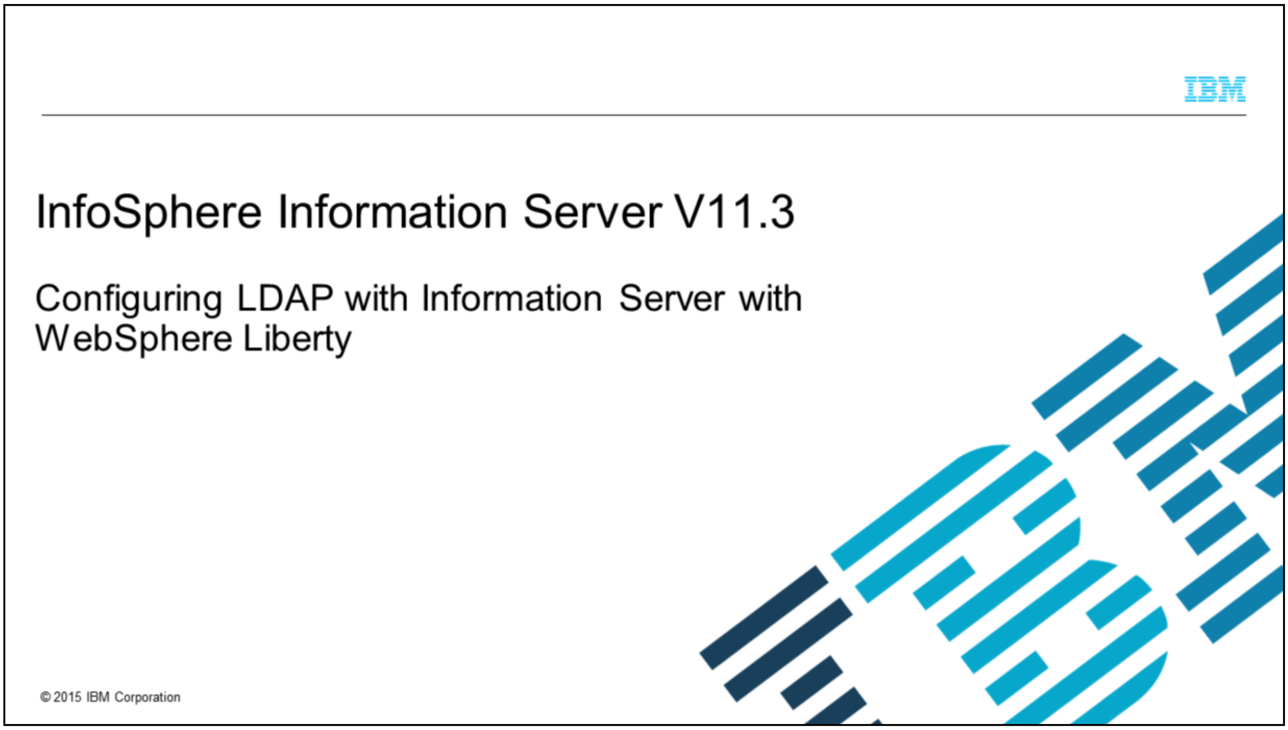
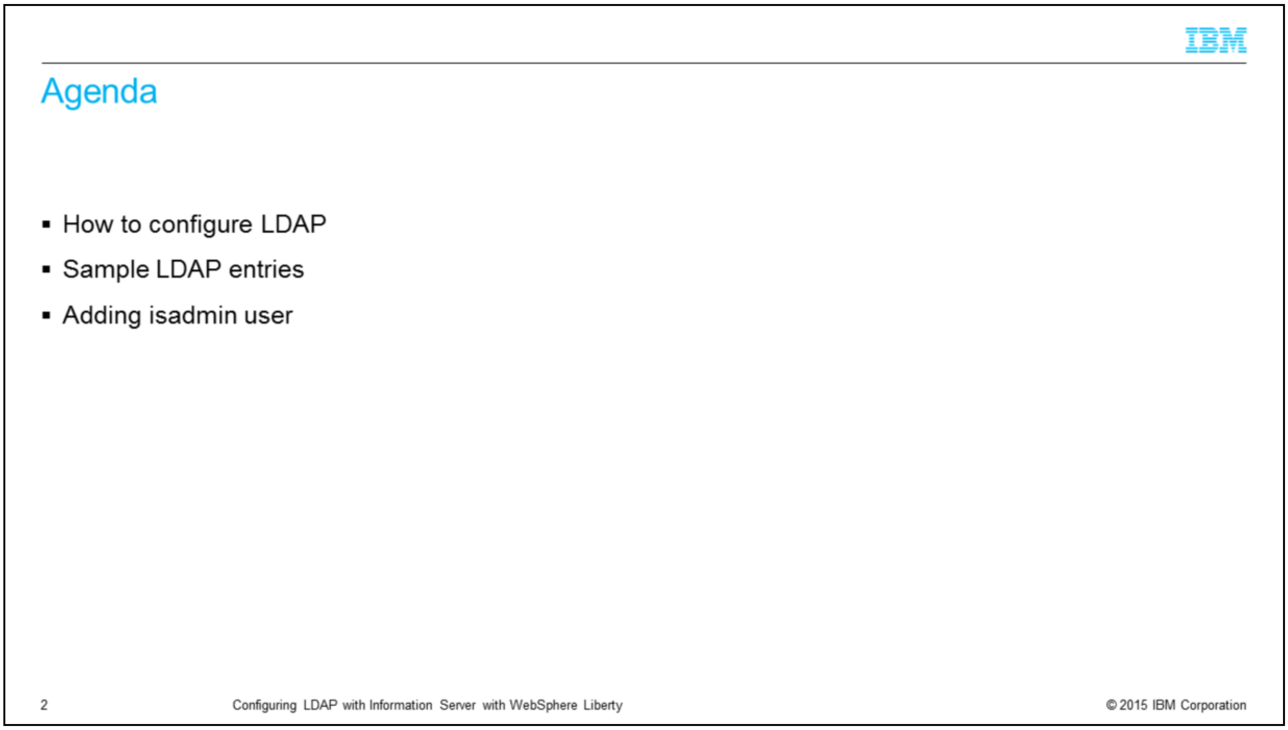


InfoSphere Information Server V11.3

Configuring LDAP with Information Server with WebSphere Liberty

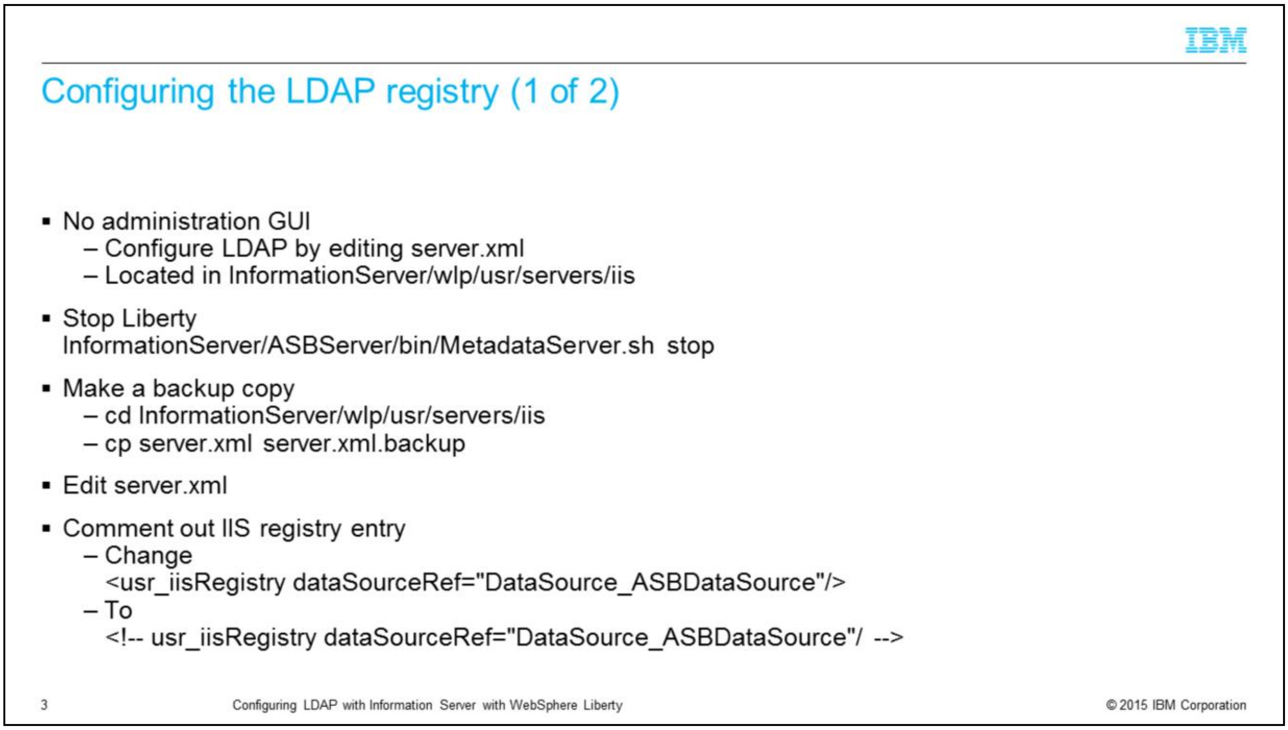
This presentation discusses how to configure Information Server version 11.3 for LDAP authentication with WebSphere® Liberty.



