiple subtrees of the same repository are included in the same realm, it might be necessary to define additional distinguished names to uniquely identify this set of entries within the realm.

General Properties

* Repository: NewcoAD

* Unique distinguished name of the base (or parent) entry in federated repositories: DC=Newco, DC=com

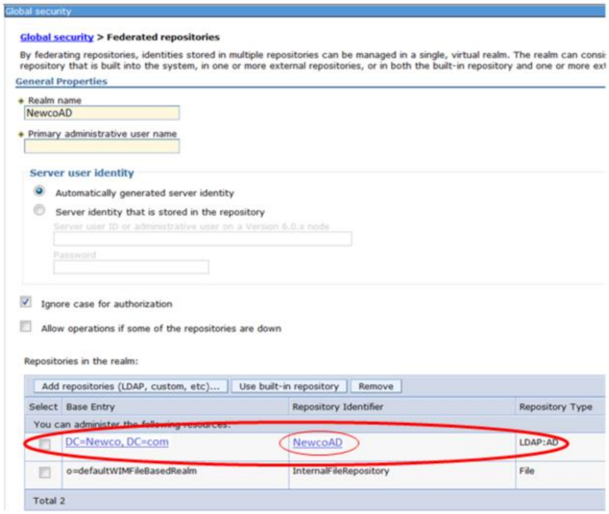
□ Distinguished name in the repository is different

Distinguished name of a subtree in the main repository:

The next step is to add the base distinguished name for the realm. If the base distinguished name for the repository is different than the realm, you can select the check box and add the base distinguished name for the repository. Click Apply and Save.

Add new repository (5 of 5)

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



Global security

Global security > Federated repositories

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm can consi repository that is built into the system, in one or more external repositories, or in both the built-in repository and one or more ext

General Properties

Realm name: NewcoAD

Primary administrative user name:

Server user identity

● Automatically generated server identity

○ Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node

Password

☑ Ignore case for authorization

□ Allow operations if some of the repositories are down

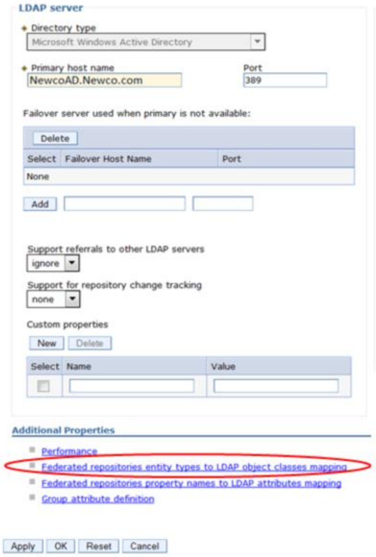
Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
□	DC=Newco, DC=com	NewcoAD	LDAP:AD
□	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 2			

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)

- Click Additional Properties => Federated repositories entity types to LDAP object classes mapping


LDAP server

◆ Directory type: Microsoft Windows Active Directory

◆ Primary host name: NewcoAD.Newco.com

Port: 389

Failover server used when primary is not available:

Select	Failover Host Name	Port
None		

Support referrals to other LDAP servers: ignore

Support for repository change tracking: none

Custom properties

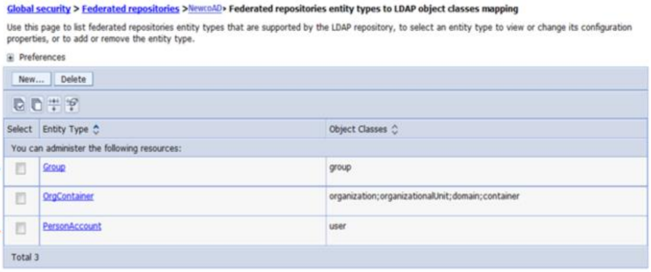
Select	Name	Value
□		

Additional Properties

- Performance
- Federated repositories entity types to LDAP object classes mapping
- Federated repositories property names to LDAP attributes mapping
- Group attribute definition

Federated repositories store the user and group filters under the LDAP entity types. Under Additional Properties, click Federated repositories entity types to LDAP object classes mapping.

