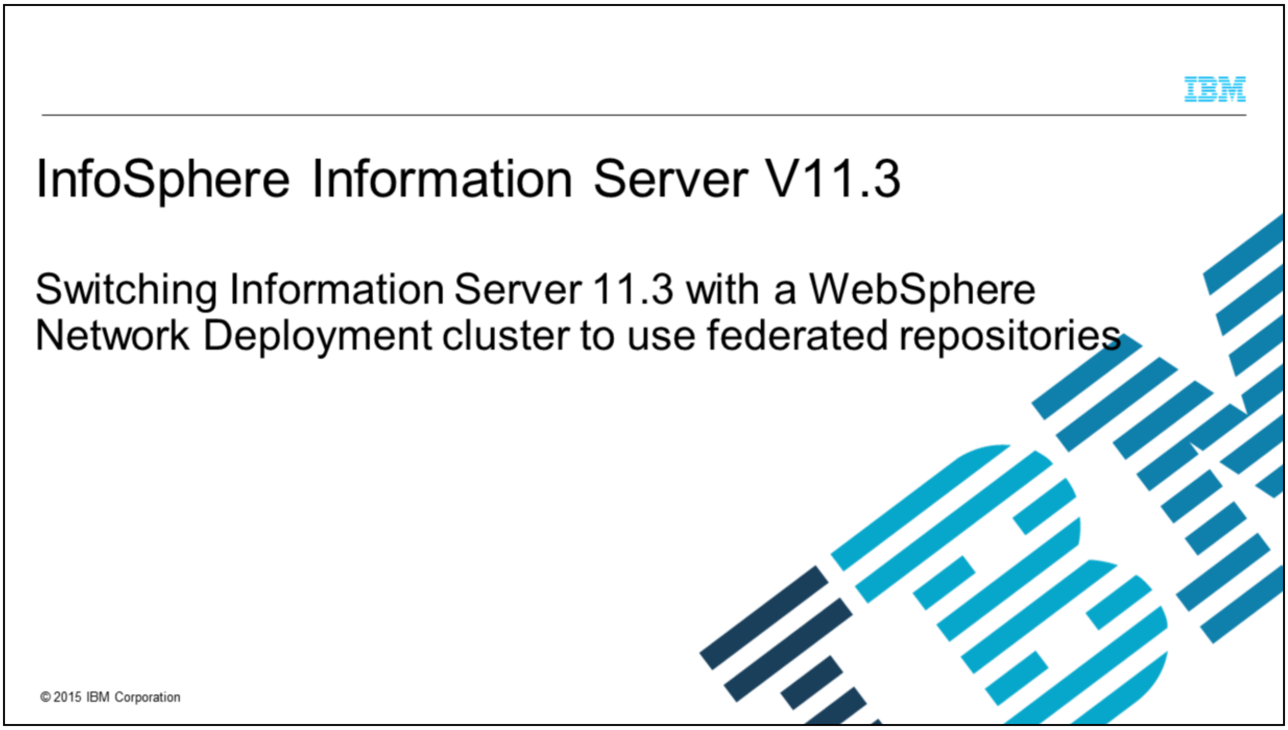
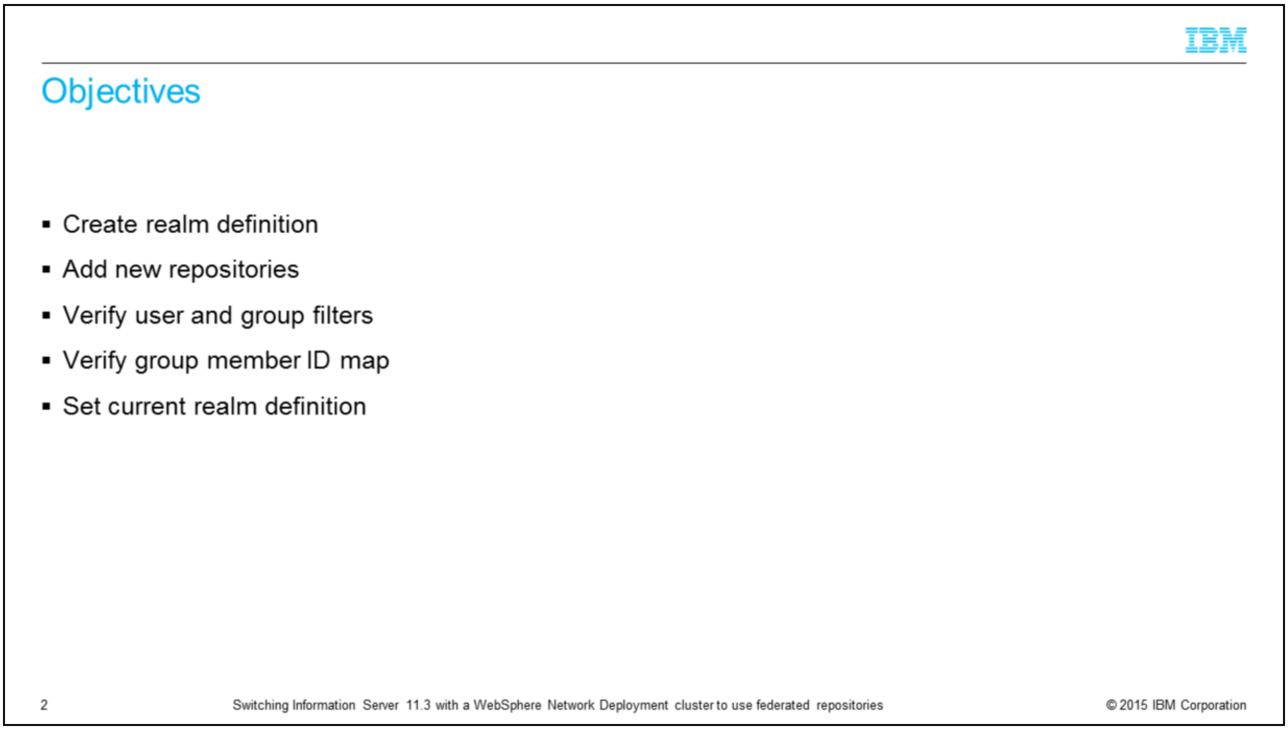