Agenda

- How to configure LDAP
- Sample LDAP entries
- Adding isadmin user

This presentation gives some sample LDAP entries for the different types of LDAP and discusses how to add the isadmin user after switching to LDAP.



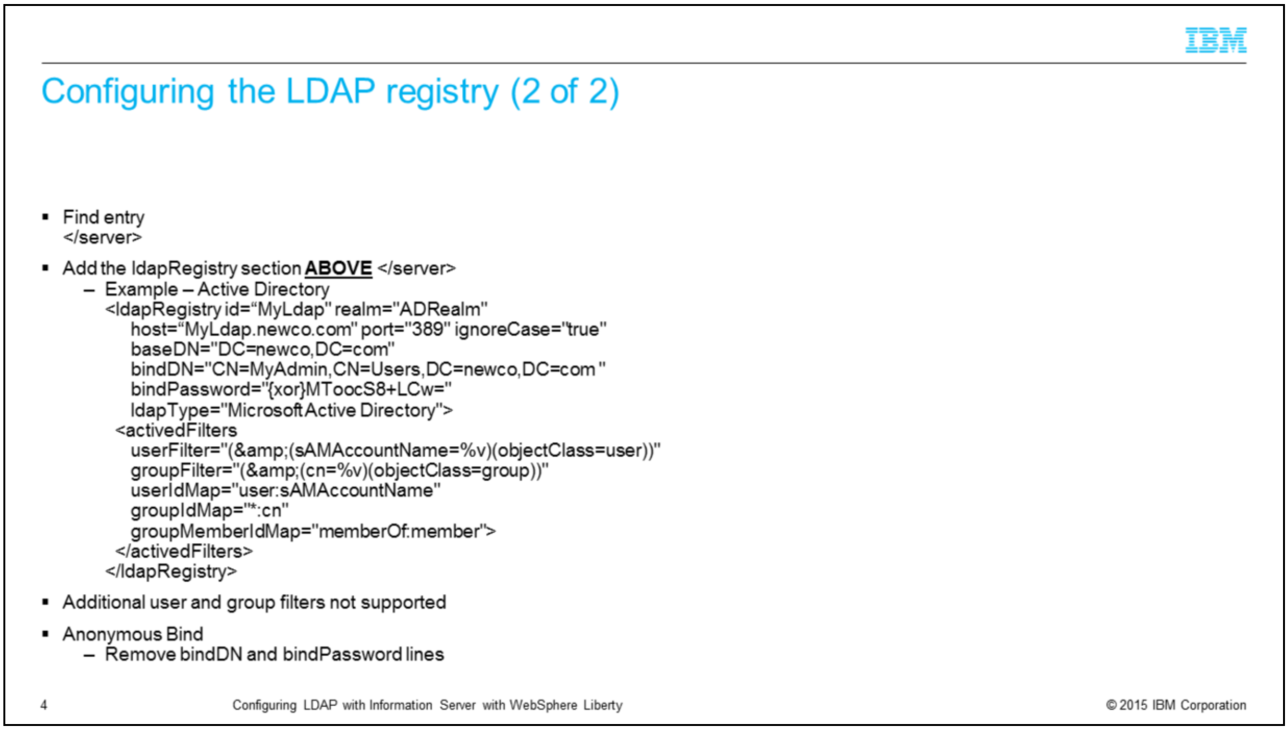
IBM

Configuring the LDAP registry (1 of 2)

- No administration GUI
  - Configure LDAP by editing server.xml
  - Located in InformationServer/wlp/usr/servers/iis
- Stop Liberty
  InformationServer/ASBServer/bin/MetadataServer.sh stop
- Make a backup copy
  - cd InformationServer/wlp/usr/servers/iis
  - cp server.xml server.xml.backup
- Edit server.xml
- Comment out IIS registry entry
  - Change
    <usr_iisRegistry dataSourceRef="DataSource_ASBDataSource"/>
  - To
    <!-- usr_iisRegistry dataSourceRef="DataSource_ASBDataSource"/ -->

Liberty is a lightweight version of WebSphere and does not have an administrative console. All LDAP configurations for Liberty must be done manually by editing the server.xml file. The server.xml file is in the profile directory for iis.

The first step in configuring LDAP is to stop the Liberty server. Next, change to the Liberty iis profile directory and make a backup copy of server.xml. Edit the server.xml file and locate the Information Server iisRegistry entry and comment it out using the syntax that is displayed on this slide.



Configuring the LDAP registry (2 of 2)

- Find entry
  </server>
- Add the ldapRegistry section **ABOVE** </server>
  - Example – Active Directory

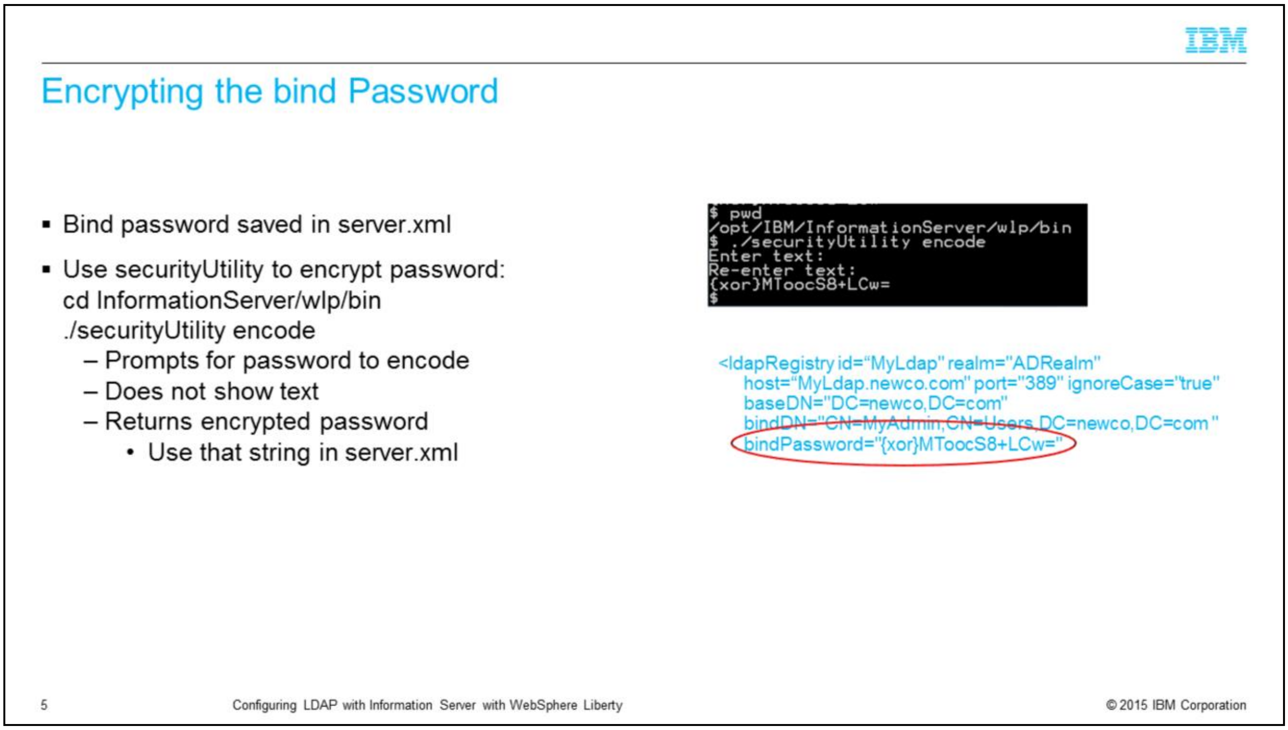
```
<ldapRegistry id="MyLdap" realm="ADRealm"
    host="MyLdap.newco.com" port="389" ignoreCase="true"
    baseDN="DC=newco,DC=com"
    bindDN="CN=MyAdmin,CN=Users,DC=newco,DC=com "
    bindPassword="{xor}MToocS8+LCw="
    ldapType="Microsoft Active Directory">
  <activedFilters
    userFilter="(&amp;(sAMAccountName=%v)(objectClass=user))"
    groupFilter="(&amp;(cn=%v)(objectClass=group))"
    userIdMap="user:sAMAccountName"
    groupIdMap="*:cn"
    groupMemberIdMap="memberOf:member">
  </activedFilters>
</ldapRegistry>
```