Verify default user and group filters (2 of 4)



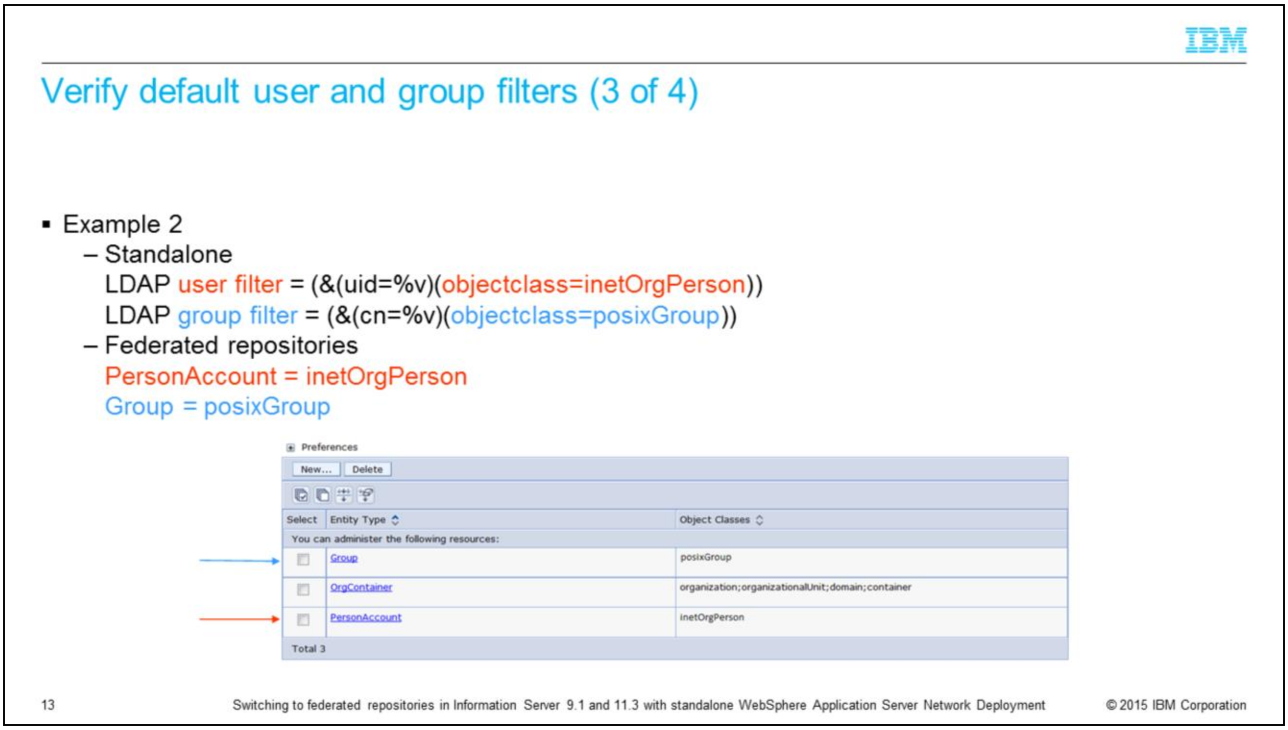
Global security > Federated repositories > NewcoAD > Federated repositories entity types to LDAP object classes mapping

Use this page to list federated repositories entity types that are supported by the LDAP repository, to select an entity type to view or change its configuration properties, or to add or remove the entity type.

