Fedora Directory Server
Sun Java System Directory Server
Essentials

F5ネットワークスジャパン株式会社
中満英生
nakamitsu@f5.com
nomo@bluecoara.net

最初に

- Fedora Directory Server → FDS
- Sun Java System Directory Server → IDS

- IDS = iPlanet Directory Server
- NDS = Netscape Directory Server
- RHDS = Red Hat Directory Server
- Sun Java System Directory Serverの正式略称
  - SDS = Solstice DiskSuite ?
  - JDS = Java Desktop System ?
  - SJDS = Sun Java Desktop System ?
  - SJSDS = Sun Java System Directory Server ?

パフォーマンス

ldapadd/ldapdeleteの速度を比較

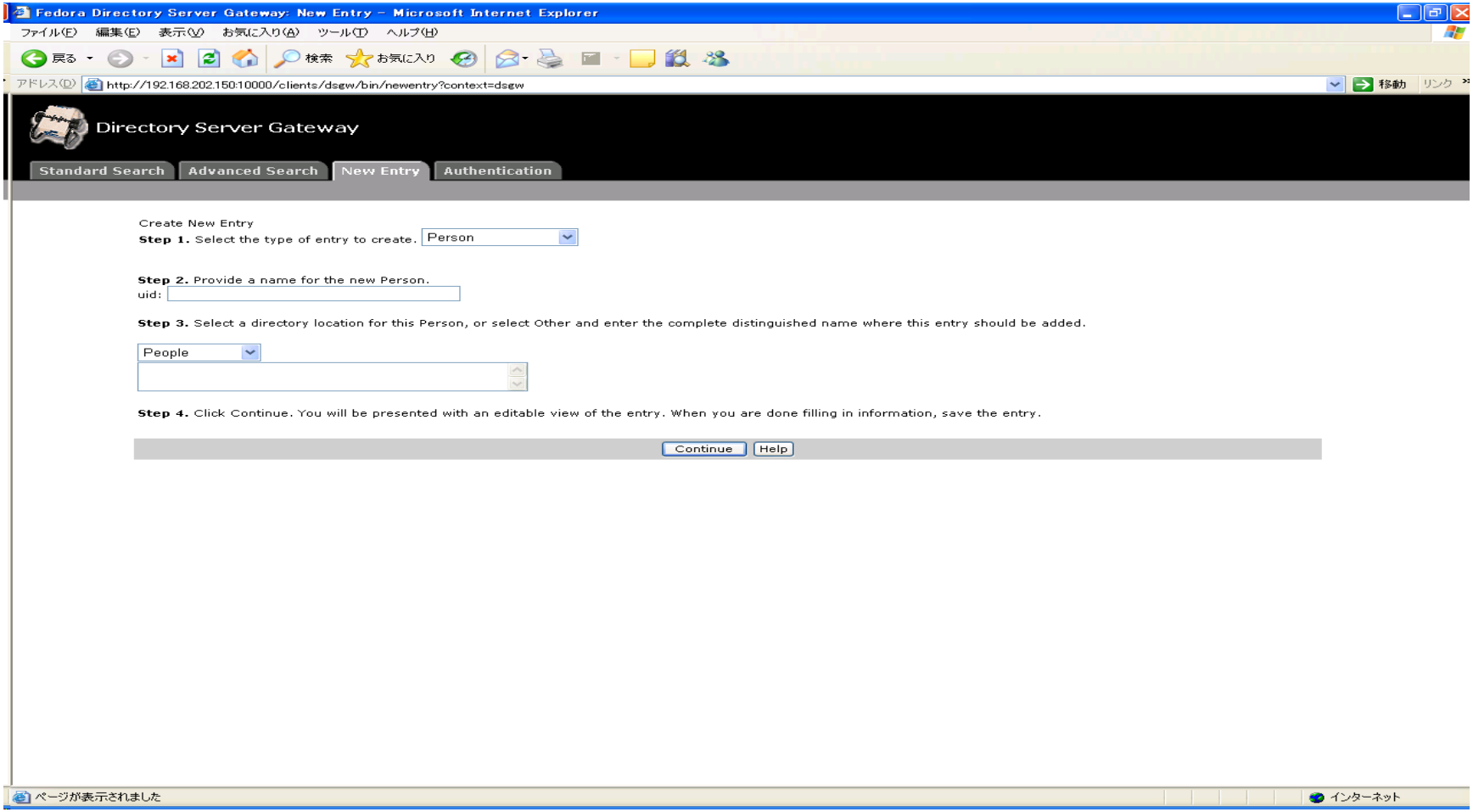
- FDSで10万件のデータを登録
  - 約10分
- FDSで10万件のデータを削除
  - 約12分
- OpenLDAPで10万件のデータを登録
  - 約50分
- OpenLDAPで10万件のデータを削除
  - 約50分

管理サーバ, コンソール

管理サーバ

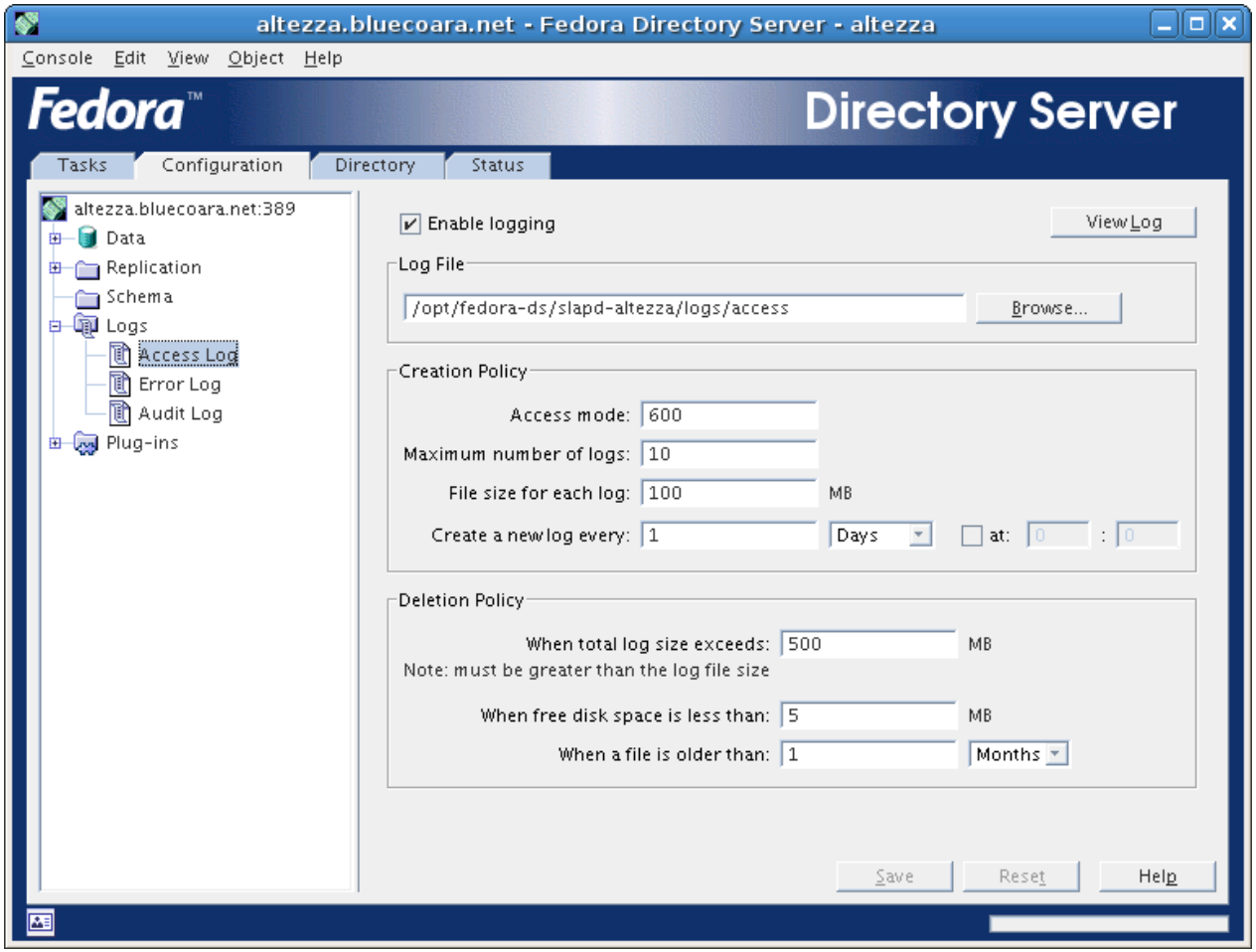
- LDAPサーバをGUIで管理
- サーバデーモンはTCPポートで動作
- 管理コンソール(startconsole)から接続
- ブラウザから接続可能 (例: http://x.x.x.x:10000/)
- ログインのためslapdを起動させておく必要あり
- FDS → /opt/fedora-ds/admin-serv
- IDS → /usr/iplanet/admserv5.1
- FDSでは，Apache-2.x(worker)を利用
- IDSでは，iPlanet WebServerを利用