- Additional user and group filters not supported
- Anonymous Bind
  - Remove bindDN and bindPassword lines

4 Configuring LDAP with Information Server with WebSphere Liberty © 2015 IBM Corporation

Next, find the tag for the end of the server section. The ldapRegistry section needs to go ABOVE this tag. The example that is displayed on this slide is an example of an Active Directory server. Although there is a section for user and group filters, additional filters are not supported and are ignored if added to this section.

If the LDAP server uses anonymous bind, remove the bindDN and bindPassword lines.



IBM

Encrypting the bind Password

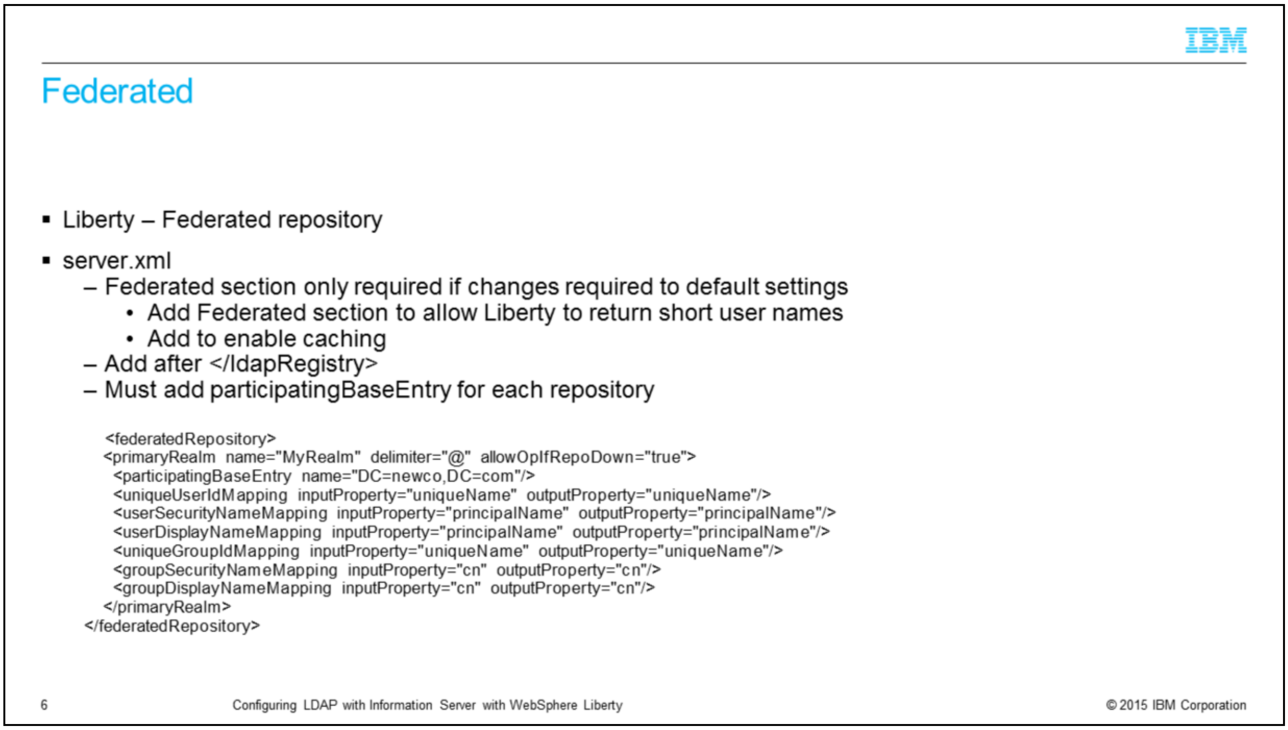
- Bind password saved in server.xml
- Use securityUtility to encrypt password:
  cd InformationServer/wlp/bin
  ./securityUtility encode
  - Prompts for password to encode
  - Does not show text
  - Returns encrypted password
    - Use that string in server.xml

```
$ pwd
/opt/IBM/InformationServer/wlp/bin
$ ./securityUtility encode
Enter text:
Re-enter text:
{xor}MToocS8+LCw=
$
```

```
<ldapRegistry id="MyLdap" realm="ADRealm"
    host="MyLdap.newco.com" port="389" ignoreCase="true"
    baseDN="DC=newco,DC=com"
    bindDN="CN=MyAdmin,CN=Users,DC=newco,DC=com "
    bindPassword="{xor}MToocS8+LCw="
```

5 Configuring LDAP with Information Server with WebSphere Liberty © 2015 IBM Corporation

Since the server.xml file is a plain text file, most users do not want the password for the bindDN displayed in the file. Liberty provides a command that is called securityUtility that allows you to encrypt the password. The command is in the wlp/bin directory. Run securityUtility encode. The command prompts for the text to be encoded. It does not show the text as it is typed for security reasons. The command has the user re-enter the text to be sure that it was typed correctly. The command then displays the encoded password that can be used in the server.xml file as shown in the example that is displayed on this slide.