Select	Entity Type	Object Classes
You can administer the following resources:		
□	Group	group
□	OrgContainer	organization;organizationalUnit;domain;container
□	PersonAccount	user
Total 3		

- 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 will 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 object class 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

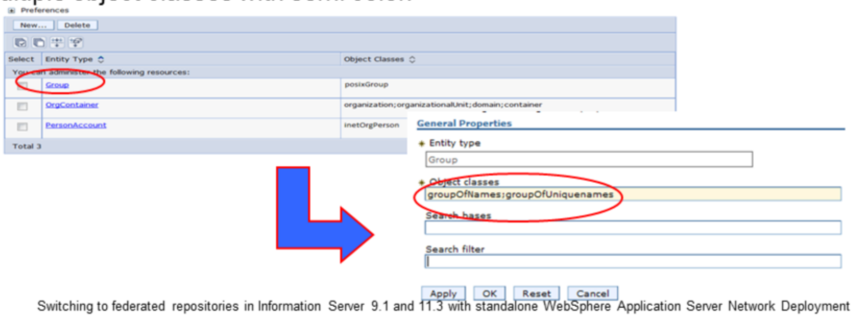
    Group = posixGroup

Select	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



⊞ Preferences

New... | Delete

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

General Properties

* Entity type: Group
* Object classes: groupOfNames;groupOfUniquenames

Search bases:

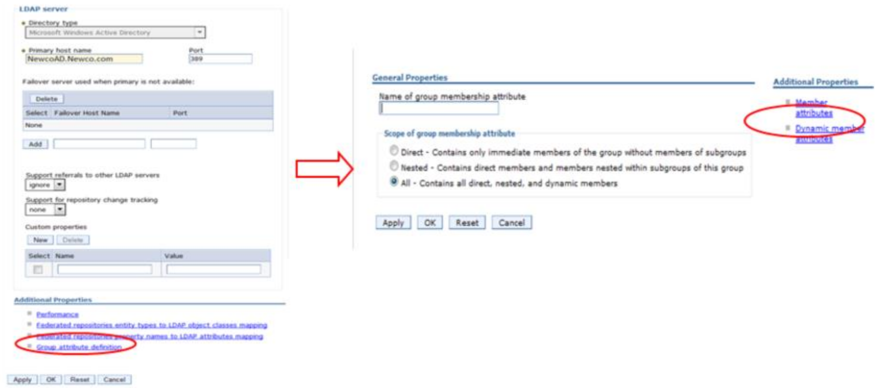
Search filter:

Apply | OK | Reset | Cancel

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 definition
  – Additional Properties => Member attributes



LDAP server

* Directory type: Microsoft Windows Active Directory

* Primary host name: NewcoAD.Newco.com

Port: 389

Failover server used when primary is not available:

Select	Failover Host Name	Port
None		

Support referrals to other LDAP servers: ignore

Support for repository change tracking: none

Custom properties

Select	Name	Value
□		

Additional Properties

- Performance
- Federated repositories entity types to LDAP object classes mapping
- Federated repositories property names to LDAP attributes mapping
- Group attribute definition

General Properties

Name of group membership attribute

Scope of group membership attribute

○ Direct - Contains only immediate members of the group without members of subgroups

