

IBM Tivoli Software



## IBM Tivoli Directory Server 6.0 - Replication

Excerpt taken from presentation given on April 24, 2007  
Implementing a replication topology: Configuring Replication

**Support Technical Exchange Web site**  
[http://www-306.ibm.com/software/sysmgmt/products/support/supp\\_tech\\_exch.html](http://www-306.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html)

8/15/2007

© 2007 IBM Corporation

## We are now ready to configure replication

**Lets take stock of where we are.**

- **At this time we have 1 authoritative master running (peer1) and two clean and synchronized systems ready to become a peer (peer2) and a replica (replica1)**
- **The user data is loaded on peer1 and we have cleaned up any unneeded replication agreements**
- **All three servers should be started at this time using the commands from slide 18**



## The best tool for replication ... as simple as ldapsearch

**When trying to determine your topology it is always a good idea to start by running the following search:**

```
#ldapsearch -h hostname -D cn=root -w ***** -s sub  
objectclass=ibm-repl*
```

**This will show us any configured replication agreement currently on the system. At this time this entry should return blank from:**

**peer1, peer2 and replica1**



## Configuring replication from the web admin tool

- **Login to the webadmin as cn=root on Peer1 (Authoritative Master)**
- **Replication Management**
  - Manage Topology
    - Add Subtree

The screenshot shows the web administration interface. On the left is a navigation tree with the following items: User properties, Server administration, Proxy administration, Schema management, Directory management, and Replication management (highlighted with a '1'). Under 'Replication management', there are sub-items: Manage credentials, Manage topology (highlighted with a '2'), Manage replication properties, Manage schedules, and Manage queues.

The main content area is titled 'Manage topology'. It contains a blue note: 'Note: Replication requires all servers in the topolog:'. Below the note is a section titled 'Replicated subtrees'. At the top of this section is a button 'Add subtree...' with a '3' next to it. Below the button is a form with a dropdown menu labeled '--- Select Action ---' and a 'Go' button. Below the form is a table with two columns: 'Select' and 'Subtree'. The table is currently empty. Below the table is the text 'Topology for selected subtree'.



## Next, we have to select our tree

There are two options in this case:

1. We can manually type in our subtree
2. We can browse and select our subtree

In this example we are going to click on Browse...

**Add replicated subtree**

Subtree DN  
\*

Master server referral LDAP URL

## Select the subtree you want to replicate

You will notice the selection screen is very similar to the Directory Management section of webadmin

**Browse entries**

Current location  
ldap://peer1:389

2

--- Select Action ---

Select	Expand	RDN	Object class
<input type="radio"/>	<input type="button" value="Expand"/>	cn=configuration	ibm-slapiTop
<input type="radio"/>	<input type="button" value="Expand"/>	cn=ibmpolicies	container
<input type="radio"/>	<input type="button" value="Expand"/>	cn=localhost	container
<input checked="" type="radio"/>	<input type="button" value="Expand"/>	o=ibm,c=us	organization

Page 1 of 1 Total: 4 Filtered: 4 Displayed: 4



## Checking our subtree

- We have selected our subtree, and the last thing we need to check is to make sure we are not using another system for our “Master Server Referral LDAP URL”!!!

Click **OK**

### Add replicated subtree

Subtree DN

\*o=ibm,c=us

Browse...

Master server referral LDAP URL

ldap://peer1:389

OK

Cancel

## This is what the basic topology will look like

**Directory Server Web Administration Tool**

peer1:389

**Manage topology**

Note: Replication requires all servers in the topology to be configured properly.

Replicated subtrees

Show topology   Add subtree...   Quiesce / Unquiesce

Select Action --- Go

Select	Subtree	Role	Status
<input type="radio"/>	O=IBM,C=US	Master	Normal

Topology for selected subtree : O=IBM,C=US

- Replication topology
  - peer1:389 1
    - Add master... 2
    - Add replica...
    - Manage gateway servers...
    - Edit agreement...
    - View schedule...
    - View server...
    - View errors...
    - Move...
    - Delete

Close



## So, what is actually taking place under the covers?

- Everything that we just did via the webadmin adds specific entries to the directory itself. Lets start with the top level object `o=ibm,c=us`

```
# ldapsearch -D cn=root -w secret -s sub -b " "
objectclass=ibm-repl*
```

```
o=IBM,c=US
```

```
objectclass=top
```

```
objectclass=organization
```

```
objectclass=ibm-replicationcontext
```

```
o=IBM
```

```
ibm-replicareferralurl=ldap://peer1:389
```