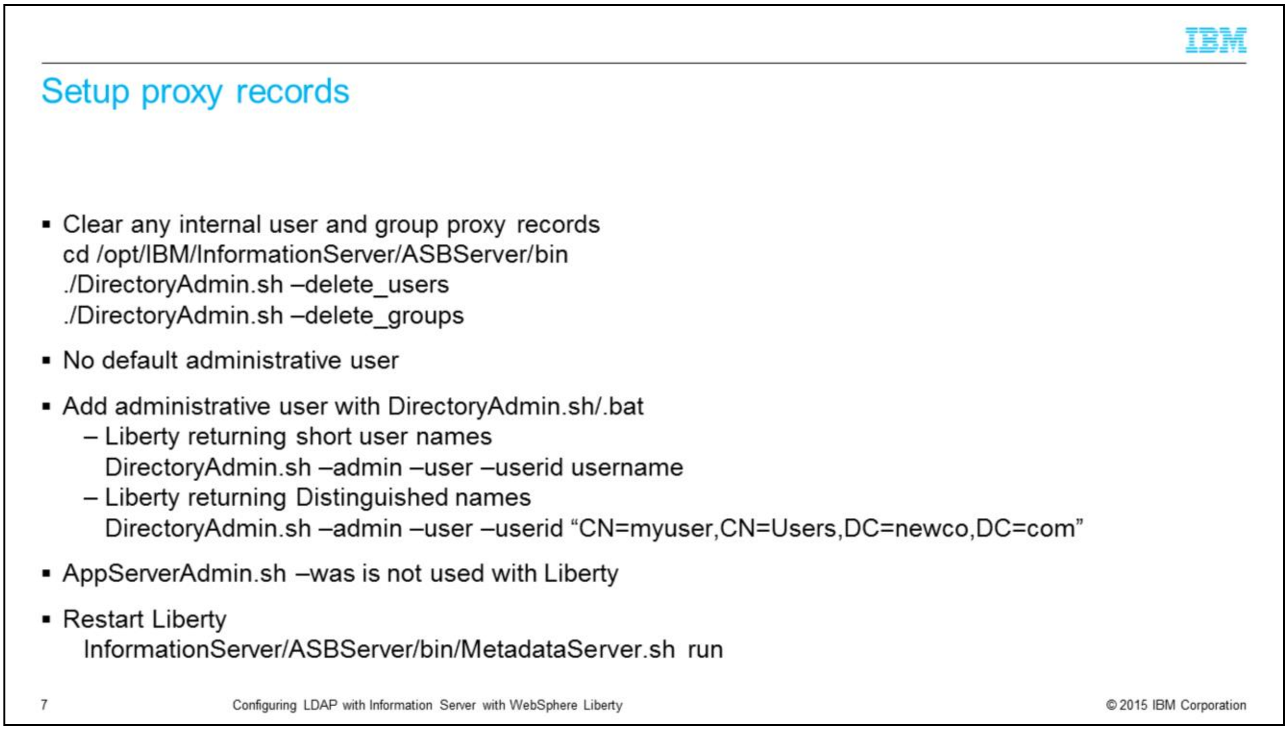
Federated

- Liberty – Federated repository
- server.xml
  - Federated section only required if changes required to default settings
    - Add Federated section to allow Liberty to return short user names
    - Add to enable caching
  - Add after </ldapRegistry>
  - Must add participatingBaseEntry for each repository

```
  <federatedRepository>
  <primaryRealm name="MyRealm" delimiter="@" allowOpIfRepoDown="true">
   <participatingBaseEntry name="DC=newco,DC=com"/>
   <uniqueUserIdMapping inputProperty="uniqueName" outputProperty="uniqueName"/>
   <userSecurityNameMapping inputProperty="principalName" outputProperty="principalName"/>
   <userDisplayNameMapping inputProperty="principalName" outputProperty="principalName"/>
   <uniqueGroupIdMapping inputProperty="uniqueName" outputProperty="uniqueName"/>
   <groupSecurityNameMapping inputProperty="cn" outputProperty="cn"/>
   <groupDisplayNameMapping inputProperty="cn" outputProperty="cn"/>
  </primaryRealm>
</federatedRepository>
```

6 Configuring LDAP with Information Server with WebSphere Liberty © 2015 IBM Corporation

Liberty uses Federated repositories only. The federatedRepository section is only required if you need to change settings to something other than the defaults. For example, if the federatedRepository section is not included, Liberty returns the user and group distinguished name to the Information Server web console the same way standalone LDAP returns the IDs with WebSphere ND. If you prefer to have the short names returned for the users and groups, add the federatedRepository section to the server.xml file as displayed on this slide. When adding the federatedRepository section, it must be added after the end of the ldapRegistry section. The entry for participatingBaseEntry must be added for each repository that is specified in server.xml.



Setup proxy records

- Clear any internal user and group proxy records
  cd /opt/IBM/InformationServer/ASBServer/bin
  ./DirectoryAdmin.sh –delete_users
  ./DirectoryAdmin.sh –delete_groups
- No default administrative user
- Add administrative user with DirectoryAdmin.sh/.bat
  - Liberty returning short user names
    DirectoryAdmin.sh –admin –user –userid username
  - Liberty returning Distinguished names
    DirectoryAdmin.sh –admin –user –userid “CN=myuser,CN=Users,DC=newco,DC=com”
- AppServerAdmin.sh –was is not used with Liberty
- Restart Liberty
  InformationServer/ASBServer/bin/MetadataServer.sh run

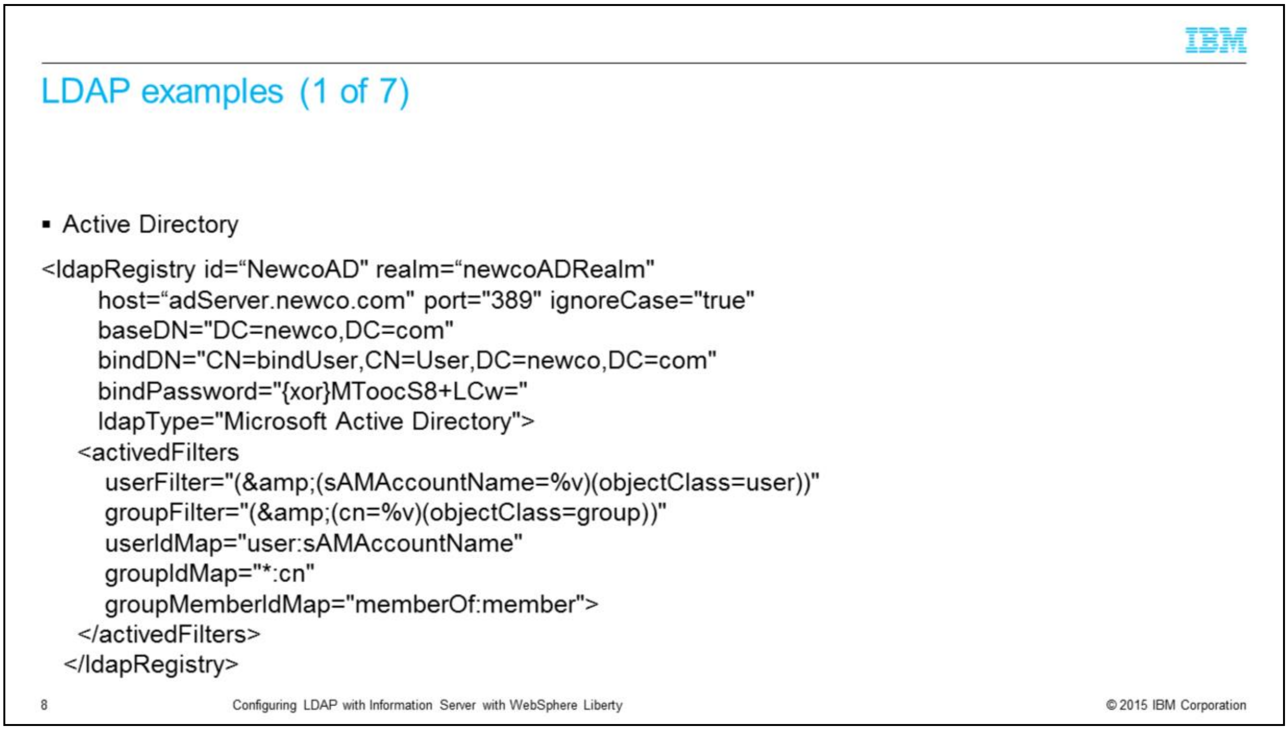
7 Configuring LDAP with Information Server with WebSphere Liberty © 2015 IBM Corporation

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

Liberty does not have a specified WebSphere administrative user the way Network Deployment, referred to as ND, does so there is no default administrative user when switching to LDAP. An Information Server administrative user needs to be added using the DirectoryAdmin command as displayed on this slide. The user ID specified in the command must match the format of the user ID that Liberty returns. For example, if the federatedRepository section is not specified, Liberty returns the user’s distinguished name, therefore, the user’s distinguished name must be specified in the DirectoryAdmin command.

The AppServerAdmin –was command is not used with Liberty since there is no WebSphere Application Server administrative user.

Once the setup is complete, restart Liberty.