InfoSphere Information Server V11.3

Switching Information Server 11.3 with a WebSphere Network Deployment cluster to use federated repositories

This presentation will discuss how to switch Information Server version 11.3 and WebSphere® Network Deployment to use federated repositories for LDAP authentication. This presentation is only applicable for clustered WebSphere ND installations. If you are using WebSphere Liberty, refer to the IEA module on Configuring LDAP with Information Server 11.3 with WebSphere Liberty.

This presentation is not valid for Information Server 11.3 with stand-alone WebSphere ND.



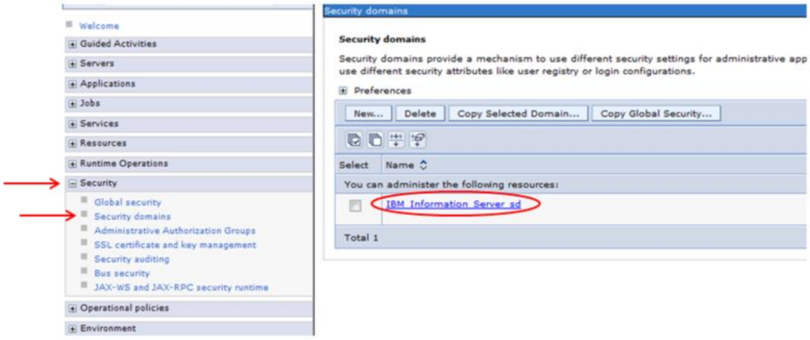
Objectives

- 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 show the user 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.

Configure realm definition (1 of 3)

- Click Security => Security domains
- Click IBM_Information_Server_sd



Security domains

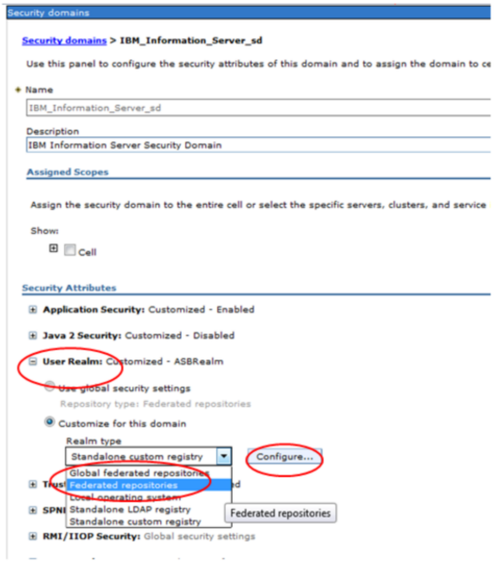
Security domains provide a mechanism to use different security settings for administrative app
use different security attributes like user registry or login configurations.

Select	Name
You can administer the following resources:	
□	IBM_Information_Server_sd
Total 1	

To set up your federated repositories, open the WebSphere administrative console, click Security and then Security domains. Click the IBM_Information_Server_sd security Domain

Configure realm definition (2 of 3)

- Click User Realm
- Click Realm Type => Federated repositories
- Click configure



Security domains

Security domains > IBM_Information_Server_sd

Use this panel to configure the security attributes of this domain and to assign the domain to ce

* Name
IBM_Information_Server_sd

Description
IBM Information Server Security Domain

Assigned Scopes

Assign the security domain to the entire cell or select the specific servers, clusters, and service

Show:
⊞ □ Cell

Security Attributes

⊞ **Application Security:** Customized - Enabled

⊞ **Java 2 Security:** Customized - Disabled

⊟ **User Realm:** Customized - ASBRealm

○ Use global security settings
Repository type: Federated repositories

● Customize for this domain

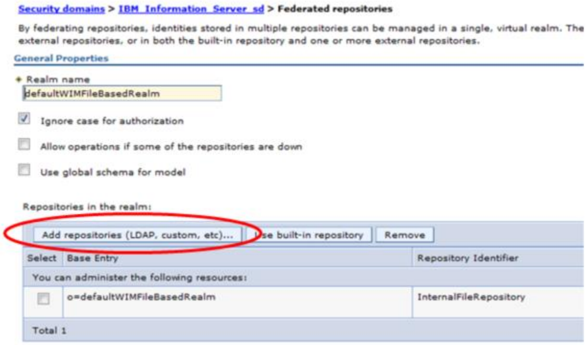
Realm type
Standalone custom registry

⊞ **RMI/IIOP Security:** Global security settings

Next, under Security Attributes click User Realm. The "Customize for this domain" radio button needs to be selected. Click the Realm type drop-down, pick Federated repositories, and click configure.