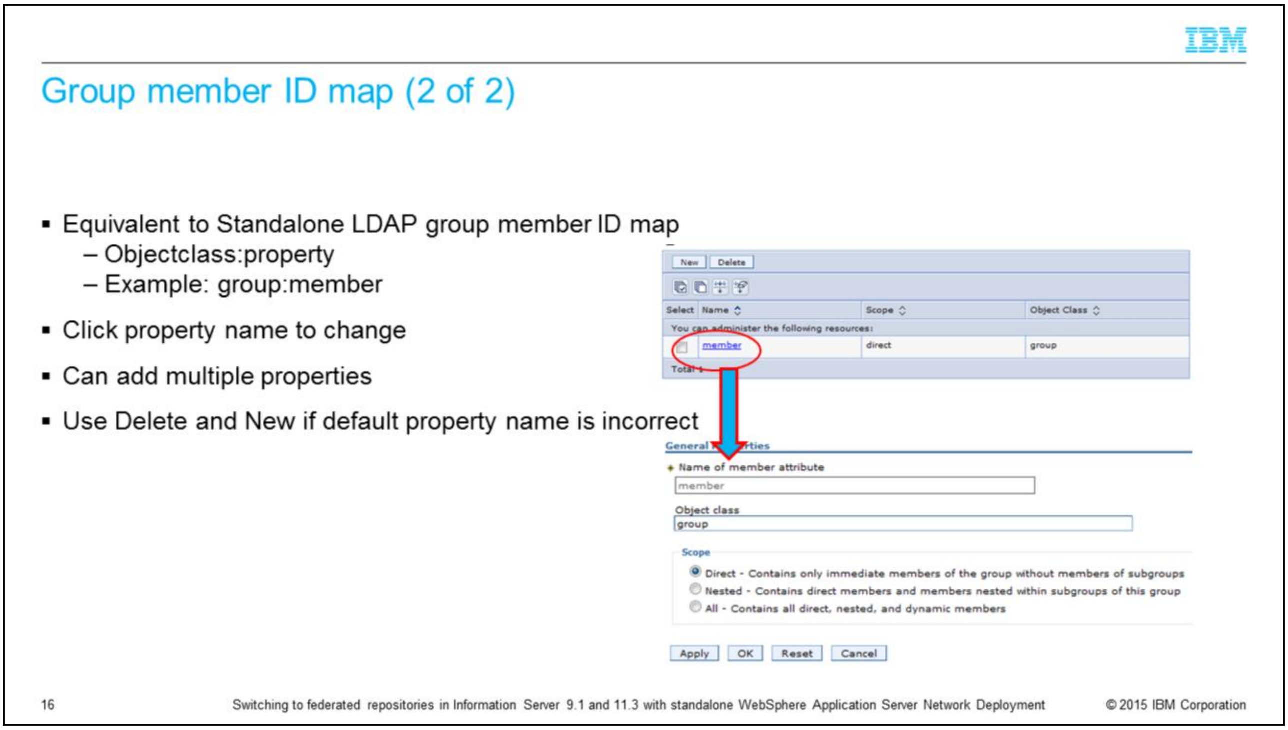
○ Nested - Contains direct members and members nested within subgroups of this group

● All - Contains all direct, nested, and dynamic members

Additional Properties

- Member attributes
- Dynamic 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 definition 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
  - – Example: group:member
- Click property name to change
- Can add multiple properties
- Use Delete and New if default property name is incorrect

Select	Name	Scope	Object Class
You can administer the following resources:			
□	member	direct	group
Total 1			

General Properties

* Name of member attribute: member

Object class: group

Scope

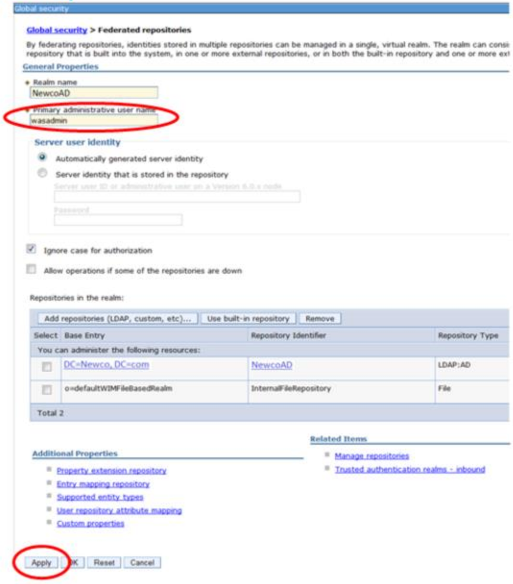
● Direct - Contains only immediate members of the group without members of subgroups
○ Nested - Contains direct members and members nested within subgroups of this group
○ All - Contains all direct, nested, and dynamic members

16 Switching to federated repositories in Information Server 9.1 and 11.3 with standalone WebSphere Application Server Network Deployment © 2015 IBM Corporation

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 administrator, 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