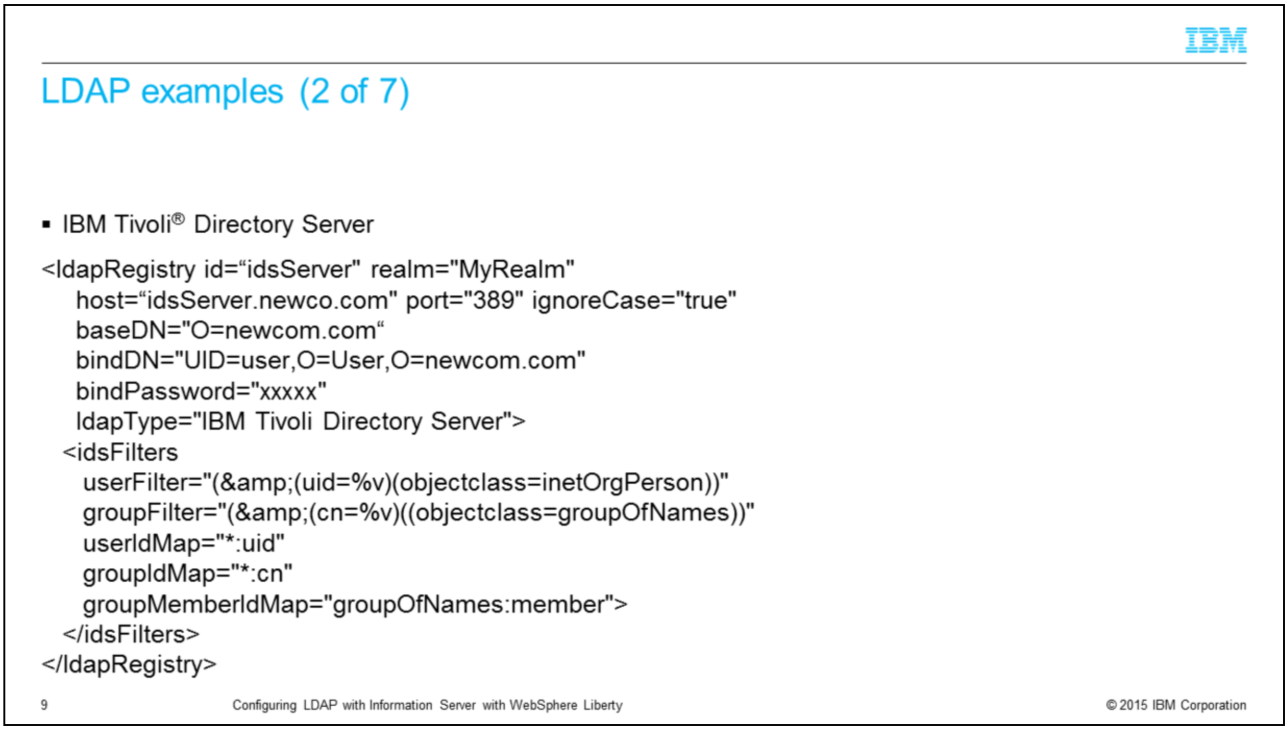
LDAP examples (1 of 7)

- Active Directory

```
<ldapRegistry id=“NewcoAD" realm=“newcoADRealm"
      host=“adServer.newco.com" port="389" ignoreCase="true"
      baseDN="DC=newco,DC=com"
      bindDN="CN=bindUser,CN=User,DC=newco,DC=com"
      bindPassword="{xor}MToocS8+LCw="
      ldapType="Microsoft Active Directory">
   <activedFilters
      userFilter="(&amp;(sAMAccountName=%v)(objectClass=user))"
      groupFilter="(&amp;(cn=%v)(objectClass=group))"
      userIdMap="user:sAMAccountName"
      groupIdMap="*:cn"
      groupMemberIdMap="memberOf:member">
   </activedFilters>
  </ldapRegistry>
```

8 Configuring LDAP with Information Server with WebSphere Liberty © 2015 IBM Corporation

The next seven slides have examples of ldapRegistry entries for different LDAP types. It is important to understand that these examples use the default filters and maps for each type of LDAP server. It is possible for the same type of LDAP to have different filters. The only way to tell is to use an LDAP browser and look at the user and group attributes on the LDAP server you are trying to connect to. This slide displays the entry for Active Directory.

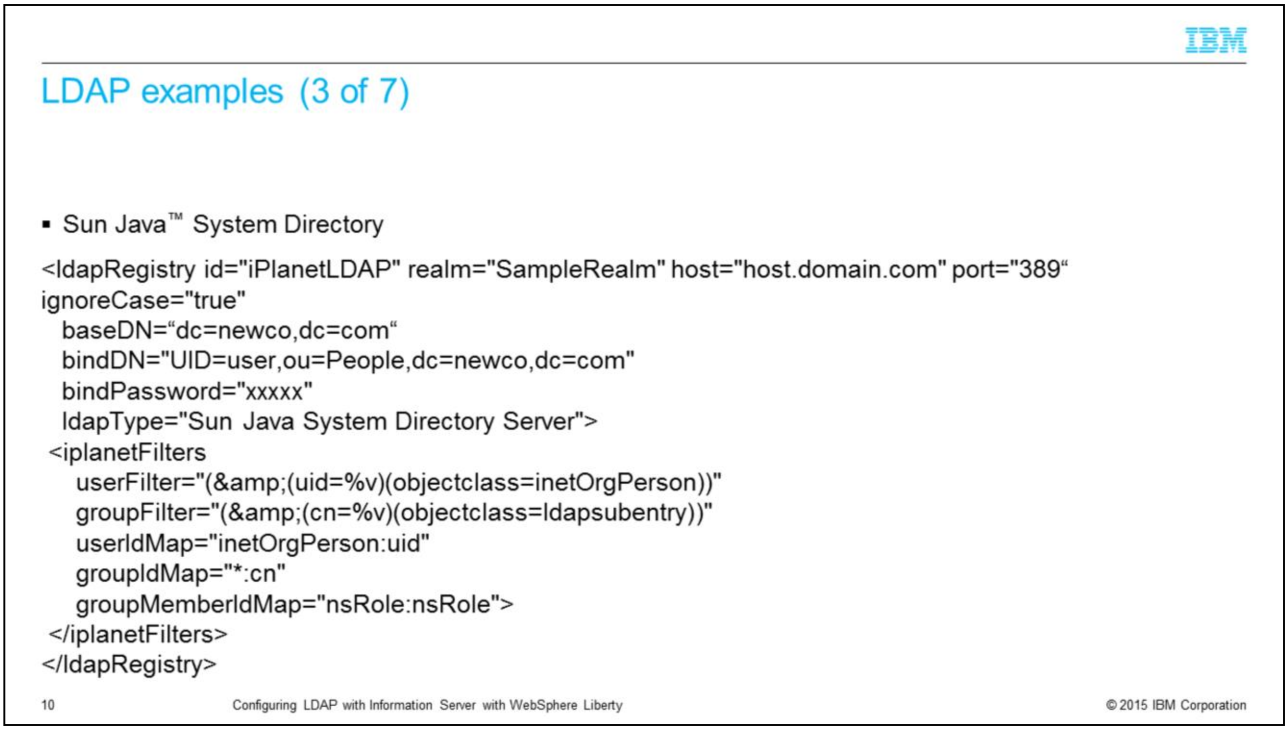


LDAP examples (2 of 7)

- IBM Tivoli® Directory Server

```
<ldapRegistry id=“idsServer" realm="MyRealm"
    host=“idsServer.newco.com" port="389" ignoreCase="true"
    baseDN="O=newcom.com“
    bindDN="UID=user,O=User,O=newcom.com"
    bindPassword="xxxxx"
    ldapType="IBM Tivoli Directory Server">
  <idsFilters
     userFilter="(&amp;(uid=%v)(objectclass=inetOrgPerson))"
     groupFilter="(&amp;(cn=%v)((objectclass=groupOfNames))"
     userIdMap="*:uid"
     groupIdMap="*:cn"
     groupMemberIdMap="groupOfNames:member">
  </idsFilters>
</ldapRegistry>
```

This slide displays an ldapRegistry entry for IBM Tivoli Directory Server.