Configure realm definition (3 of 3)

- InternalFileRepository exists by default
  - Internal to WebSphere
  - May add service users that do not exist in LDAP
- Click Add repositories
  - Create new repositories
  - Add multiple search bases
  - to existing repository



Security domains > IBM Information Server sd > Federated repositories

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

General Properties

* Realm name
defaultWIMFileBasedRealm

☑ Ignore case for authorization

□ Allow operations if some of the repositories are down

□ Use global schema for model

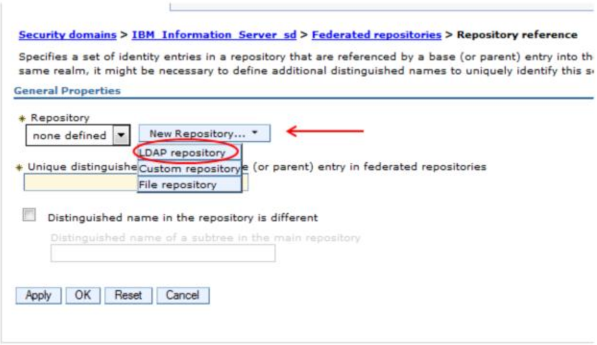
Repositories in the realm:

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

On the Federated repositories screen, you will see that the internal file repository is created automatically. This repository can be used to create local internal users that do not exist in LDAP. Next, add the first LDAP repository. Click the Add repository button.

Add new repository (1 of 4)

- Click New Repository drop down menu
- Select LDAP repository



Security domains > IBM_Information_Server_sd > Federated repositories > Repository reference

Specifies a set of identity entries in a repository that are referenced by a base (or parent) entry into th same realm, it might be necessary to define additional distinguished names to uniquely identify this s

General Properties

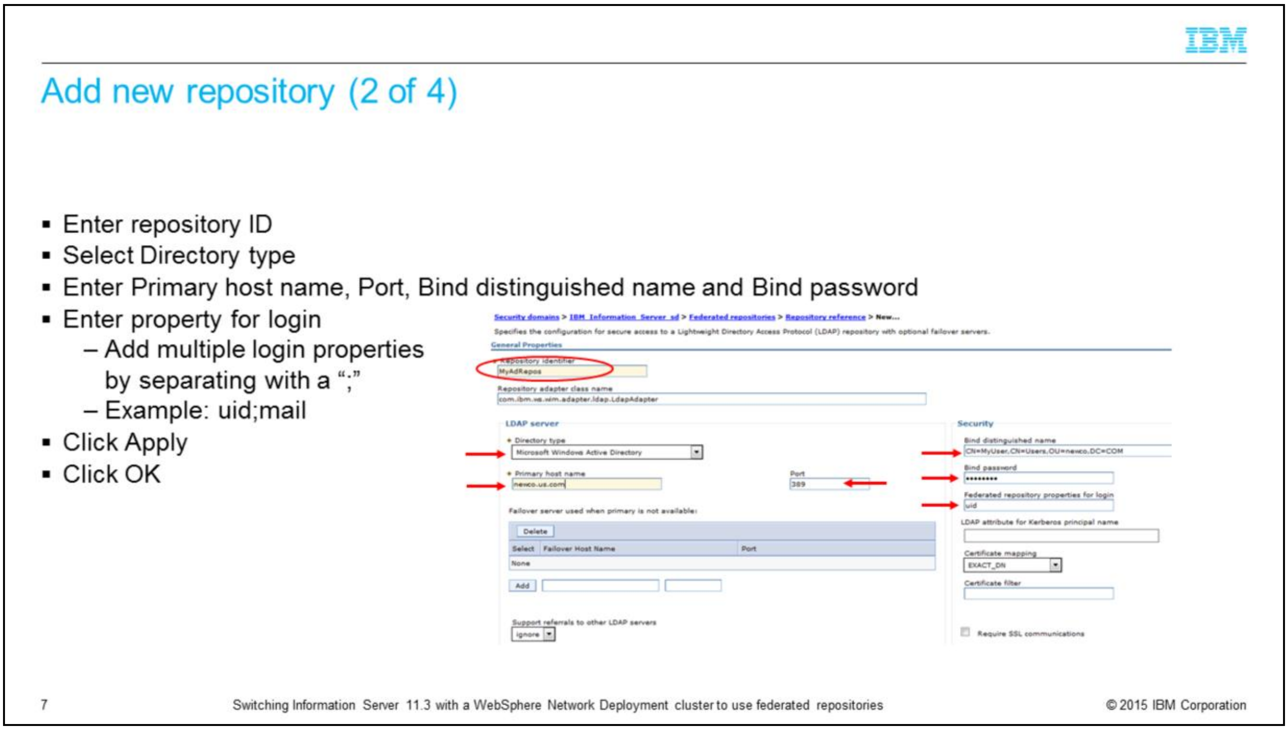
* Repository: none defined

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

□ Distinguished name in the repository is different

Distinguished name of a subtree in the main repository

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



Add new repository (2 of 4)