Global security > Federated repositories

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm can consi repository that is built into the system, in one or more external repositories, or in both the built-in repository and one or more ext

General Properties

* Realm name: NewcoAD

* Primary administrative user name: wasadmin

Server user identity

● Automatically generated server identity

○ Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node

Password

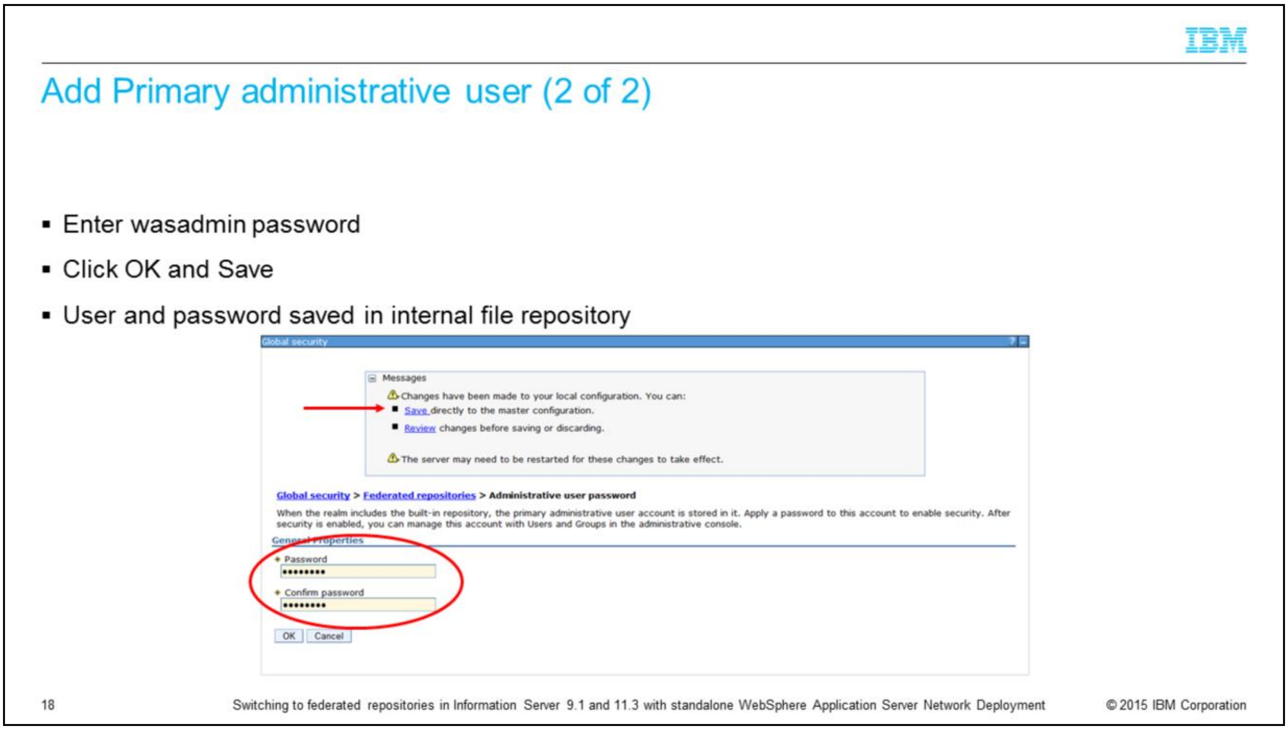
☑ Ignore case for authorization

□ Allow operations if some of the repositories are down

Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
□	DC=Newco, DC=com	NewcoAD	LDAP:AD
□	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 2			

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 OK and Save
- User and password saved in internal file repository

Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

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

Global security > Federated repositories > Administrative user password

When the realm includes the built-in repository, the primary administrative user account is stored in it. Apply a password to this account to enable security. After security is enabled, you can manage this account with Users and Groups in the administrative console.