ブラウザによる接続
http://x.x.x.x:10000/

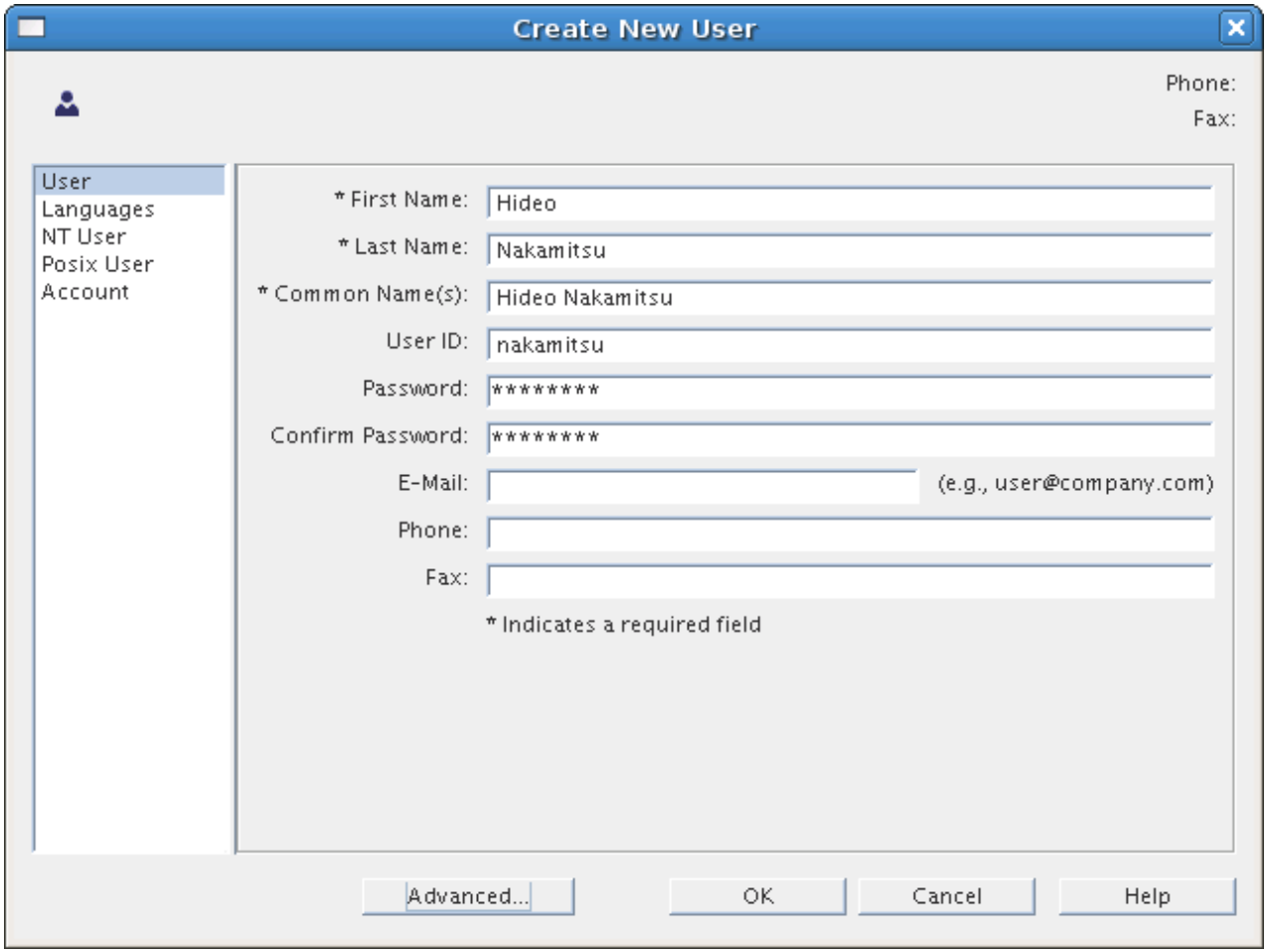


管理コンソール(1/3)
起動，停止，管理

管理コンソール(2/3)
ログ設定



管理コンソール(3/3)
エントリ追加



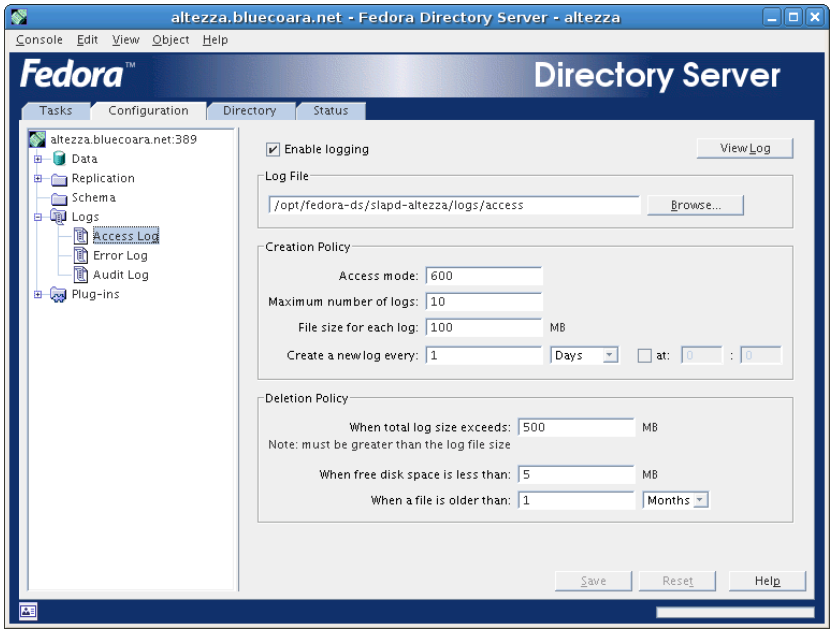
設定

設定ファイル

- 設定内容はLDAPツリー中に格納される
- 実体はdse.ldifというファイル
- ldapmodifyでディレクトリ中のパラメータを変更すれば，即時設定が反映される
- 最小限のダウンタイム！

設定変更例 オンライン(1)

- GUIより変更
- GUI上で操作を行うと，バックグラウンドでLDAPエントリが修正される



設定変更例 オンライン(2)

- ldapmodifyによる変更

changelog.ldif

```
dn: cn=config
replace: nsslapd-accesslog
nsslapd-accesslog: /opt/fedora-ds/slapd-host/logs/new_access
```

```
% ldapmodify -x -D "cn=Directory Manager" \
  -w abcd1234 -f changelog.ldif
```

設定変更例
オフライン(1)

- slapdプロセスを停止
- config/dse.ldifを編集
- slapdプロセスを起動

dse.ldifの種類

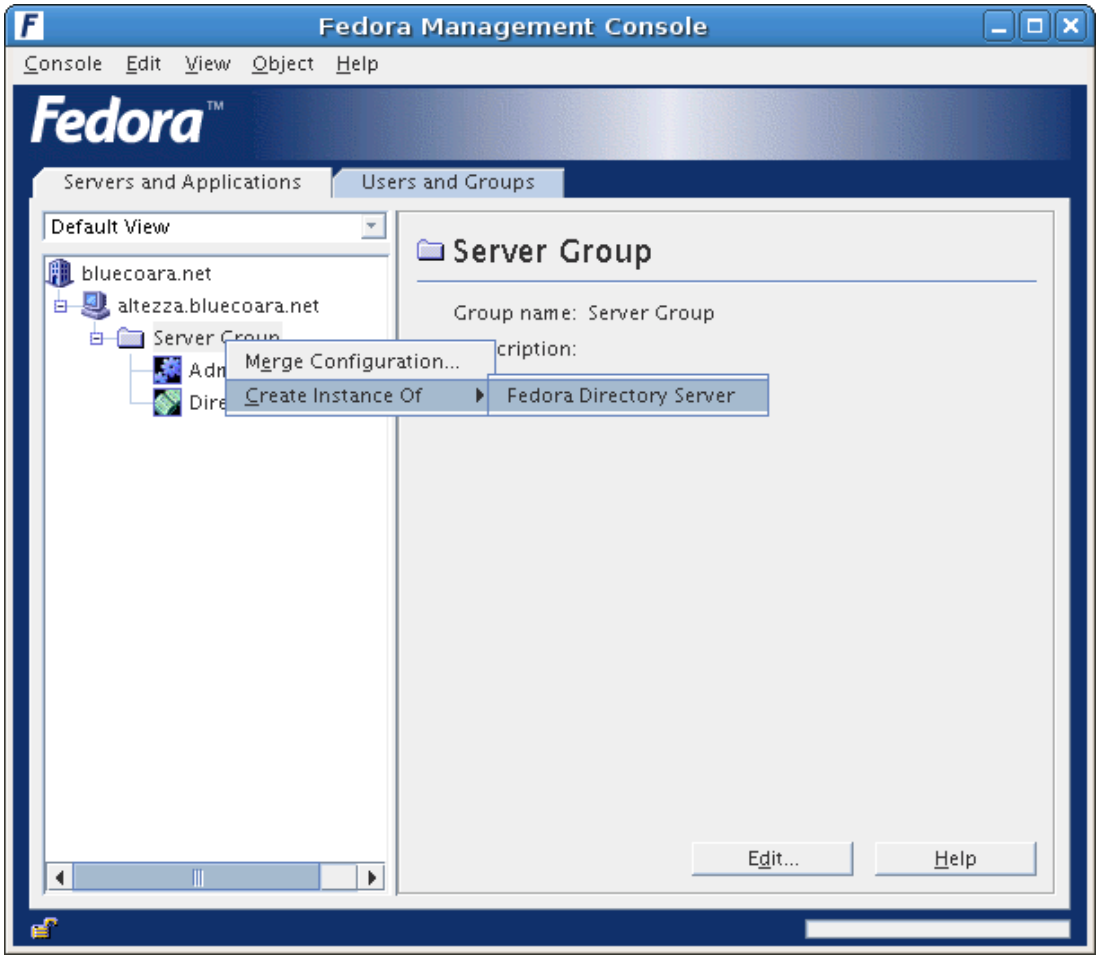
- dse.ldif
  - 実際の設定ファイル．ldapmodifyなど行うと即時ファイルが変更される
- dse.ldif.bak
  - dse.ldif変更前に作成されるバックアップ
- dse.ldif.startOK
  - サーバ起動時にdse.ldifファイルのコピーが記録される