- Enter repository ID
- Select Directory type
- Enter Primary host name, Port, Bind distinguished name and Bind password
- Enter property for login
  - Add multiple login properties by separating with a ";"
  - Example: uid;mail
- Click Apply
- Click OK

Security domains > IBM Information Server sd > 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: MyAdRepos

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

LDAP server

* Directory type: Microsoft Windows Active Directory

* Primary host name: newco.us.com

Port: 389

Failover server used when primary is not available:

Select	Failover Host Name	Port
None		

Support referrals to other LDAP servers: ignore

Security

Bind distinguished name: CN=MyUser,CN=Users,OU=newco,DC=COM

Bind password: •••••••••

Federated repository properties for login: uid

LDAP attribute for Kerberos principal name:

Certificate mapping: EXACT_DN

Certificate filter:

□ Require SSL communications

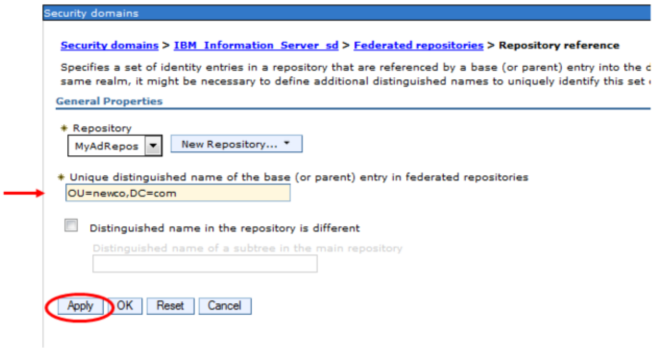
7 Switching Information Server 11.3 with a WebSphere Network Deployment cluster to use federated repositories © 2015 IBM Corporation

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 that the correct directory type is selected as it will determine the default values for the LDAP configuration.

Next, enter the LDAP server name and port number. Then, enter your bind distinguished name and password. If your system uses anonymous bind, these fields can be left blank. Be sure that the bind DN is the fully distinguished name for the user. There is also a "Federated repository properties for login" 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' email address for example, enter mail into this field. 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 that the message box does not display any errors. Click OK

Add new repository (3 of 4)

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



Security domains > IBM_Information_Server_sd > Federated repositories > Repository reference

Specifies a set of identity entries in a repository that are referenced by a base (or parent) entry into the d
same realm, it might be necessary to define additional distinguished names to uniquely identify this set

General Properties

* Repository
MyAdRepos ▾ New Repository... ▾

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

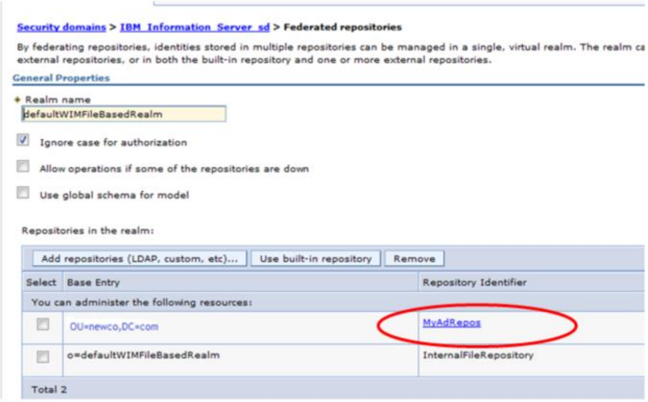
□ Distinguished name in the repository is different

Distinguished name of a subtree in the main repository

The next step is to add the base distinguished name for the federated repository. If the base distinguished name for the repository is different from the federated repository, you can select the check box “Distinguished name in the repository is different” and add the base distinguished name for the repository. Click Apply and Save.

Add new repository (4 of 4)

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



Security domains > IBM_Information_Server_sd > Federated repositories

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm ca external repositories, or in both the built-in repository and one or more external repositories.