General Properties

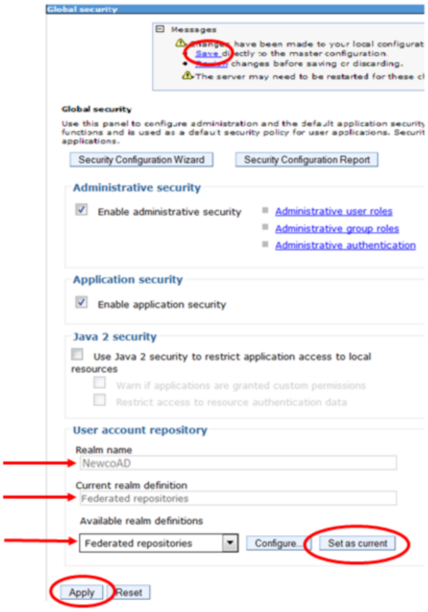
* Password: ••••••••

* Confirm password: ••••••••

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 OK and Save.

Set current realm definition

- Ensure Federated repositories is selected under Available realm definitions
- Click Set as current
- Current realm definition changes to federated repositories and Realm name is displayed
- Click Apply
- Click Save
- Restart WebSphere



Global security

⊟ Messages

⚠ Changes have been made to your local configurat

- Save directly to the master configuration.
- Review changes before saving or discarding.

⚠ The server may need to be restarted for these cl

Global security

Use this panel to configure administration and the default application security functions and is used as a default security policy for user applications. Securit applications.

[Security Configuration Wizard] [Security Configuration Report]

Administrative security

☑ Enable administrative security

- Administrative user roles
- Administrative group roles
- Administrative authentication

Application security

☑ Enable application security

Java 2 security

☐ Use Java 2 security to restrict application access to local resources

☐ Warn if applications are granted custom permissions

☐ Restrict access to resource authentication data

User account repository

Realm name: NewcoAD

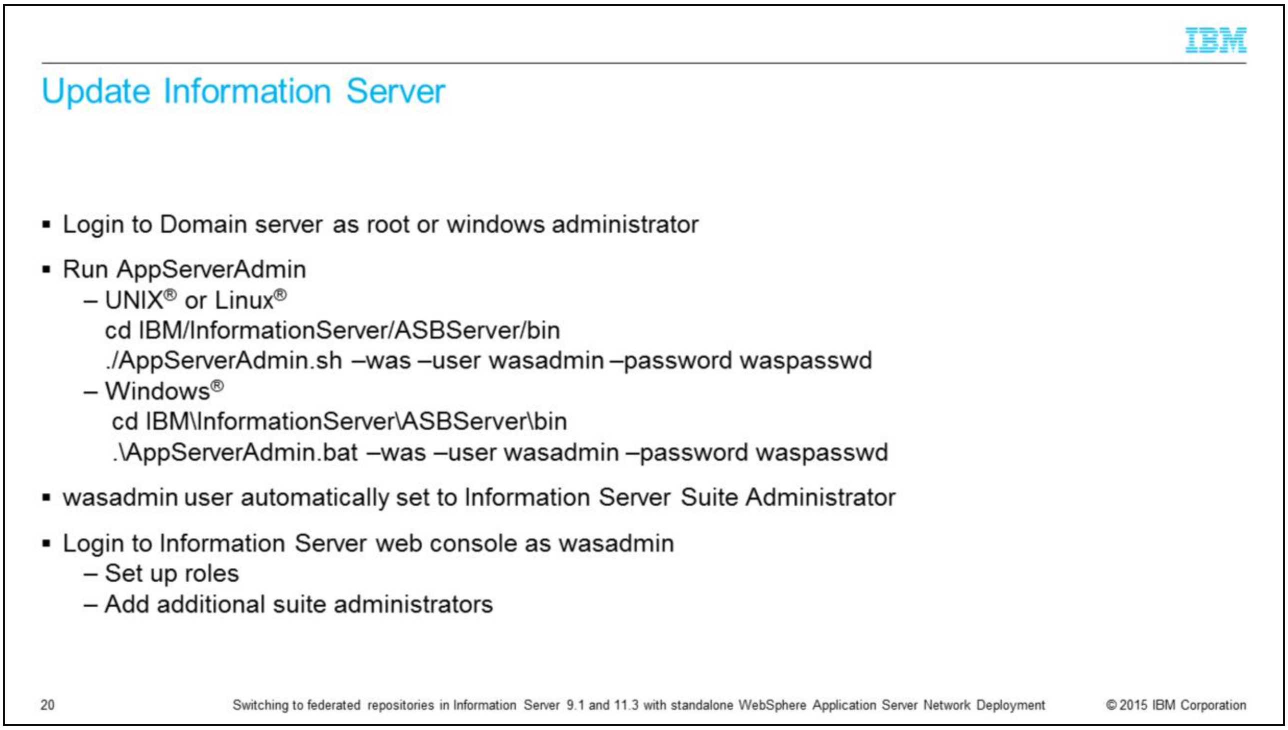
Current realm definition: Federated repositories