複数インスタンス

複数インスタンス

- 顧客A向けにdc=example,dc=com，顧客B向けにdc=example,dc=netを提供したい
- OpenLDAPの場合，2種類のslapd.confを用意して対応可能
  - # slapd –f 設定ファイル –h ldap://x.x.x.x:389
- FDS/IDSは複数インスタンスに対応しているため，管理コンソールから簡単に別インスタンスを作成可能

新規インスタンスの作成



インスタンスディレクトリ

- /opt/fedora-ds/slapd-main/start-slapd

- /opt/fedora-ds/slapd-sub1/start-slapd
- /opt/fedora-ds/slapd-sub2/start-slapd
- /opt/fedora-ds/slapd-sub3/start-slapd

ツリー構成

OpenLDAPでツリーと言えば

- slapd.confに定義されているsuffix
- suffix “dc=bluecoara,dc=net”
- 全てのデータはこのツリー以下に保存される
.

FDS/IDSのツリー構成

- dc=bluecoara,dc=net
  - 基本となるSuffix. 実体は$inst/db/userRoot/
- o=NetscapeRoot
  - ディレクトリサーバ全体を管理するツリー. 複数インスタンスなどの情報はここに. メインインスタンスのみに存在. 実体は$maininst/db/NetscapeRoot/
- cn=config
  - それぞれのインスタンスでの設定が保存される. 実体は$inst/config/dse.ldif
- cn=monitor
  - モニタリング用の設定が保存される. 実体は$inst/config/dse.ldif
- cn=schema
  - 各種スキーマが保存される. 実体は$inst/config/schema/

バックアップ，リストア

バックアップ，リストア

- tar/cp
- LDIF形式によるエクスポート，インポート
  - OpenLDAPでのslapcat，slapadd
- 管理コンソールからGUI操作

バックアップ

- db2ldif –n userRoot
- db2ldif –s “dc=bluecoara,dc=net”

- -n instance_name
- -s suffix_name

- インスタンス名はdse.ldif内に定義．デフォルトのユーザツリーはuserRoot，設定ツリーはNetscapeRootとして定義済み．

dse.ldifの一部

- dn: cn="dc=bluecoara,dc=net",cn=mapping tree,cn=config
- objectClass: top
- objectClass: extensibleObject
- objectClass: nsMappingTree
- cn: "dc=bluecoara,dc=net"
- nsslapd-state: backend
- nsslapd-backend: userRoot

リストア

- ldif2db –n userRoot –l ldiffile
- ldif2db –s “dc=bluecoara,dc=net” –l ldiffile

- デーモンプロセス停止中に行う

その他バックアップ，リストア

- db2ldifで作成されるLDIFにはldapsearchした場合には見えないACI情報など付加される
  .
- そのためldapsearch > backupfileはバックアップと言えない
- 必要に応じてo=NetscapeRootもバックアップ

ACI

Access Control Instructions

ACI設定

- ou=People,dc=bluecoara,dc=net以下のツリーで，ユーザ自身が自分のエントリを自由に編集できるようにするACI
- ACI設定も当然LDAP中に登録する
- オンライン・オフライン設定

オンラインACI設定

- ldapmodifyするだけでアクセス設定が完了

```
dn: ou=People, dc=bluecoara,dc=net
objectClass: top
objectClass: organizationalunit
ou: People
aci: (targetattr = "*")
  (version 3.0;acl "Allow self entry modification";allow
  (all)(userdn = "ldap:///self");
  )
```

複雑なACI設定(1)

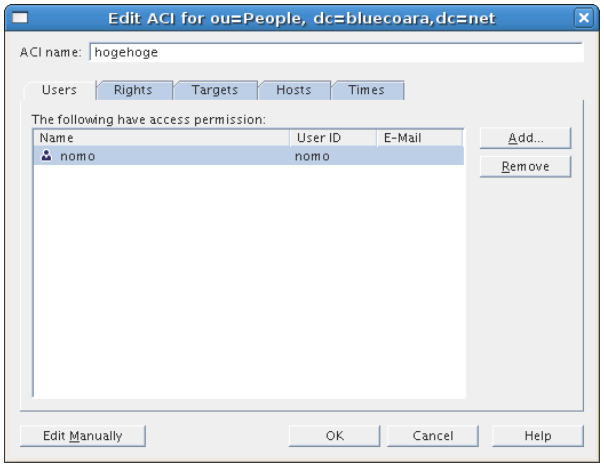
- 複雑な設定も・・・.

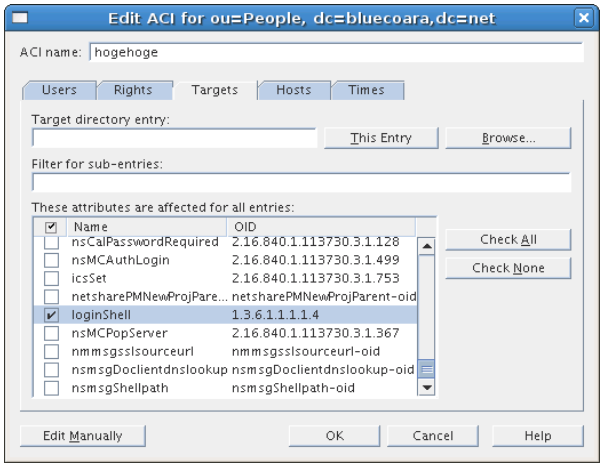
```
aci: (targetattr = "loginShell")
  (version 3.0;acl "hogehoge";allow(delete,add)
  (userdn = "ldap:///uid=nomo,ou=People, dc=bluecoara,dc=net")
  and (timeofday >= "900" and timeofday < "1900");)
```

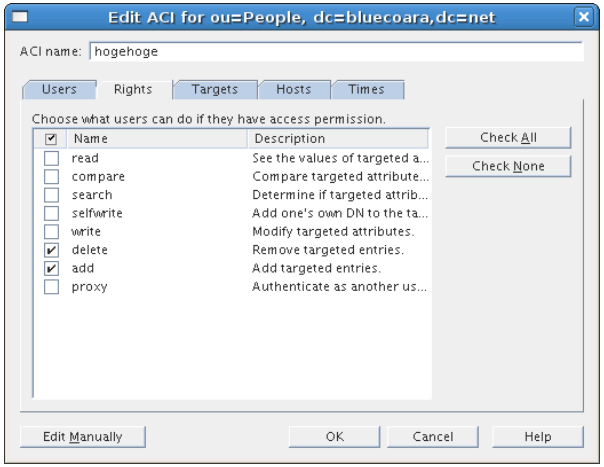
- loginShell属性に対してuid=nomoは delete/addのみ9:00～19:00までの間で可能

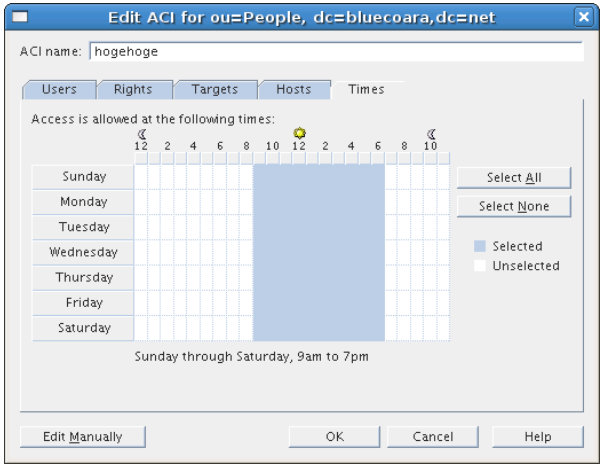
.