General Properties

✦ Realm name
defaultWIMFileBasedRealm

☑ Ignore case for authorization

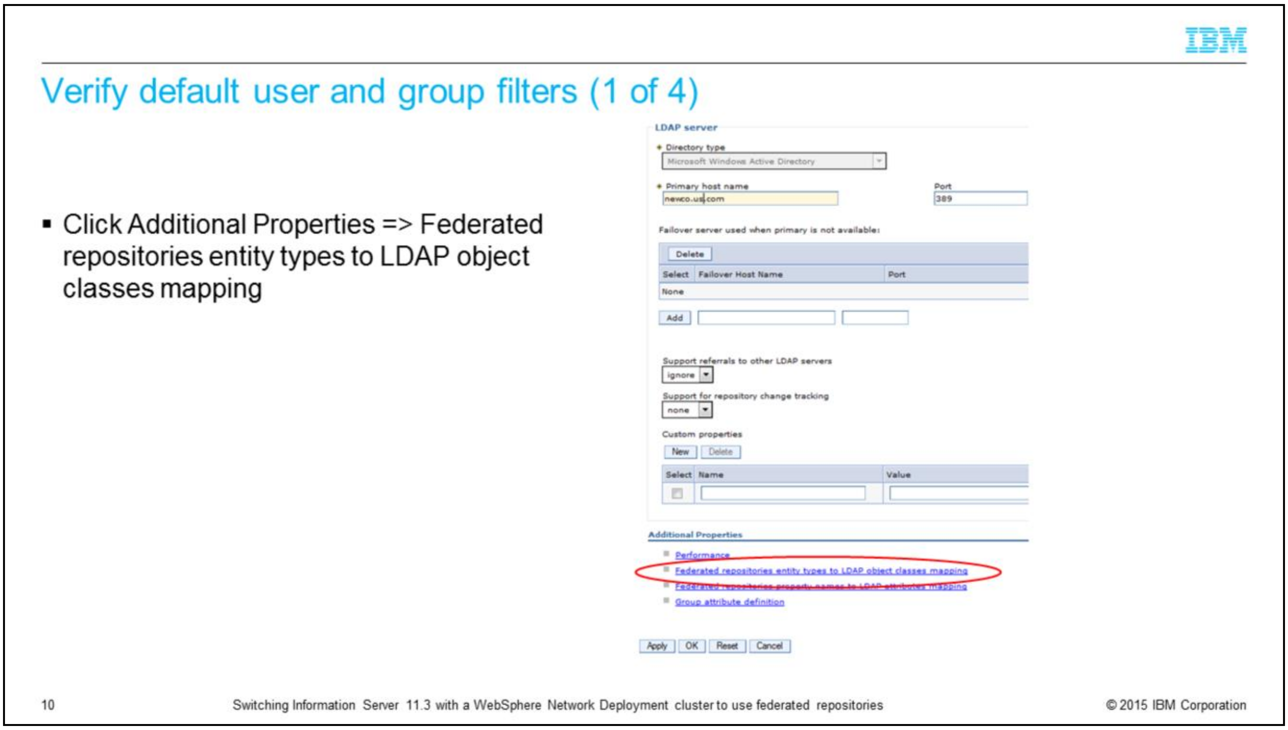
☐ Allow operations if some of the repositories are down

☐ Use global schema for model

Repositories in the realm:

Select	Base Entry	Repository Identifier
You can administer the following resources:		
☐	OU=newco,DC=com	MyAdRepos
☐	o=defaultWIMFileBasedRealm	InternalFileRepository
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 that the default user and group filters are correct. Click the repository identifier of the repository just created.



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: newco.us.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

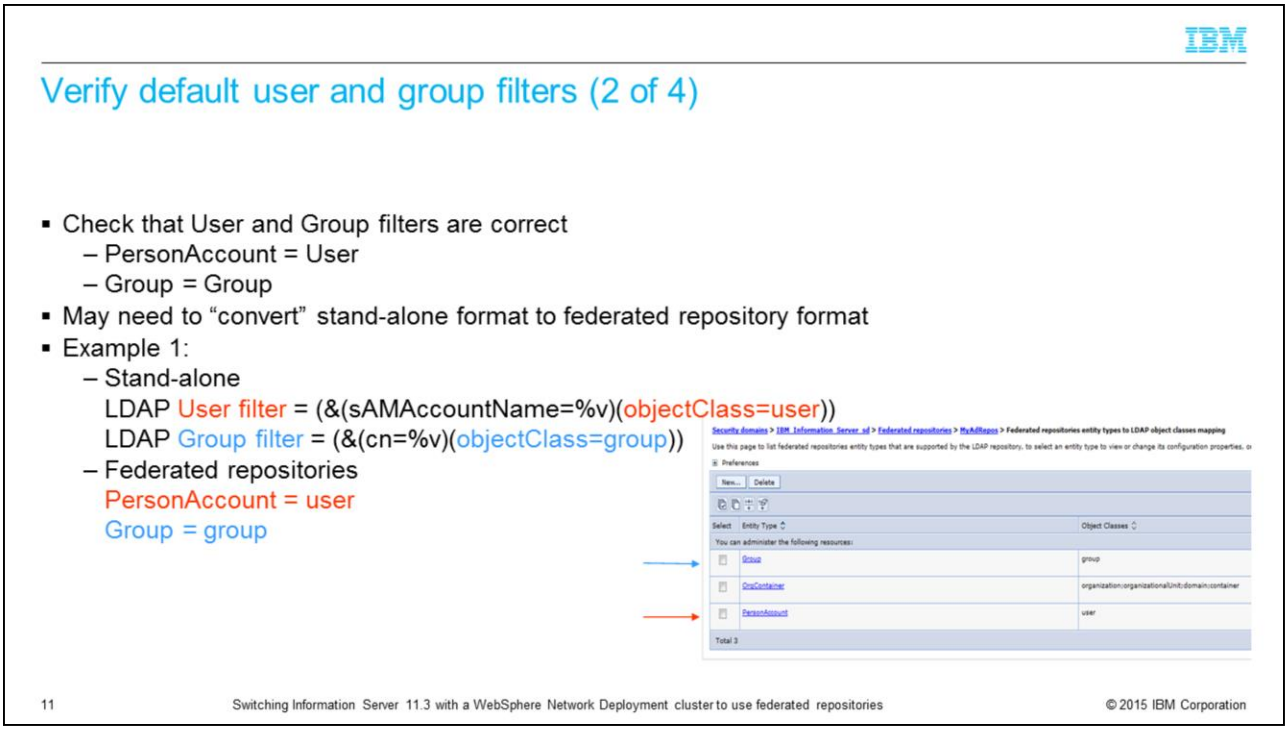
Select	Name	Value
□		

Additional Properties

- Federated repositories entity types to LDAP object classes mapping

IBM
Delete
Add
New
Delete
Performance
Federated repositories property names to LDAP attributes mapping
Group attribute definition
Apply
OK
Reset
Cancel