Available realm definitions: Federated repositories ▾ [Configure...] [Set as current]

[Apply] [Reset]

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 and Realm name displayed. 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.

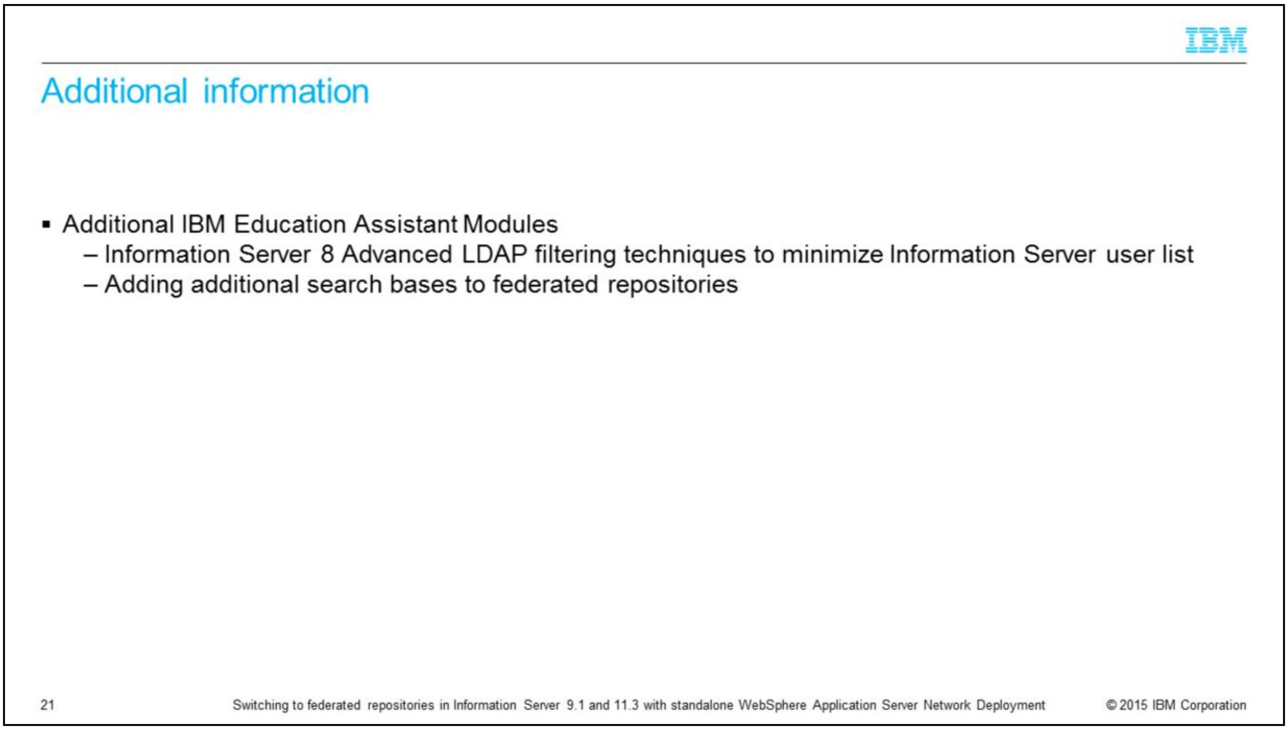


Update Information Server

- Login to Domain server as root or 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 administrators

The next step is to run the AppServerAdmin command. The AppServerAdmin command line utility needs to be run 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.