複雑なACI設定(2)


Edit ACI for ou=People, dc=bluecoara,dc=net
ACI name: hogehoge
Users Rights Targets Hosts Times
The following have access permission:
Name User ID E-Mail
nomo nomo
Add...
Remove
Edit Manually
OK
Cancel
Help


Edit ACI for ou=People, dc=bluecoara,dc=net
ACI name: hogehoge
Users Rights Targets Hosts Times
Target directory entry:
This Entry
Browse...
Filter for sub-entries:
These attributes are affected for all entries:
Name OID
nsCalPasswordRequired 2.16.840.1.113730.3.1.128
nsMCAuthLogin 2.16.840.1.113730.3.1.499
icsSet 2.16.840.1.113730.3.1.753
netsharePMNewProjPare... netsharePMNewProjParent-oid
loginShell 1.3.6.1.1.1.1.4
nsMCPopServer 2.16.840.1.113730.3.1.367
nmmsgsslsourceurl nmmsgsslsourceurl-oid
nsmsgDoclientdnslookup nsmsgDoclientdnslookup-oid
nsmsgShellpath nsmsgShellpath-oid
Check All
Check None
Edit Manually
OK
Cancel
Help


Edit ACI for ou=People, dc=bluecoara,dc=net
ACI name: hogehoge
Users Rights Targets Hosts Times
Choose what users can do if they have access permission.
Name Description
read See the values of targeted a...
compare Compare targeted attribute...
search Determine if targeted attrib...
selfwrite Add one's own DN to the ta...
write Modify targeted attributes.
delete Remove targeted entries.
add Add targeted entries.
proxy Authenticate as another us...
Check All
Check None
Edit Manually
OK
Cancel
Help


Edit ACI for ou=People, dc=bluecoara,dc=net
ACI name: hogehoge
Users Rights Targets Hosts Times
Access is allowed at the following times:
12 2 4 6 8 10 12 2 4 6 8 10
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Select All
Select None
Selected
Unselected
Sunday through Saturday, 9am to 7pm
Edit Manually
OK
Cancel
Help

ACI設定のコツ

- 実現したいACIは一度GUIから作成し，以後はそれをテンプレートとしてCUIで管理する

クライアントツール

クライアントツール

- $ds/shared/bin/ldapsearch etc・・・
- $ds/plugins/slapd/slapi/include/ldap.h
- $ds/clients/lib/libldap60.so

- liblber.soは無いので注意

冗長化・負荷分散

冗長化

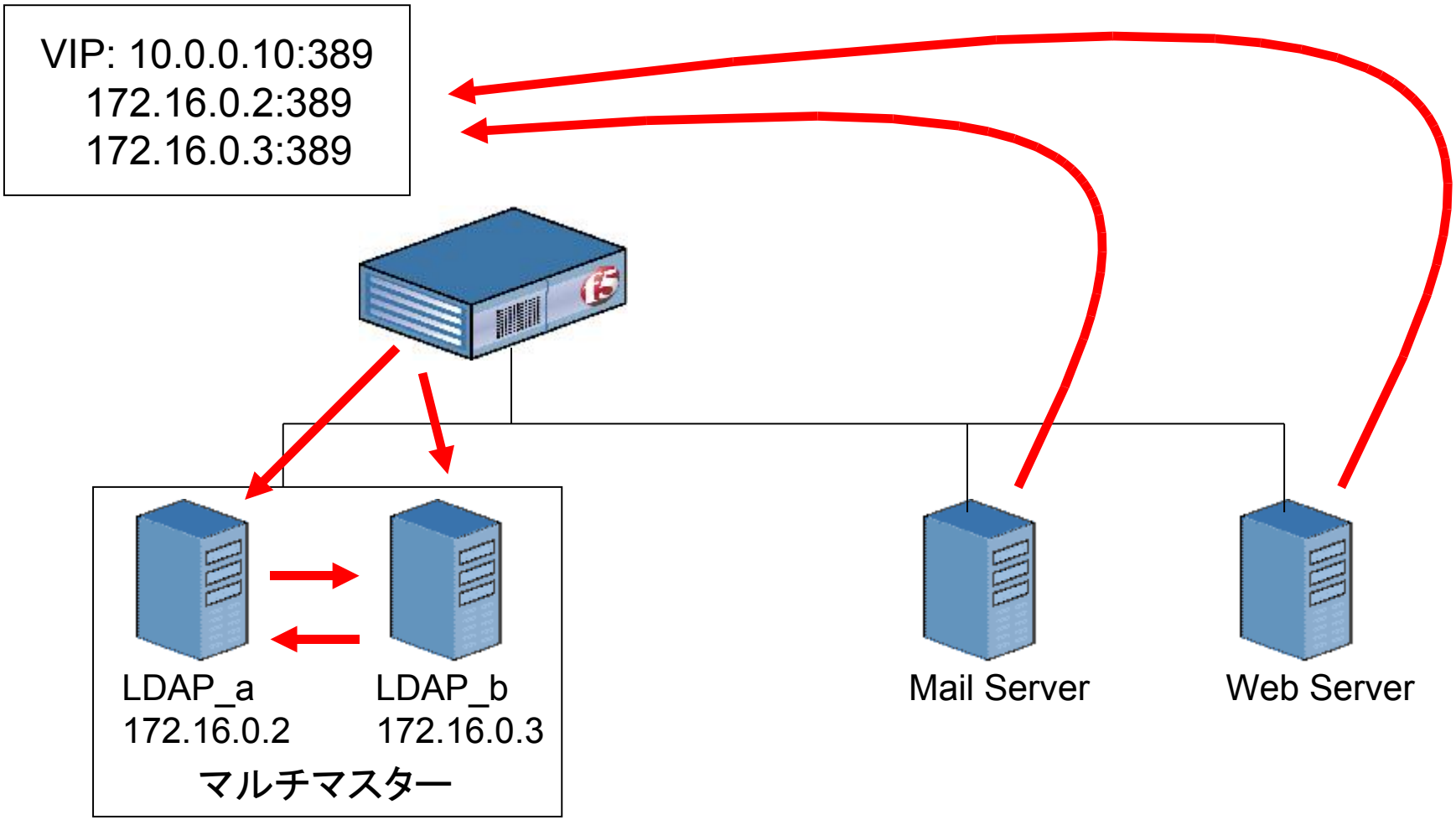
- DBサーバなどではActive/StandbyのHAクラスタが一般的
- Active/Active構成で互いが互いを非同期でアップデートしあう = マルチマスターレプリケーション構成
- OpenLDAPではマルチマスターが実装されようとしていたものの，まだまだ実用的ではない

レプリケーションの概念

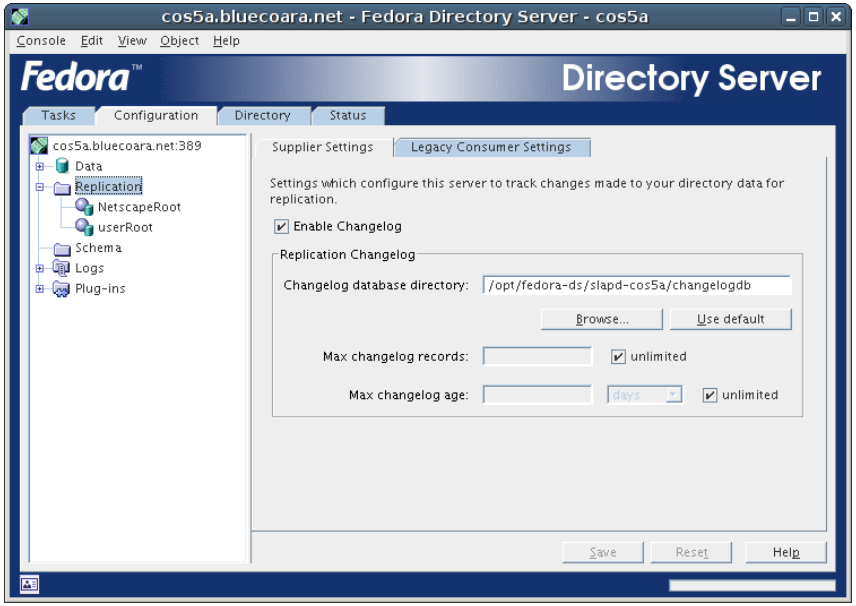
- サプライヤ
  - コンシューマに情報を提供するLDAPサーバ
- コンシューマ
  - サプライヤから情報提供を受けるLDAPサーバ

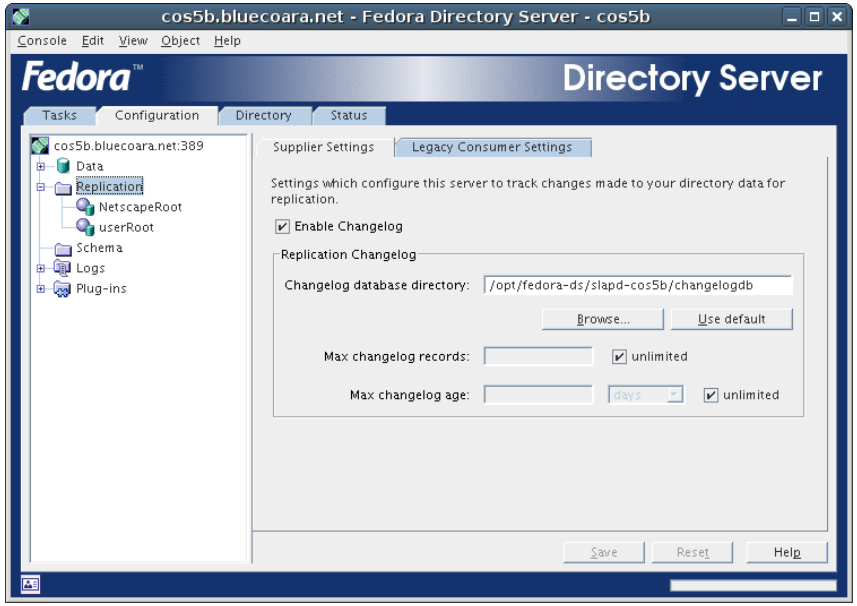
- サプライヤがコンシューマのポートに対して自発的にldapaddなどすることによりレプリケーションが行われる
- コンシューマがサプライヤから情報をダウンロードするわけではないので注意