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)

- Check that User and Group filters are correct
  - PersonAccount = User
  - Group = Group
- May need to “convert” stand-alone format to federated repository format
- Example 1:
  - Stand-alone

    LDAP User filter = (&(sAMAccountName=%v)(objectClass=user))

    LDAP Group filter = (&(cn=%v)(objectClass=group))
  - Federated repositories

    PersonAccount = user

    Group = group

Security domains > IBM Information Server sd > Federated repositories > MyAdRepos > 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, o

⊞ Preferences

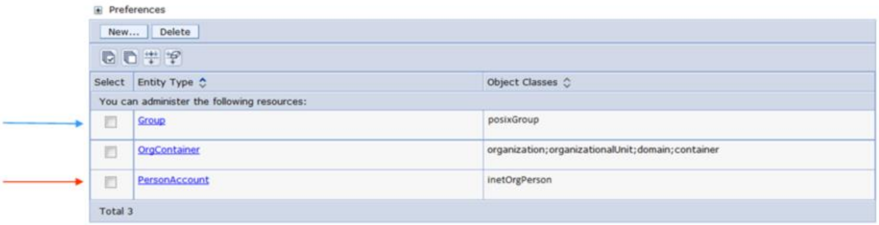
Select	Entity Type	Object Classes
You can administer the following resources:		
□	Group	group
□	OrgContainer	organization;organizationalUnit;domain;container
□	PersonAccount	user
Total 3		

11 Switching Information Server 11.3 with a WebSphere Network Deployment cluster to use federated repositories

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 stand-alone LDAP syntax for the default user and group filters. 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. 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
  - Stand-alone
    LDAP user filter = (&(uid=%v)(objectclass=inetOrgPerson))
    LDAP group filter = (&(cn=%v)(objectclass=posixGroup))
  - Federated repositories
    PersonAccount = inetOrgPerson
    Group = posixGroup

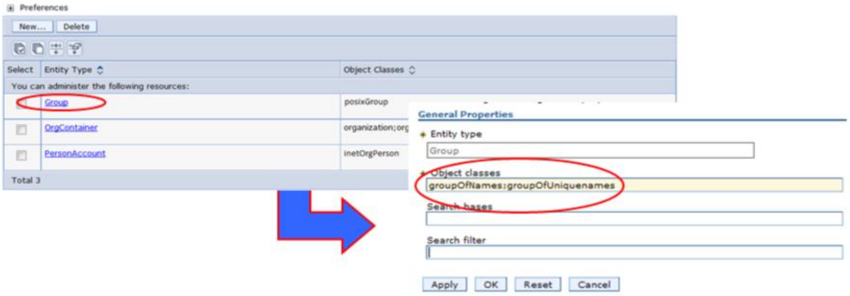


Select	Entity Type	Object Classes
You can administer the following resources:		
□	Group	posixGroup
□	OrgContainer	organization;organizationalUnit;domain;container
□	PersonAccount	inetOrgPerson
Total 3		

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 the 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



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

General Properties

Entity type: Group

Object classes: groupOfNames;groupOfUniquenames

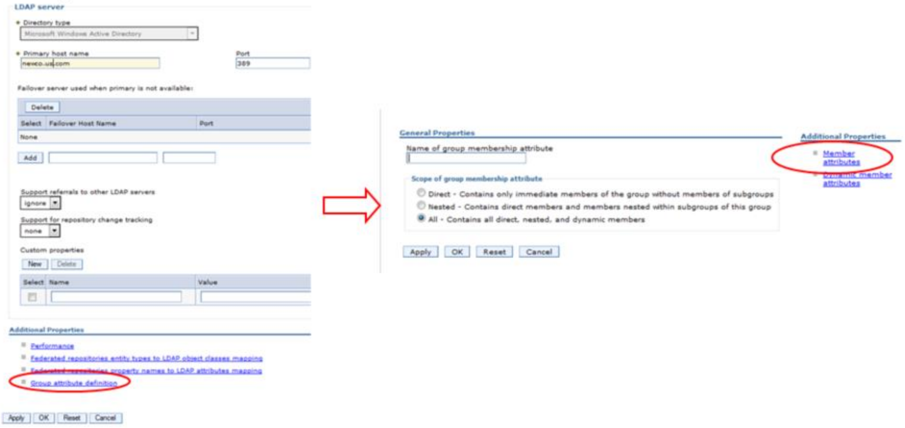
Search bases:

Search filter:

If the default object class set by WebSphere is incorrect for your LDAP server, click the entity type that 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: newco.us.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
□		