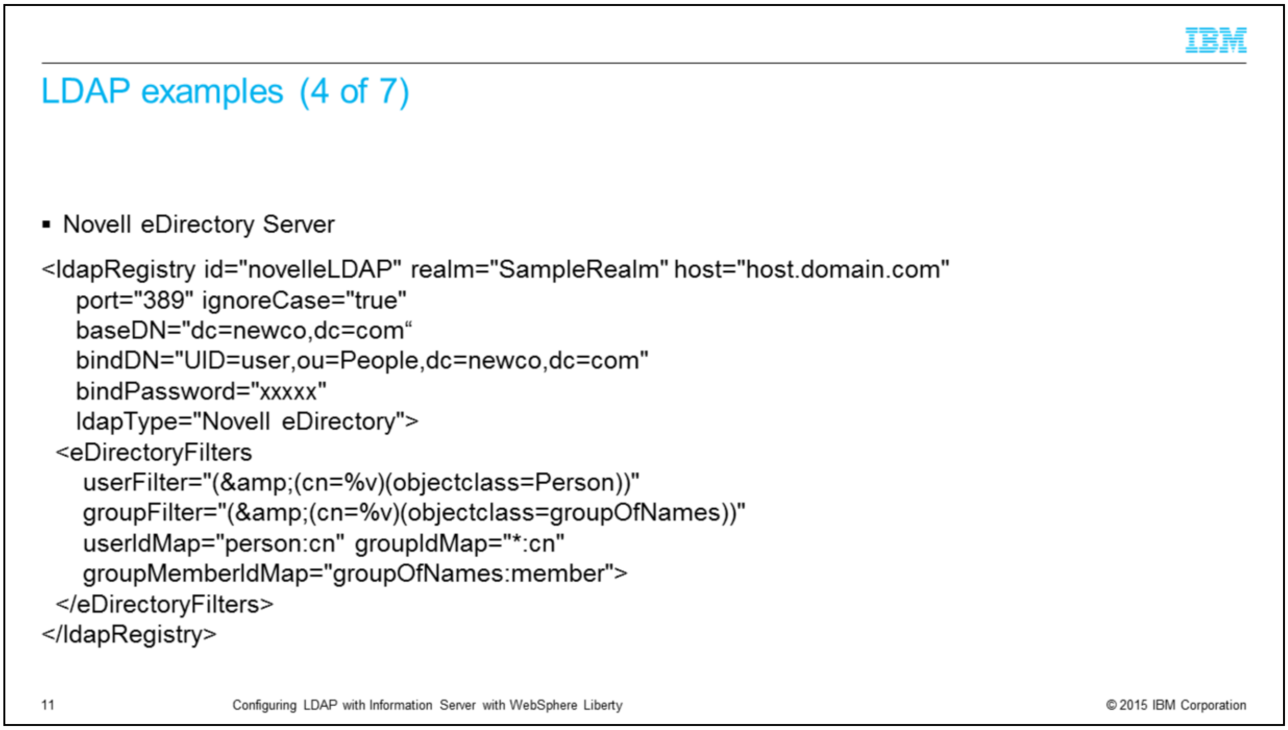
LDAP examples (3 of 7)

- Sun Java™ System Directory

```
<ldapRegistry id="iPlanetLDAP" realm="SampleRealm" host="host.domain.com" port="389“
ignoreCase="true"
  baseDN=“dc=newco,dc=com“
  bindDN="UID=user,ou=People,dc=newco,dc=com"
  bindPassword="xxxxx"
  ldapType="Sun Java System Directory Server">
 <iplanetFilters
    userFilter="(&amp;(uid=%v)(objectclass=inetOrgPerson))"
    groupFilter="(&amp;(cn=%v)(objectclass=ldapsubentry))"
    userIdMap="inetOrgPerson:uid"
    groupIdMap="*:cn"
    groupMemberIdMap="nsRole:nsRole">
 </iplanetFilters>
</ldapRegistry>
```

10 Configuring LDAP with Information Server with WebSphere Liberty © 2015 IBM Corporation

This slide displays the ldapRegistry entry for Sun Java System Directory.

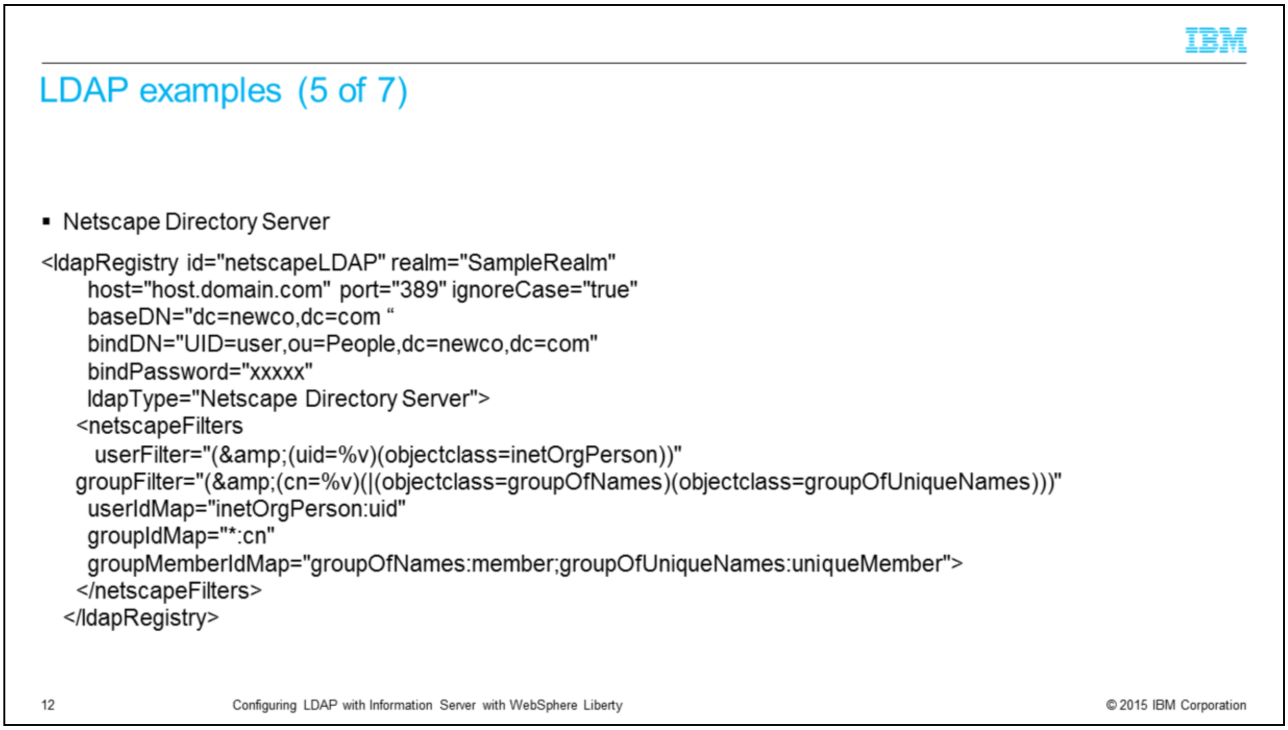


LDAP examples (4 of 7)

- Novell eDirectory Server

```
<ldapRegistry id="novelleLDAP" realm="SampleRealm" host="host.domain.com"
    port="389" ignoreCase="true"
    baseDN="dc=newco,dc=com“
    bindDN="UID=user,ou=People,dc=newco,dc=com"
    bindPassword="xxxxx"
    ldapType="Novell eDirectory">
  <eDirectoryFilters
     userFilter="(&amp;(cn=%v)(objectclass=Person))"
     groupFilter="(&amp;(cn=%v)(objectclass=groupOfNames))"
     userIdMap="person:cn" groupIdMap="*:cn"
     groupMemberIdMap="groupOfNames:member">
  </eDirectoryFilters>
</ldapRegistry>
```

This slide displays the ldapRegistry entry for Novell eDirectory Server.



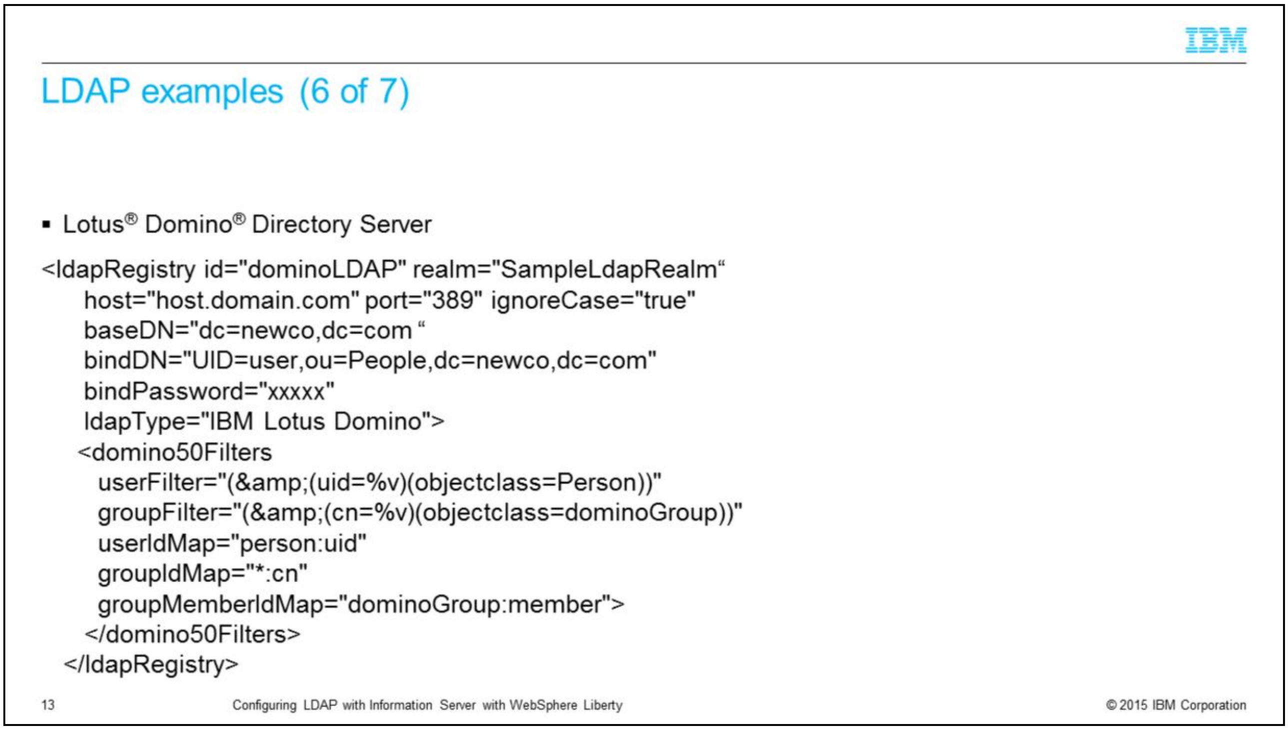
LDAP examples (5 of 7)