冗長化 + 負荷分散

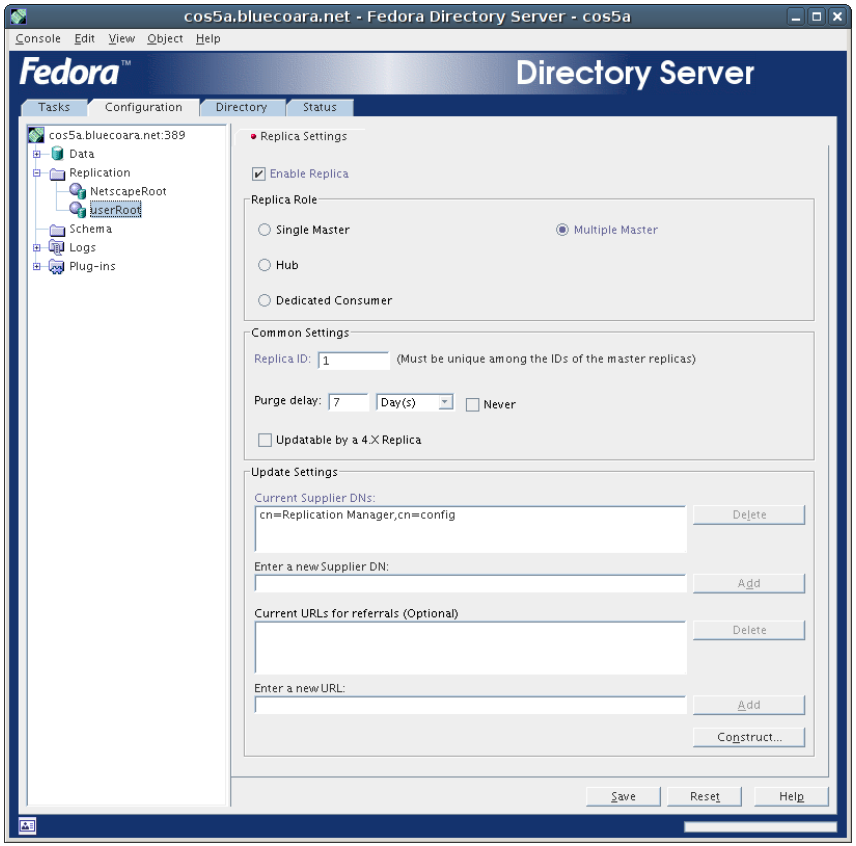

VIP: 10.0.0.10:389
172.16.0.2:389
172.16.0.3:389
LDAP_a
172.16.0.2
LDAP_b
172.16.0.3
マルチマスター
Mail Server
Web Server