General Properties

Name of group membership attribute

Scope of group membership attribute

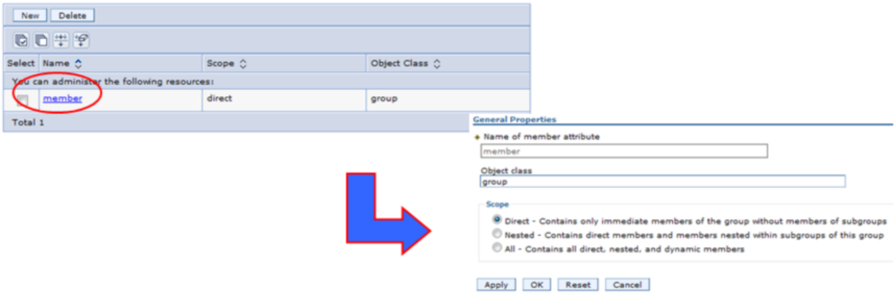
○ Direct - Contains only immediate members of the group without members of subgroups
○ Nested - Contains direct members and members nested within subgroups of this group
● All - Contains all direct, nested, and dynamic members

Delete
Add
New
Delete
Additional Properties
Performance
Federated repositories entity types to LDAP object classes mapping
Federated repositories property names to LDAP attributes mapping
Group attribute definition
Apply
OK
Reset
Cancel
Additional Properties
Member attributes
Dynamic member attributes
Apply
OK
Reset
Cancel

The last thing that needs to be verified is the Group member ID map. On the properties page for your repository, 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 Stand-alone 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 member ID map 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

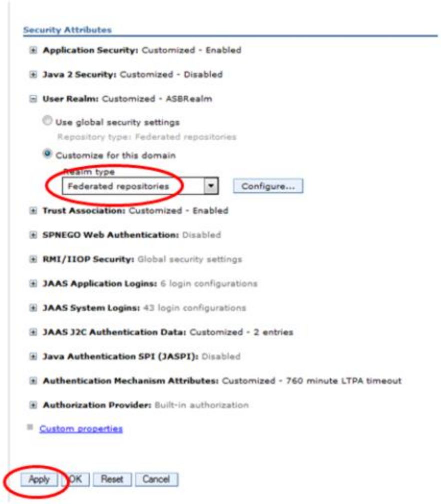
Scope

● 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

The LDAP format for the group member ID map is objectClass and property name. This example shows the LDAP syntax of group:member. For federated repositories, the name is member and the object class is group. If the member ID map of your LDAP server is different than the WebSphere default, delete the existing member ID map and click New to add a new member ID map with the appropriate name and object class.

Set realm definition

- Security domains => IBM_Information_Server_sd
- Realm type = Federated repositories
- Click apply
- Restart WebSphere



Security Attributes

⊞ **Application Security:** Customized - Enabled

⊞ **Java 2 Security:** Customized - Disabled

⊟ **User Realm:** Customized - ASBRealm

○ Use global security settings

Repository type: Federated repositories

● Customize for this domain

Realm type

Federated repositories

⊞ **Trust Association:** Customized - Enabled

⊞ **SPNEGO Web Authentication:** Disabled

⊞ **RMI/IIOP Security:** Global security settings

⊞ **JAAS Application Logins:** 6 login configurations

⊞ **JAAS System Logins:** 43 login configurations

⊞ **JAAS J2C Authentication Data:** Customized - 2 entries

⊞ **Java Authentication SPI (JASPI):** Disabled

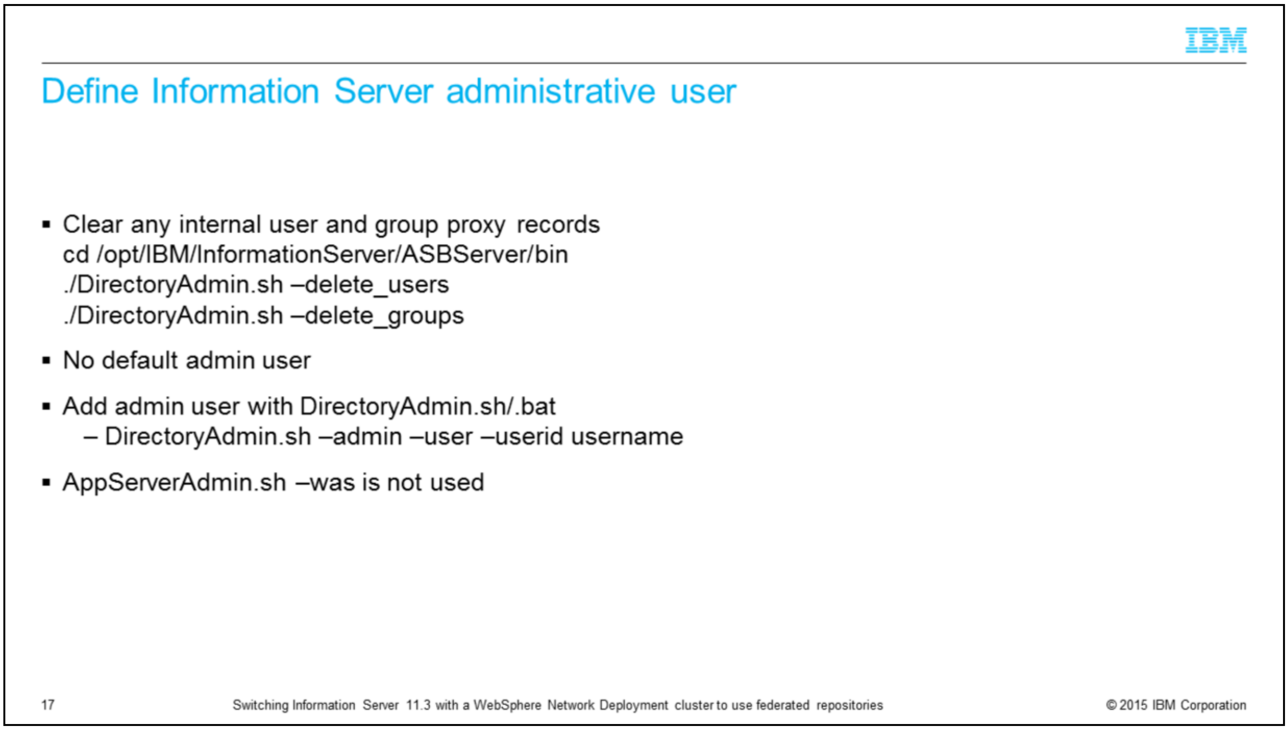
⊞ **Authentication Mechanism Attributes:** Customized - 760 minute LTPA timeout