- Netscape Directory Server

```
<ldapRegistry id="netscapeLDAP" realm="SampleRealm"
       host="host.domain.com" port="389" ignoreCase="true"
       baseDN="dc=newco,dc=com “
       bindDN="UID=user,ou=People,dc=newco,dc=com"
       bindPassword="xxxxx"
       ldapType="Netscape Directory Server">
     <netscapeFilters
        userFilter="(&amp;(uid=%v)(objectclass=inetOrgPerson))"
     groupFilter="(&amp;(cn=%v)(|(objectclass=groupOfNames)(objectclass=groupOfUniqueNames)))"
       userIdMap="inetOrgPerson:uid"
       groupIdMap="*:cn"
       groupMemberIdMap="groupOfNames:member;groupOfUniqueNames:uniqueMember">
     </netscapeFilters>
   </ldapRegistry>
```

12 Configuring LDAP with Information Server with WebSphere Liberty © 2015 IBM Corporation

This slide displays the ldapRegistry entry for Netscape Directory Server.

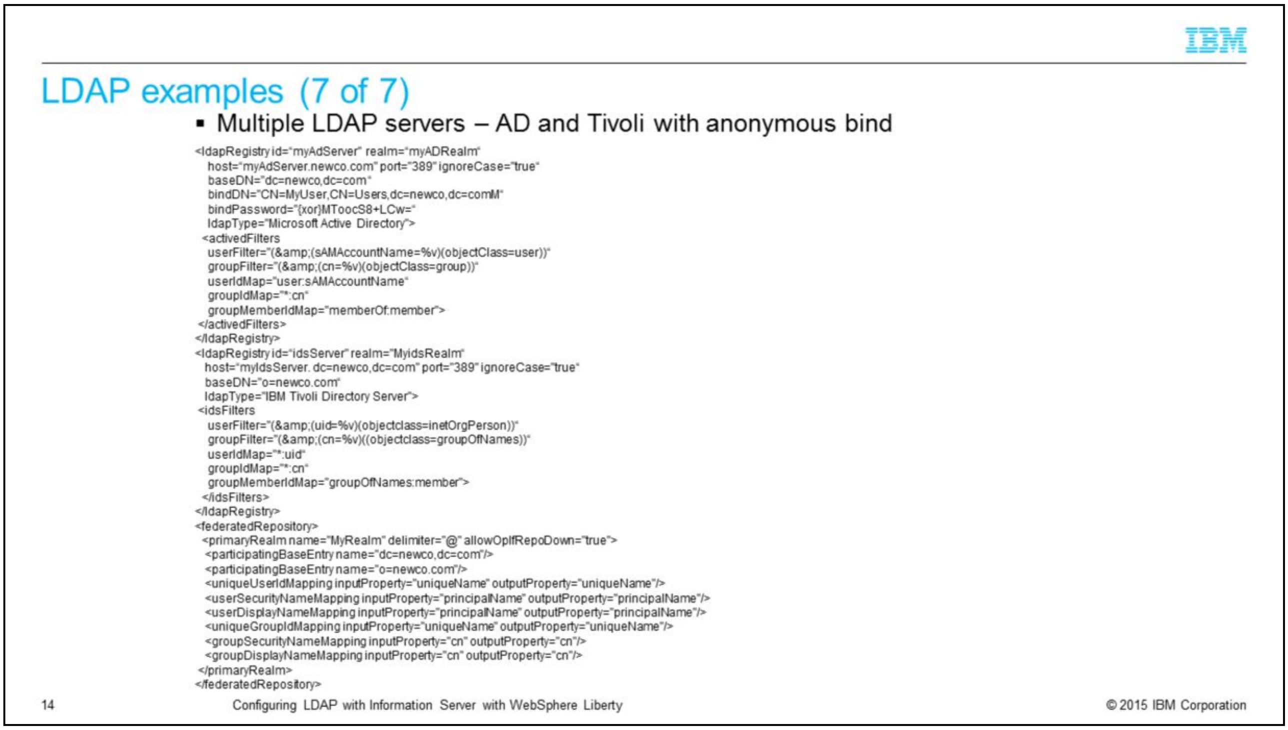


LDAP examples (6 of 7)

- Lotus® Domino® Directory Server

```
<ldapRegistry id="dominoLDAP" realm="SampleLdapRealm“
     host="host.domain.com" port="389" ignoreCase="true"
     baseDN="dc=newco,dc=com “
     bindDN="UID=user,ou=People,dc=newco,dc=com"
     bindPassword="xxxxx"
     ldapType="IBM Lotus Domino">
    <domino50Filters
       userFilter="(&amp;(uid=%v)(objectclass=Person))"
       groupFilter="(&amp;(cn=%v)(objectclass=dominoGroup))"
       userIdMap="person:uid"
       groupIdMap="*:cn"
       groupMemberIdMap="dominoGroup:member">
     </domino50Filters>
  </ldapRegistry>
```

This slide displays the ldapRegistry entry for Lotus Domino Directory Server.

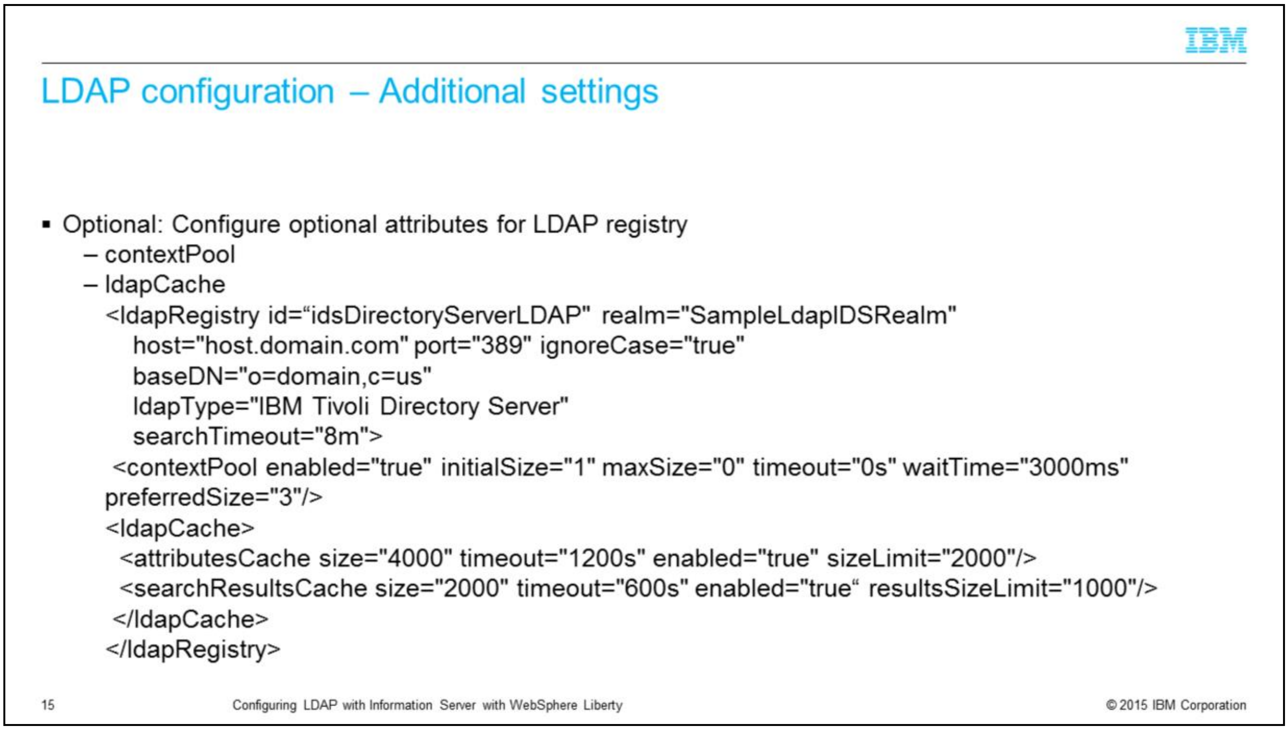


LDAP examples (7 of 7)