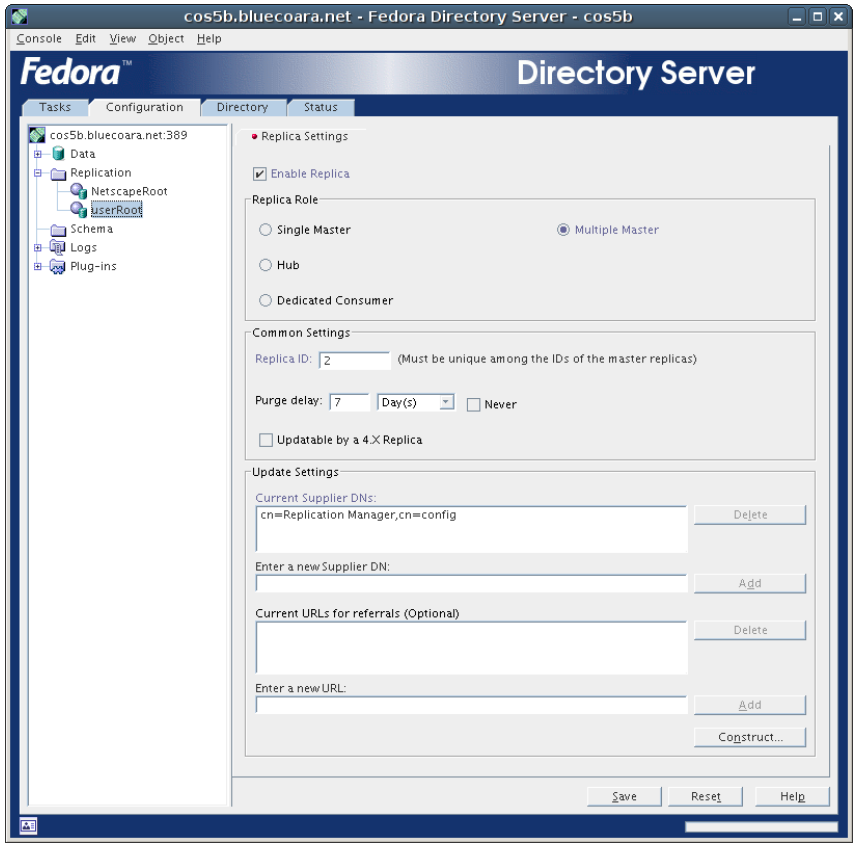
マルチマスター設定(1)
ChangeLog指定



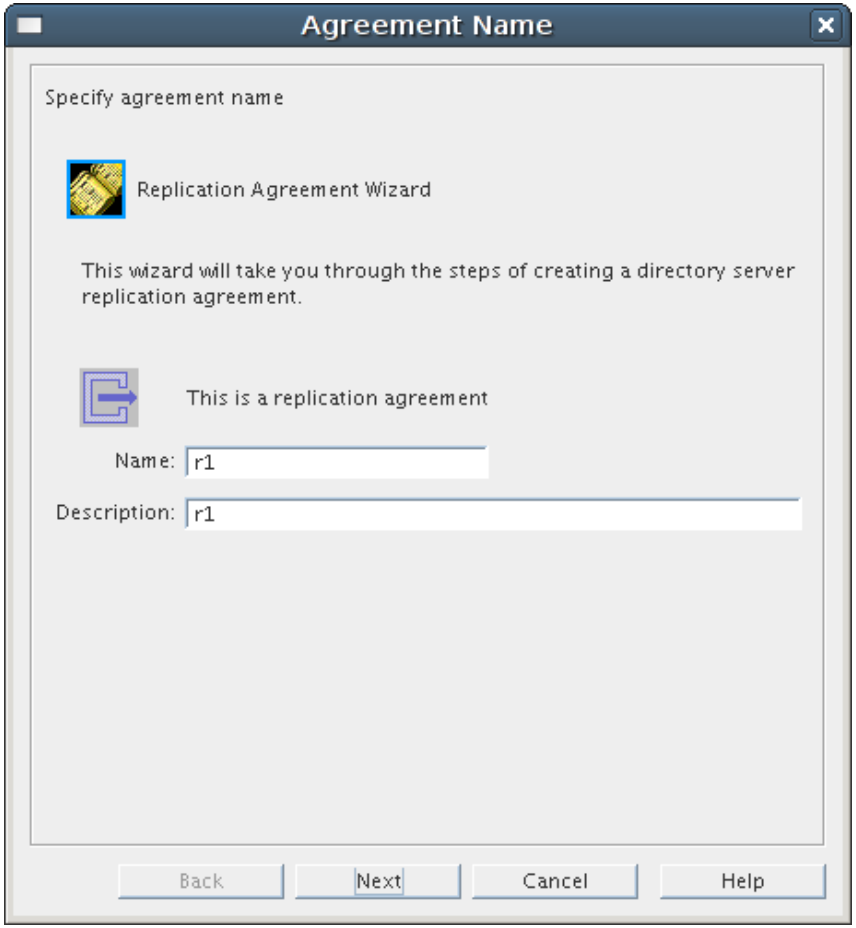


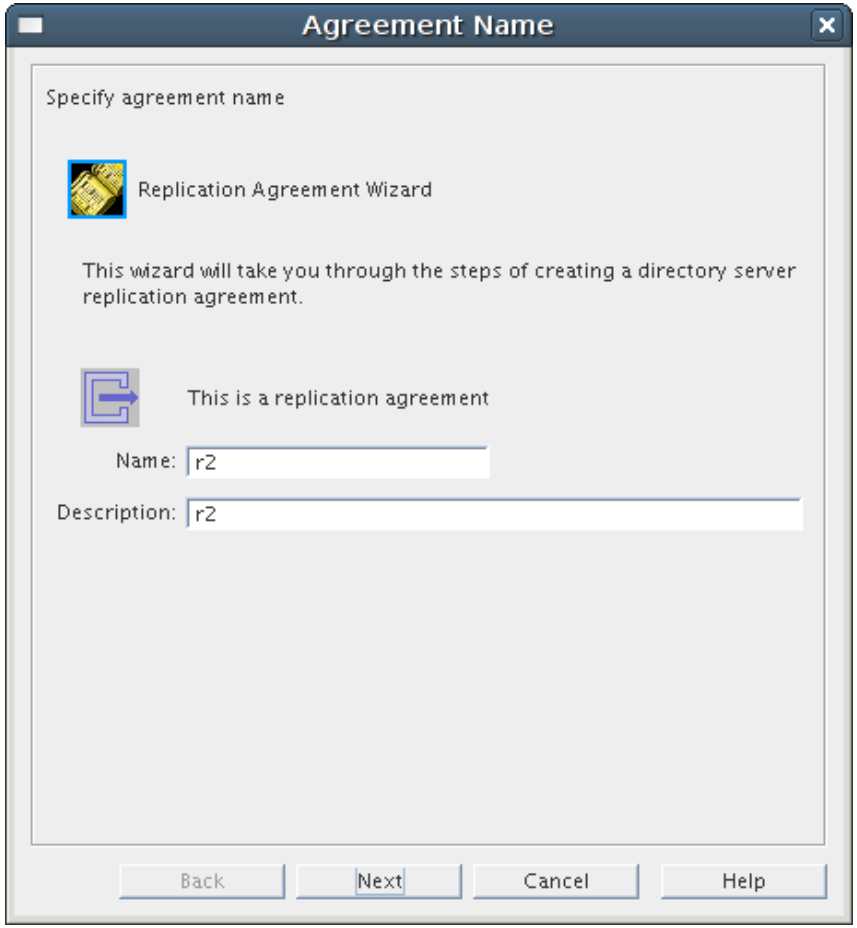
マルチマスター設定(2)
レプリカ設定



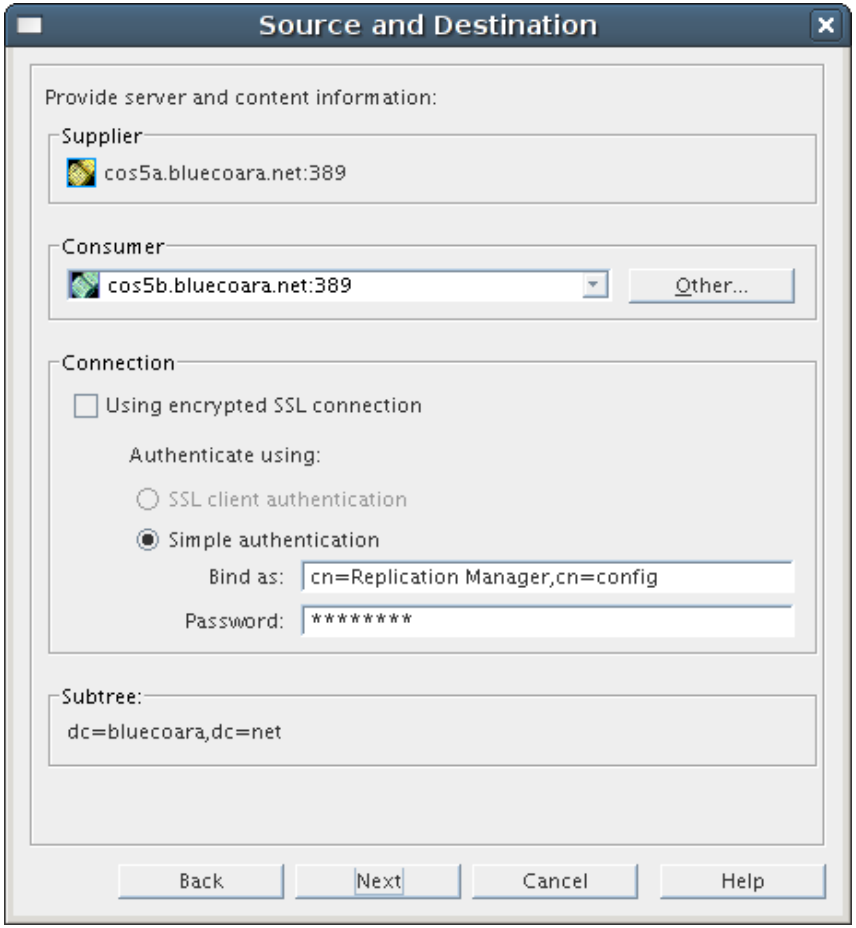


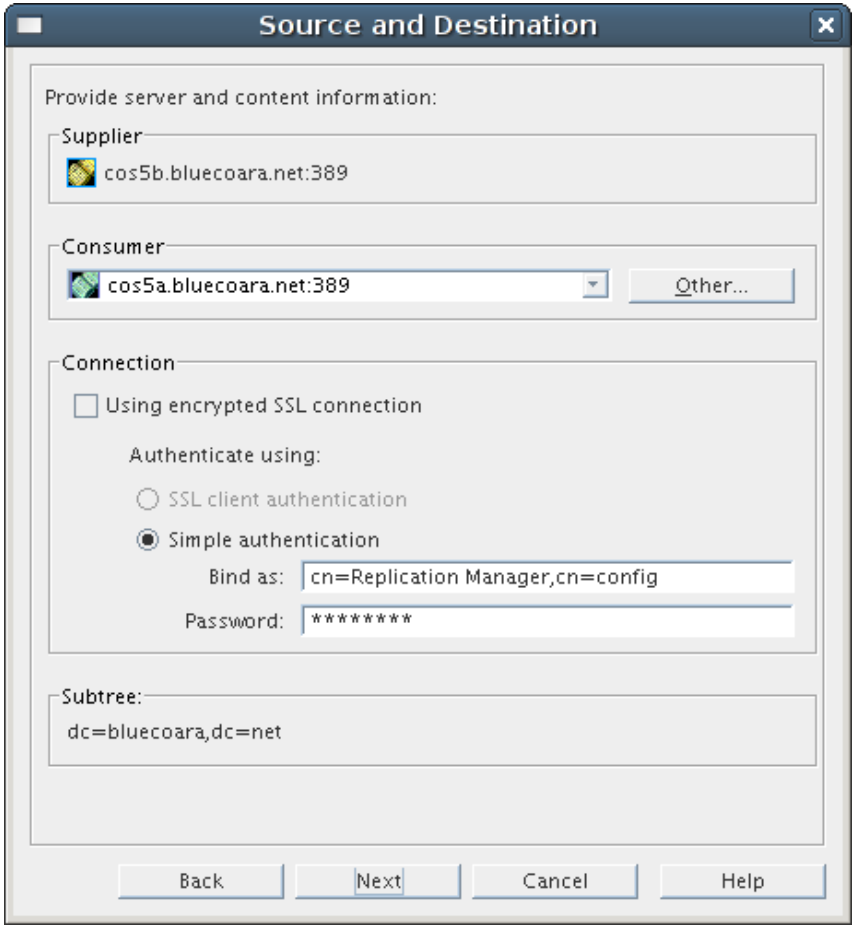