## Defining the replica group

- **Once the top level entry is set, then we must create an object where all replication related data will be stored. This is called the replicaGroup and looks like:**

```
ibm-replicaGroup=default,o=ibm,c=us
```

```
ibm-replicagroup=default
```

```
objectclass=ibm-replicagroup
```

```
objectclass=top
```

## Next we have the definition of the master

- **This is a very important entry as it tells Peer1 that he is actually a master for this section of the tree and looks like:**

**cn=peer1:389,ibm-replicaGroup=default,o=ibm,c=us**

**objectclass=ibm-replicasubentry**

**objectclass=top**

**ibm-replicaserverid=peer1**

**ibm-replicationserverismaster=TRUE**

**cn=peer1:389**



## Add a Master screens...

peer1:389

Add master

Server

Subtree  
O=IBM,C=US

Additional

Hostname  
peer2

Port  
389

Enable SSL encryption

Server is a gateway

Peer master name (leave blank to use host name)

Server ID  
peer2 1

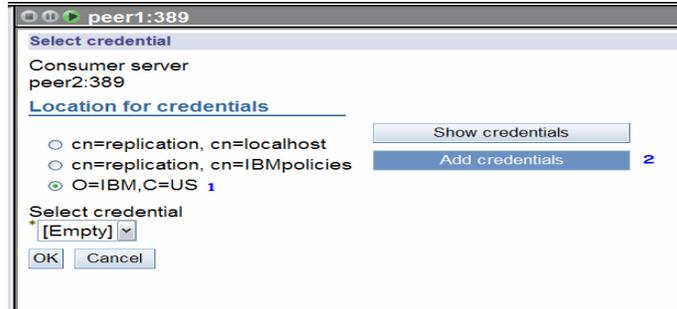
Description

Credential object

This field requires a value.  2

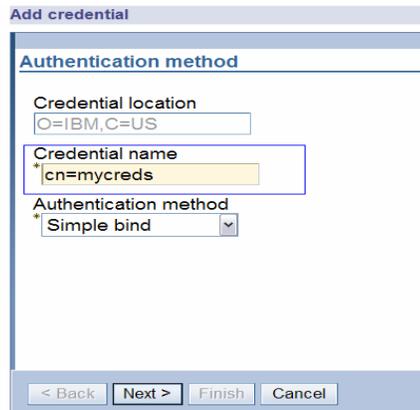
## Adding the credential object – OUTBOUND!

- **Ok, so in this panel what we are doing is setting our OUTBOUND credential. This will be the bind dn that is used when PEER1 tries to replicate to any other system.**



## Adding the credential – Naming your credential object

- In this first screen you can name the credential object anything you want:



**Add credential**

**Authentication method**

Credential location  
O=IBM,C=US

Credential name  
\*cn=mycreds

Authentication method  
\*Simple bind

< Back   Next >   Finish   Cancel

## Setting your bind credential.

- **The key to this dn is that it MUST NOT BE the cn=root dn. In fact, this dn should not match any real user on your system. In my case I will use cn=replbind**

Simple bind

Bind DN  
\* cn=replbind

Bind password  
\* .....

Confirm password  
\* .....

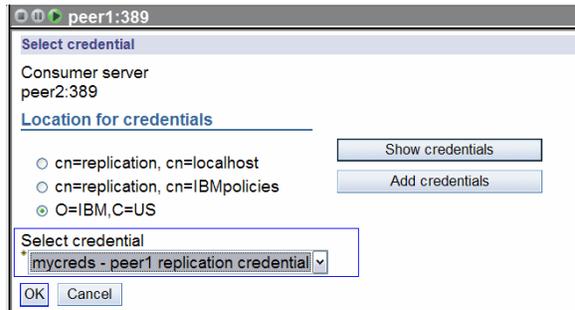
Description  
peer1 replication credential

< Back Next > Finish Cancel



## The view of our newly created cred

- We can now see the credential object we created stored under the o=ibm,c=us tree:



Click **OK**

## We are back in the Add Master screen

- We can now see the credential object we created as part of this agreement. Next we must click on the Additional tab:

peer1:389

Add master

Server

Additional

Subtree  
O=IBM,C=US

Hostname  
peer2

Port  
389

Enable SSL encryption

Server is a gateway

Peer master name (leave blank to use host name)

Server ID  
peer2

Get server ID

Description

Credential object  
cn=mycreds,ibm-replica

Select...

Edit...