- Multiple LDAP servers – AD and Tivoli with anonymous bind

```
<ldapRegistry id="myAdServer" realm="myADRealm"
   host="myAdServer.newco.com" port="389" ignoreCase="true"
   baseDN="dc=newco,dc=com"
   bindDN="CN=MyUser,CN=Users,dc=newco,dc=comM"
   bindPassword="{xor}MToocS8+LCw="
   ldapType="Microsoft Active Directory">
  <activedFilters
   userFilter="(&amp;(sAMAccountName=%v)(objectClass=user))"
   groupFilter="(&amp;(cn=%v)(objectClass=group))"
   userIdMap="user:sAMAccountName"
   groupIdMap="*:cn"
   groupMemberIdMap="memberOf:member">
 </activedFilters>
</ldapRegistry>
<ldapRegistry id="idsServer" realm="MyidsRealm"
  host="myIdsServer. dc=newco,dc=com" port="389" ignoreCase="true"
  baseDN="o=newco.com"
  ldapType="IBM Tivoli Directory Server">
 <idsFilters
   userFilter="(&amp;(uid=%v)(objectclass=inetOrgPerson))"
   groupFilter="(&amp;(cn=%v)((objectclass=groupOfNames))"
   userIdMap="*:uid"
   groupIdMap="*:cn"
   groupMemberIdMap="groupOfNames:member">
  </idsFilters>
</ldapRegistry>
<federatedRepository>
  <primaryRealm name="MyRealm" delimiter="@" allowOpIfRepoDown="true">
   <participatingBaseEntry name="dc=newco,dc=com"/>
   <participatingBaseEntry name="o=newco.com"/>
   <uniqueUserIdMapping inputProperty="uniqueName" outputProperty="uniqueName"/>
   <userSecurityNameMapping inputProperty="principalName" outputProperty="principalName"/>
   <userDisplayNameMapping inputProperty="principalName" outputProperty="principalName"/>
   <uniqueGroupIdMapping inputProperty="uniqueName" outputProperty="uniqueName"/>
   <groupSecurityNameMapping inputProperty="cn" outputProperty="cn"/>
   <groupDisplayNameMapping inputProperty="cn" outputProperty="cn"/>
 </primaryRealm>
</federatedRepository>
```

This slide displays an example of the server.xml entries when using multiple LDAP servers for authentication and the federatedRepository section.



LDAP configuration – Additional settings

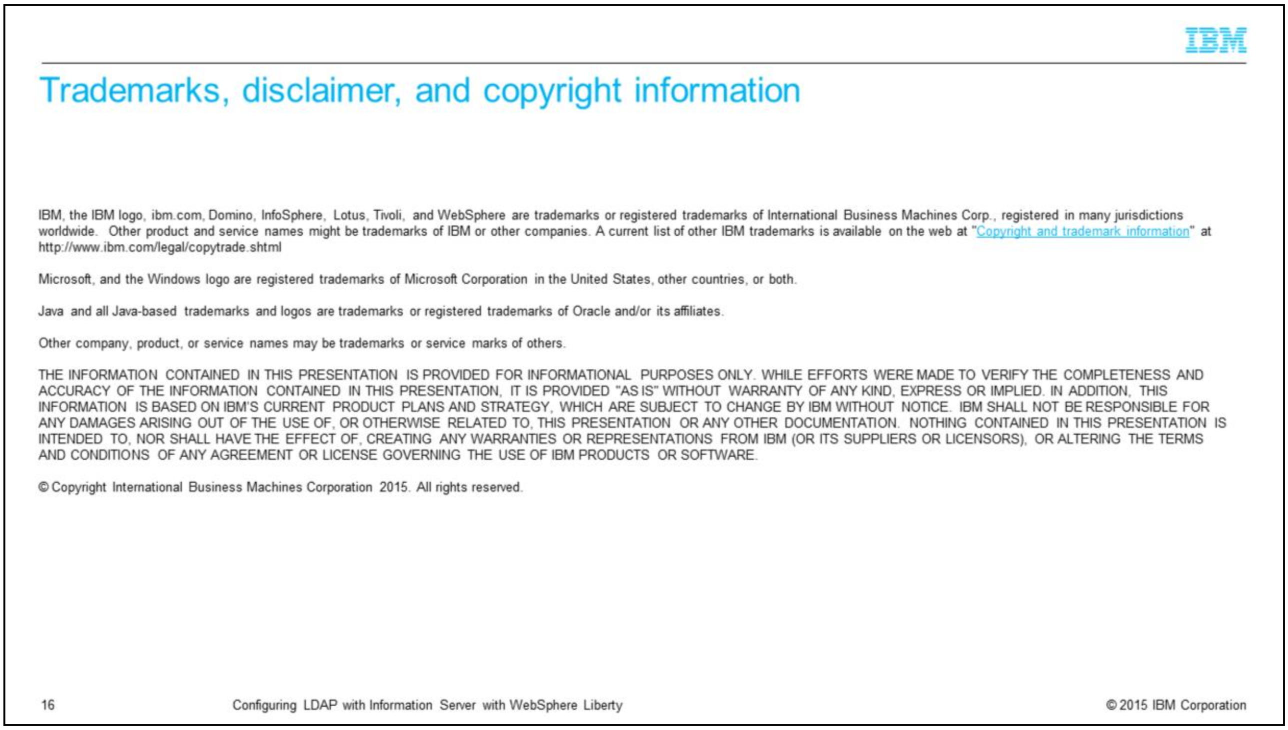
- Optional: Configure optional attributes for LDAP registry
  - contextPool
  - ldapCache

```
<ldapRegistry id=“idsDirectoryServerLDAP" realm="SampleLdapIDSRealm"
   host="host.domain.com" port="389" ignoreCase="true"
   baseDN="o=domain,c=us"
   ldapType="IBM Tivoli Directory Server"
   searchTimeout="8m">
 <contextPool enabled="true" initialSize="1" maxSize="0" timeout="0s" waitTime="3000ms"
preferredSize="3"/>
<ldapCache>
  <attributesCache size="4000" timeout="1200s" enabled="true" sizeLimit="2000"/>
  <searchResultsCache size="2000" timeout="600s" enabled="true“ resultsSizeLimit="1000"/>
 </ldapCache>
</ldapRegistry>
```

15 Configuring LDAP with Information Server with WebSphere Liberty © 2015 IBM Corporation

You can configure other optional attributes for the LDAP registry, such as contextPool or ldapCache, as given in the example displayed on this slide. Federated user registry uses the context pooling mechanism to improve the performance of concurrent access to an LDAP server. Context pooling works at a higher level than the connection pooling. Each context entry in the context pool corresponds to a socket connection to the LDAP server. The bind credentials that are used by this pool are specified when configuring the LDAP registry.

Federated repository uses the cache mechanism for performance enhancement. It caches information about the LDAP users and groups based on the user operations performed. For example, if you perform a search operation on the LDAP users and groups, the result of the operation is cached. You can enable the ldapCache element in the server.xml file as displayed on this slide.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, Domino, InfoSphere, Lotus, Tivoli, 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

Microsoft, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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.