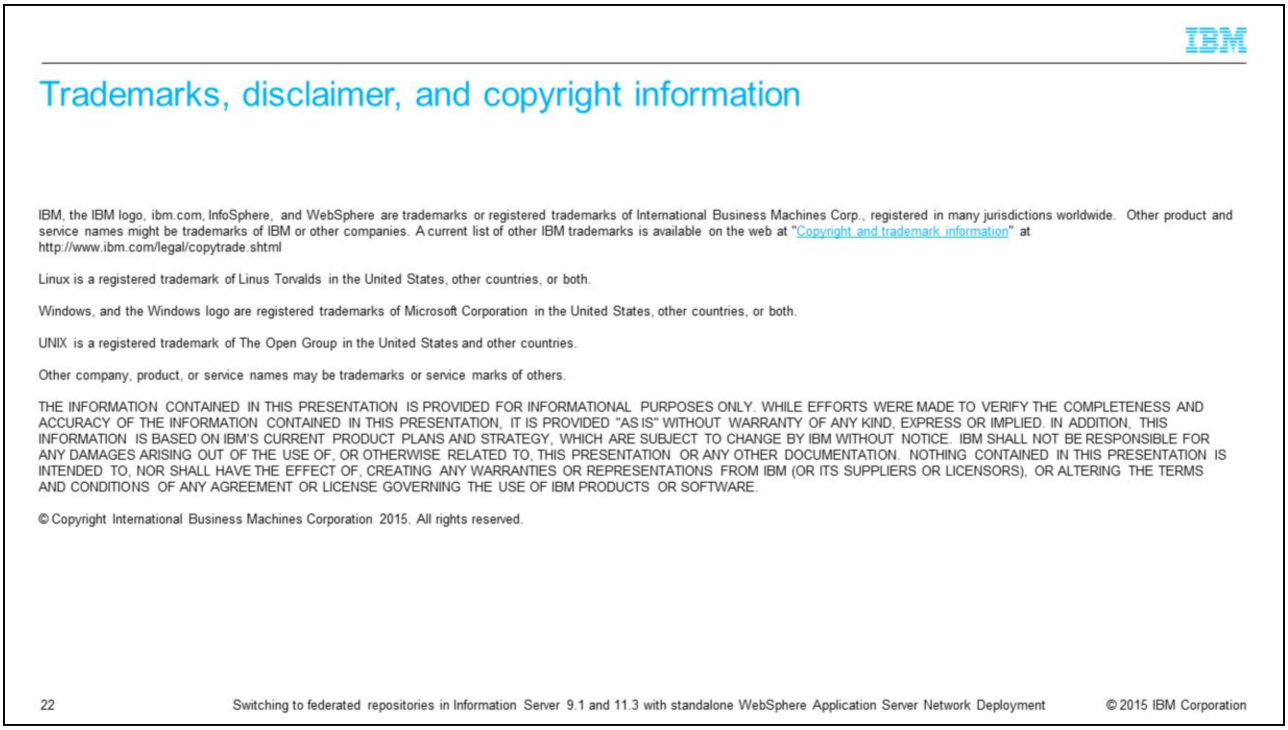
Once that has completed successfully, you are ready to go into the Information Server web console. The first time you login to the Information Server web console, you need to use the primary administrative user you specified on slide 6. This user will automatically be an Information Server suite administrator. 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

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

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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.