OK Cancel



## The Additional Tab:

**Add master**

Server	Select replication schedule or enter DN (optional)
<b>Additional</b>	None <input type="text"/> <input type="button" value="Add..."/>
	Capabilities replicated to consumer
	<input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Refresh"/> --- Select Action --- <input type="button" value="Go"/>
	<b>Select Capabilities</b>
	<input checked="" type="checkbox"/> Filter ACLs
	<input checked="" type="checkbox"/> Password Policy
	<b>Consumer</b>
	<input checked="" type="checkbox"/> Add credential information on consumer
	Consumer admin DN
	<input type="text" value="cn=root"/>
	Consumer admin password
	<input type="password" value="•••••"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

## The Create additional supplier agreements screen

- **This screen is what builds the replication agreements between each system. This is a way for us to customize how we want to replicate, in this case I want both agreements:**

**Create additional supplier agreements** [Logfiles](#) [Help](#)

Agreements will be created for the following master servers to act as suppliers to this server. Uncheck any agreements that you do not want to be created.

Agreements

--- Select Action ---

Select	Supplier	Consumer
<input checked="" type="checkbox"/>	cn=peer2:389	cn=peer1:389
<input checked="" type="checkbox"/>	cn=peer1:389	cn=peer2:389



## Next it will ask you if you want to restart Peer2...

I will typically answer no to this question as:

1. It takes a while for the ibmslapd process to restart
2. I will be restarting peer2 anyway during the data sync later

**Admin demon port** [Logfiles Help](#)

Consumer server need to be restarted for supplier credential to take effect.  
Please enter admin demon port to restart the server.

Consumer

Admin demon port

Do you want to start/restart the consumer server?



## Next the ITDS server will fill in the gaps

- **At this stage the replication subsystems will collect topology information and then create the credential information that is still required for this topology to work.**

Click **OK**

[Logfiles](#) [Help](#)

**i** The manage topology function will now collect information for agreements that need to be created on addition of new peer master.

OK



## As part of 6.0 replication it will also...

- **The replication manager will create the credentials needed on Peer2 to replicate back to Peer1**

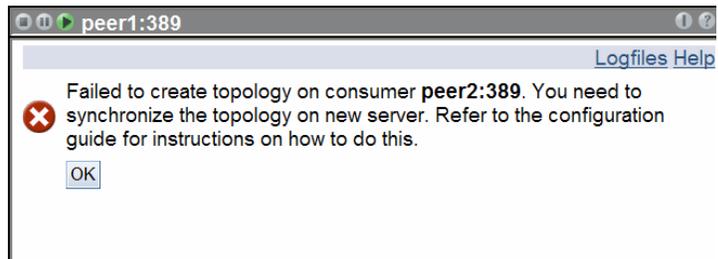
The screenshot shows a configuration window titled 'peer1:389'. It contains the following elements:

- Select credential:** A list with 'Supplier server peer2:389' and 'Consumer server peer1:389'. Two blue arrows point from the text to the 'peer2:389' and 'peer1:389' entries respectively.
- Location for credentials:** A section with two radio buttons: 'cn=replication, cn=IBMpolicies' (unselected) and 'O=IBM,C=US' (selected). To the right are 'Show credentials' and 'Add credentials' buttons.
- Select credential:** A dropdown menu showing 'mycreds - peer1 replication credential'.
- Consumer:** A section with a checked checkbox 'Add credential information on consumer'.
- Consumer admin DN:** A text field containing 'cn=root'.
- Consumer admin password:** A text field with masked characters '•••••'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

## Because I didn't restart both Peer1 and Peer2...

- **This is an error message you are going to get almost every time, ignore it (We will sync when we have all agreements built anyway).**

Click **OK**





## One more informational message...

- **Finally the replication management system will let us know our topology is complete:**

Click **OK**

[Logfiles Help](#)

**i** Server **peer2:389** has been added to the replication topology. However, data must be synchronized in order to fully initialize the new server. Refer to the configuration guide for instructions on how to do this.

OK



## Will ask us if we want to restart Peer1

- I usually skip this step due to the same reasons as before, BUT .. You have to pay attention here. If you do NOT restart your Master the credential object will not be in play and as such Peer2 will NOT be able to replicate to Peer1 ... we will discuss in detail later.

Click **NO**

[Logfiles](#) [Help](#)



Consumer server **peer1:389** need to be restarted for supplier credential to take effect.  
Do you want to restart the server?