⊞ **Authorization Provider:** Built-in authorization

Custom properties

Next, set federated repositories as your realm definition. Go back to the Security => Security domains => IBM_Information_Server_sd page. Make sure that Federated repositories is set for the Realm type. Click Apply and Save.

At this point, you have completed the basic setup for federated repositories. You need to stop and restart the WebSphere cluster.



Define Information Server administrative user

- Clear any internal user and group proxy records

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

- No default admin user
- Add admin user with DirectoryAdmin.sh/.bat
  - DirectoryAdmin.sh –admin –user –userid username
- AppServerAdmin.sh –was is not used

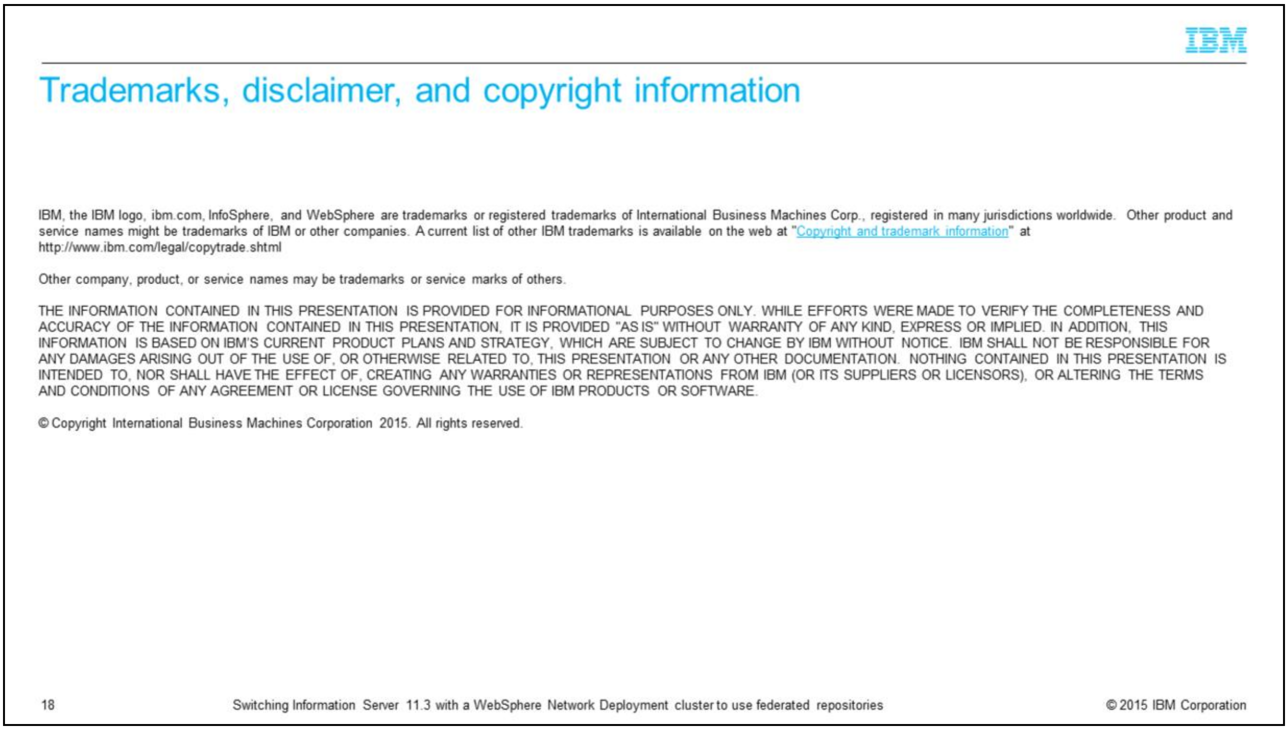
17 Switching Information Server 11.3 with a WebSphere Network Deployment cluster to use federated repositories © 2015 IBM Corporation

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.

An IS admin user will need to be added using the DirectoryAdmin command shown on this slide. The userid that is specified in the command must be the user’s short name so that it will match what is returned to Information Server by WebSphere.

The AppServerAdmin –was command is not used with a WebSphere Cluster.

The Information Server and Federated repository configuration is now complete.



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

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.