マルチマスター設定(3)
Agreement設定



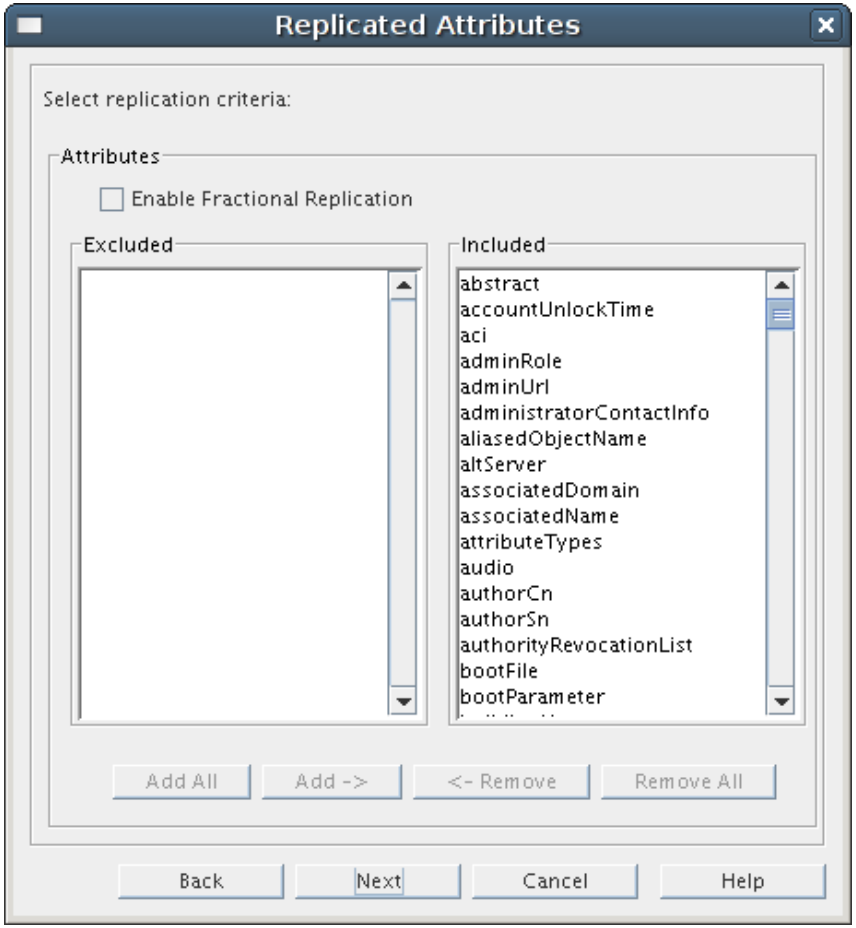


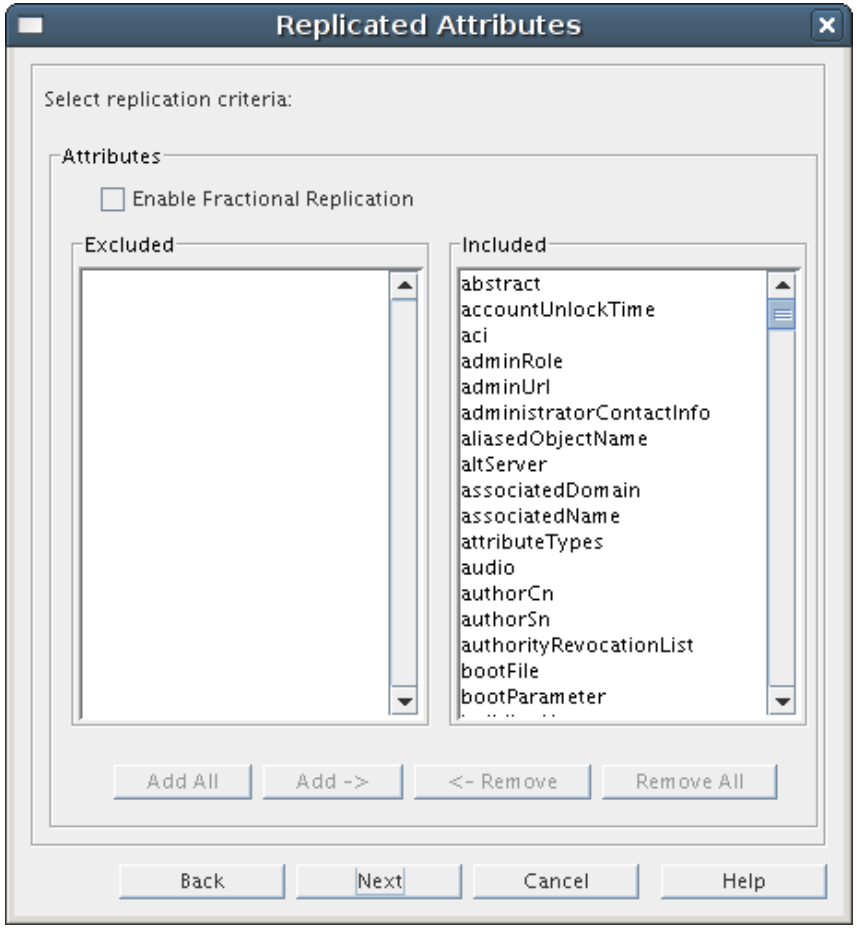
マルチマスター設定(4)
Agreement設定



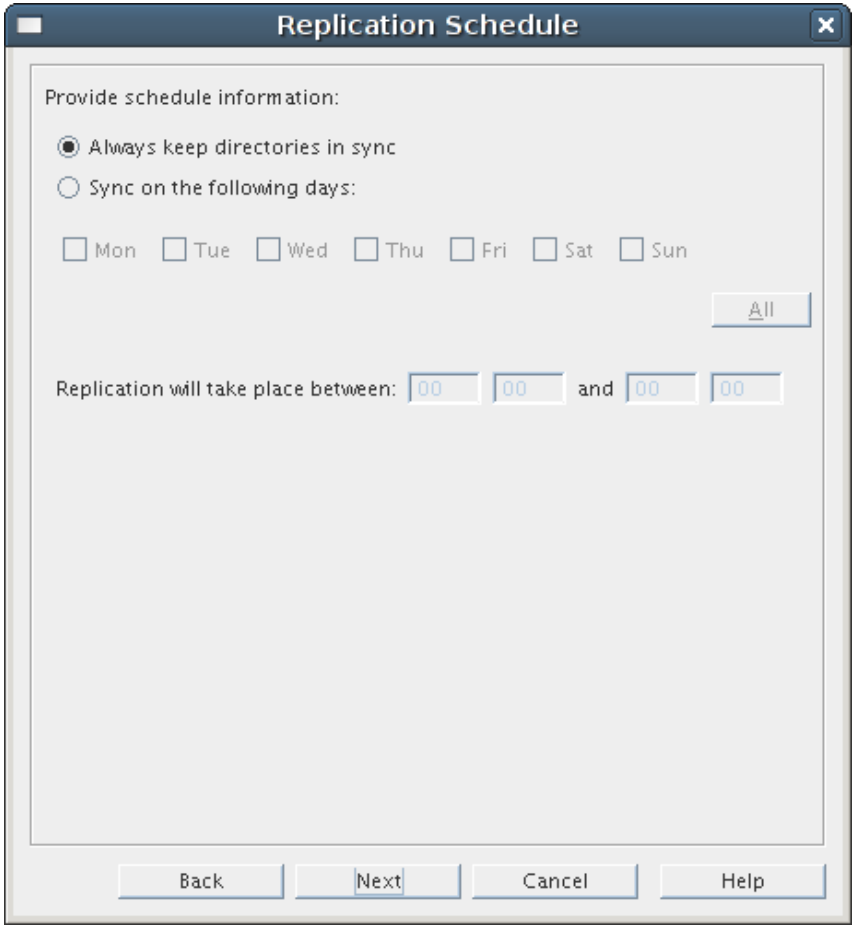


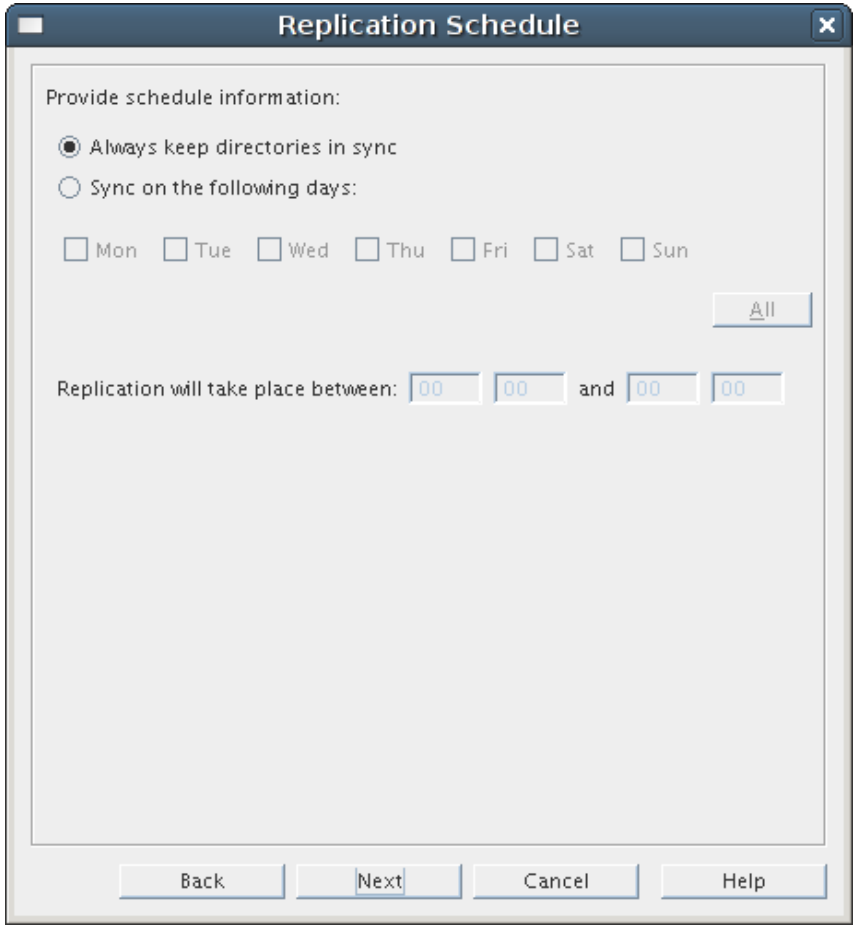