## Lets look at what is actually added

- When we add the credential to the consumer for INBOUND replication the update is not made to the database, but is actually stored within the `ibmslapd.conf` file:

**dn: cn=Supplier1177533245327, cn=configuration**

**cn: Supplier1177533245327**

**ibm-slapdmasterdn: cn=replbind**

**ibm-slapdmasterpw: {AES256}URuLoPlzqApEBtS8gtOK0g==**

**ibm-slapdreplicasubtree: O=IBM, C=US**

**objectclass: ibm-slapdconfigentry**

**objectclass: ibm-slapdsupplier**

**objectclass: top**

## What a peer to peer topology looks like

- At this point we only have Peer1 and Peer2 in our peer to peer replication agreement, but this is what the topology looks like:

The screenshot shows the 'peer1:389' management window. It displays a 'Replicated subtrees' table with one entry: 'O=IBM,C=US' with a 'Master' role and 'Normal' status. Below the table, a tree view shows the 'Replication topology' for 'O=IBM,C=US', which includes a 'peer1:389' subtree and a 'peer2:389' subtree. A context menu is open over the 'peer1:389' subtree, listing actions such as 'Add master...', 'Add replica...', 'Manage gateway servers...', 'Edit agreement...', 'View schedule...', 'View server...', 'View errors...', 'Move...', and 'Delete'.

Select	Subtree	Role	Status
<input type="radio"/>	O=IBM,C=US	Master	Normal

Topology for selected subtree : O=IBM,C=US

- Replication topology
  - peer1:389
    - peer2:389
      - peer1:389

## So lets take another dive under the covers... ;-)

- Using the `ldapsearch` we spoke of in slide 28 we can review how each of these tasks we took show up in the directory.
- First lets look at the credential object.

`cn=mycreds,ibm-replicaGroup=default,O=IBM,C=US`

`replicacredentials=replbind (This is the Password!)`

`description=peer1 replication credential`

`objectclass=ibm-replicationcredentials`

`objectclass=ibm-replicationcredentialssimple`

`objectclass=top`

`replicabinddn=cn=replbind (This is the bind dn used)`

`cn=mycreds`



## The actual agreements.

- **There are two agreements that make up the replication between Peer1 and Peer2. It is important to understand how these agreements look, and the function of each**
- **The key: Write it down.**  
**Consumer, Supplier, Subtree**



## Peer1 to Peer2 agreement

**This is how the agreement will appear where Peer2 is acting as a consumer (replica) while Peer1 is acting as a supplier (master)**

```
cn=peer2:389,cn=peer1:389,ibm-replicaGroup=default,O=IBM,C=US
ibm-replicaconsumerid=peer2
ibm-replicationonhold=TRUE
ibm-replicacredentialsdn=cn=mycreds,ibm-
  replicaGroup=default,O=IBM,C=US
ibm-replicaurl=ldap://peer2:389
objectclass=ibm-replicationagreement
objectclass=top
cn=peer2:389
```



## And the Peer2 to Peer1 agreement...

- **Basically the same but in the correct order for this configuration:**  
**cn=peer1:389,cn=peer2:389,ibm-replicaGroup=default,O=IBM,C=US**  
**ibm-replicaconsumerid=peer1**  
**ibm-replicationonhold=TRUE**  
**ibm-replicacredentialsn=cn=mycreds,ibm-**  
**replicaGroup=default,O=IBM,C=US**  
**ibm-replicaurl=ldap://peer1:389**  
**objectclass=ibm-replicationagreement**  
**objectclass=top**  
**cn=peer1:389**

## Lather... rinse ... repeat

- **We use the same steps to add our other subtrees. In this configuration I want to have my schema and passwordPolicy attributes replicate so I add the cn=ibmpolicies subtree**

The screenshot shows the 'peer1:389' window in the administration console. The 'Manage topology' section is active, displaying a note: 'Note: Replication requires all servers in the topology to be configured properly.' Below this, the 'Replicated subtrees' section contains a table with two entries:

Select	Subtree	Role	Status
<input checked="" type="radio"/>	CN=IBMPOLICIES	Master	Normal
<input type="radio"/>	O=IBM,C=US	Master	Normal

Below the table, the 'Topology for selected subtree : CN=IBMPOLICIES' section shows a tree view with 'peer1:389' selected. To the right of the tree are three buttons: 'Add master...', 'Add replica...', and 'Manage gateway servers...'.



## Copyright and trademark information

© Copyright IBM Corporation 2000 - 2007. All rights reserved.

U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM web site pages may contain other proprietary notices and copyright information which should be observed.

IBM trademarks

<http://www.ibm.com/legal/copytrade.shtml#ibm>

**Fair use guidelines for use and reference of IBM trademarks**

<http://www.ibm.com/legal/copytrade.shtml#fairuse>

**General rules for proper reference to IBM product names**

<http://www.ibm.com/legal/copytrade.shtml#general>

**Special attributions**

IBM, the IBM logo and DB2 are trademarks of International Business Machines Corporation in the United States, other countries, or both.

MMX, Pentium, and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

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

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Other company, product or service names may be trademarks or service marks of others.