マルチマスター設定(5)
Agreement設定



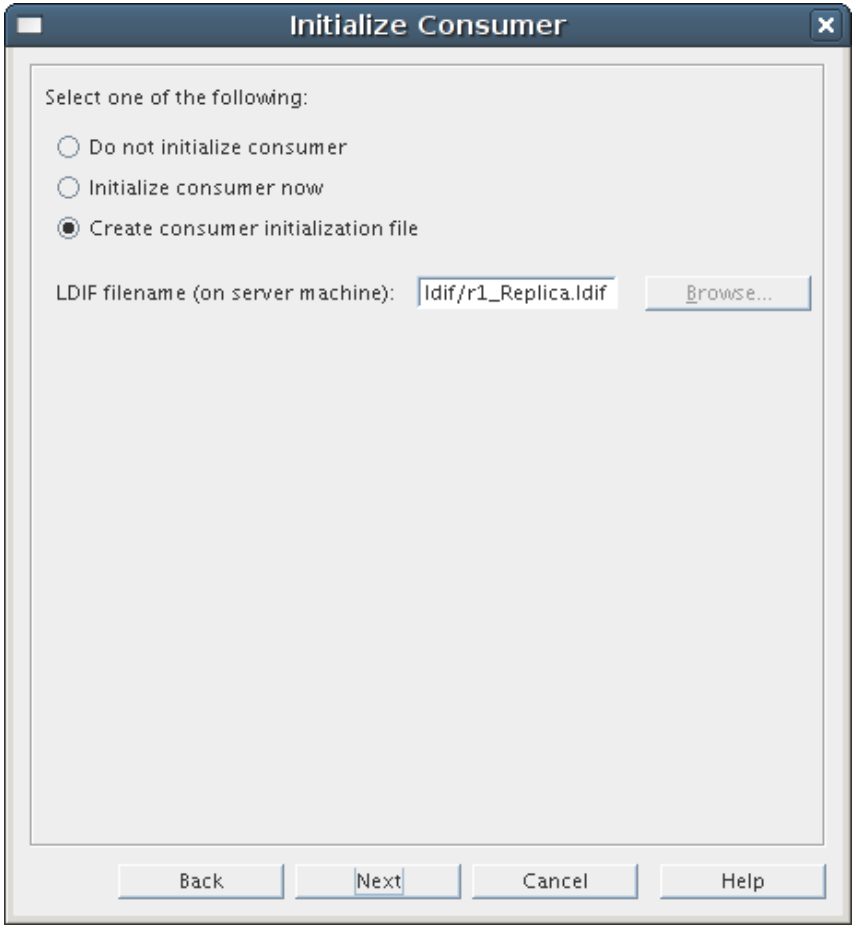


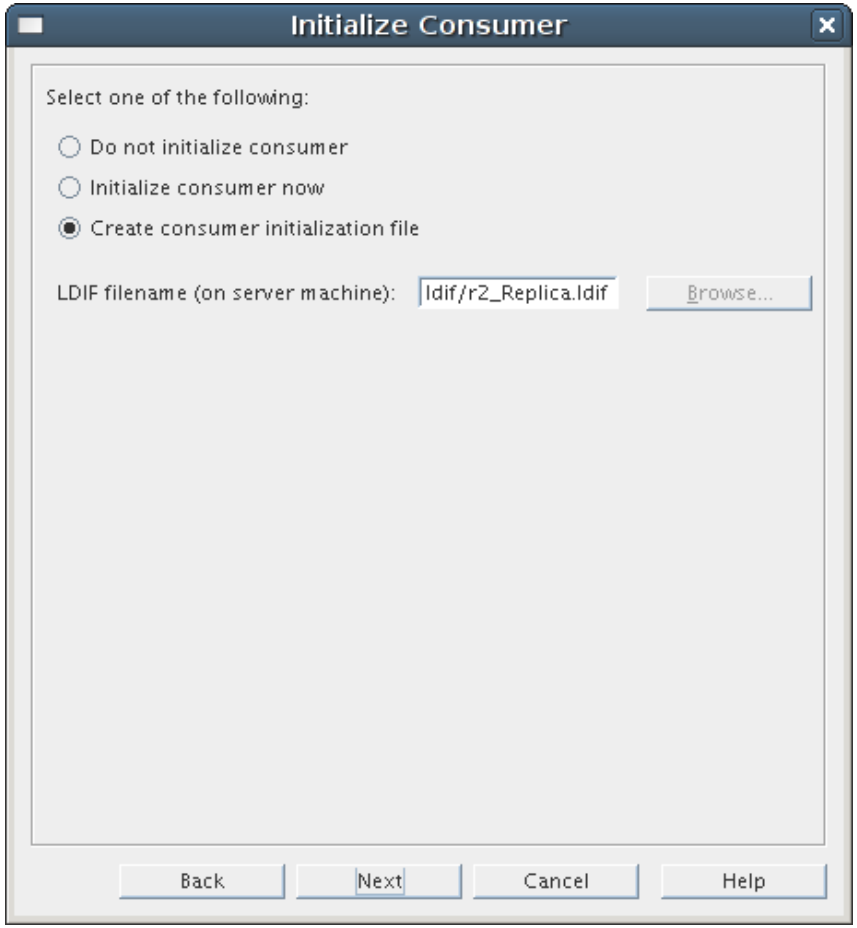
マルチマスター設定(6)
Agreement設定



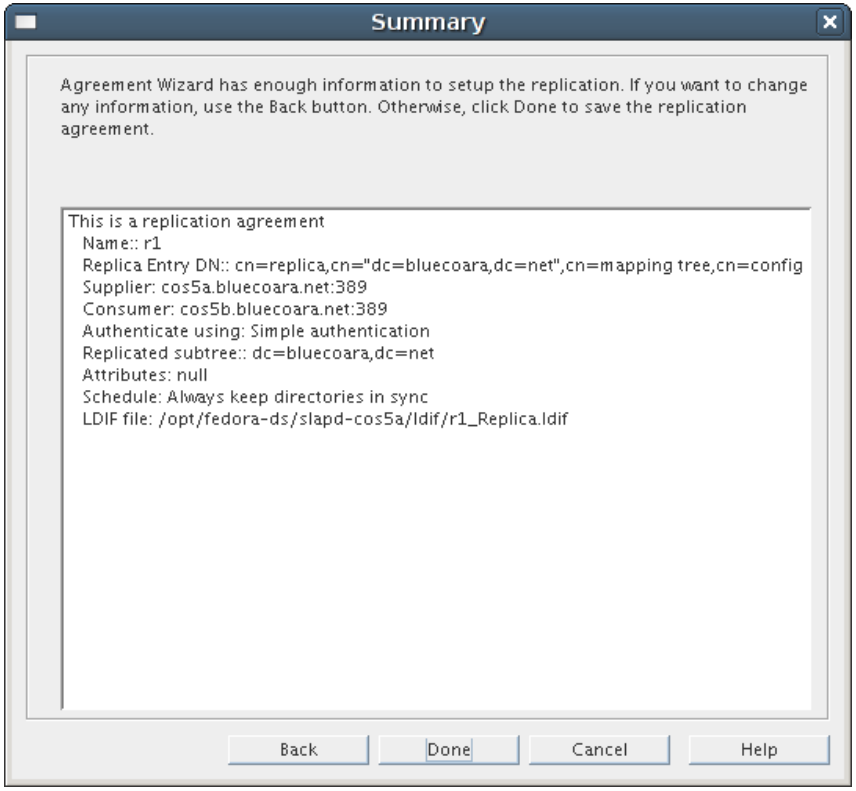


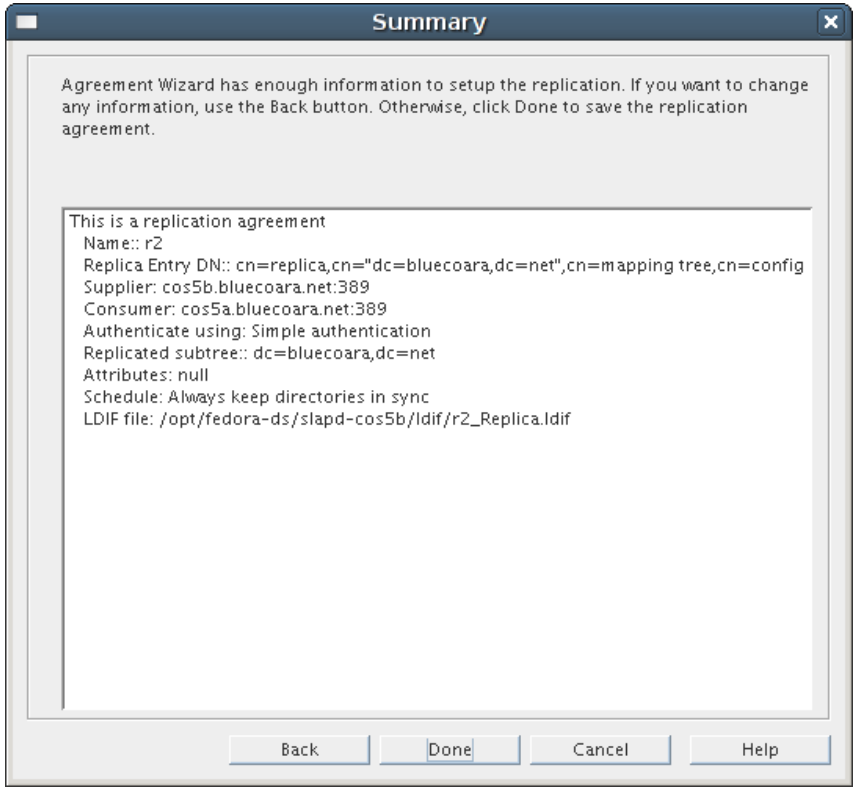
マルチマスタ設定(7)
Agreement設定



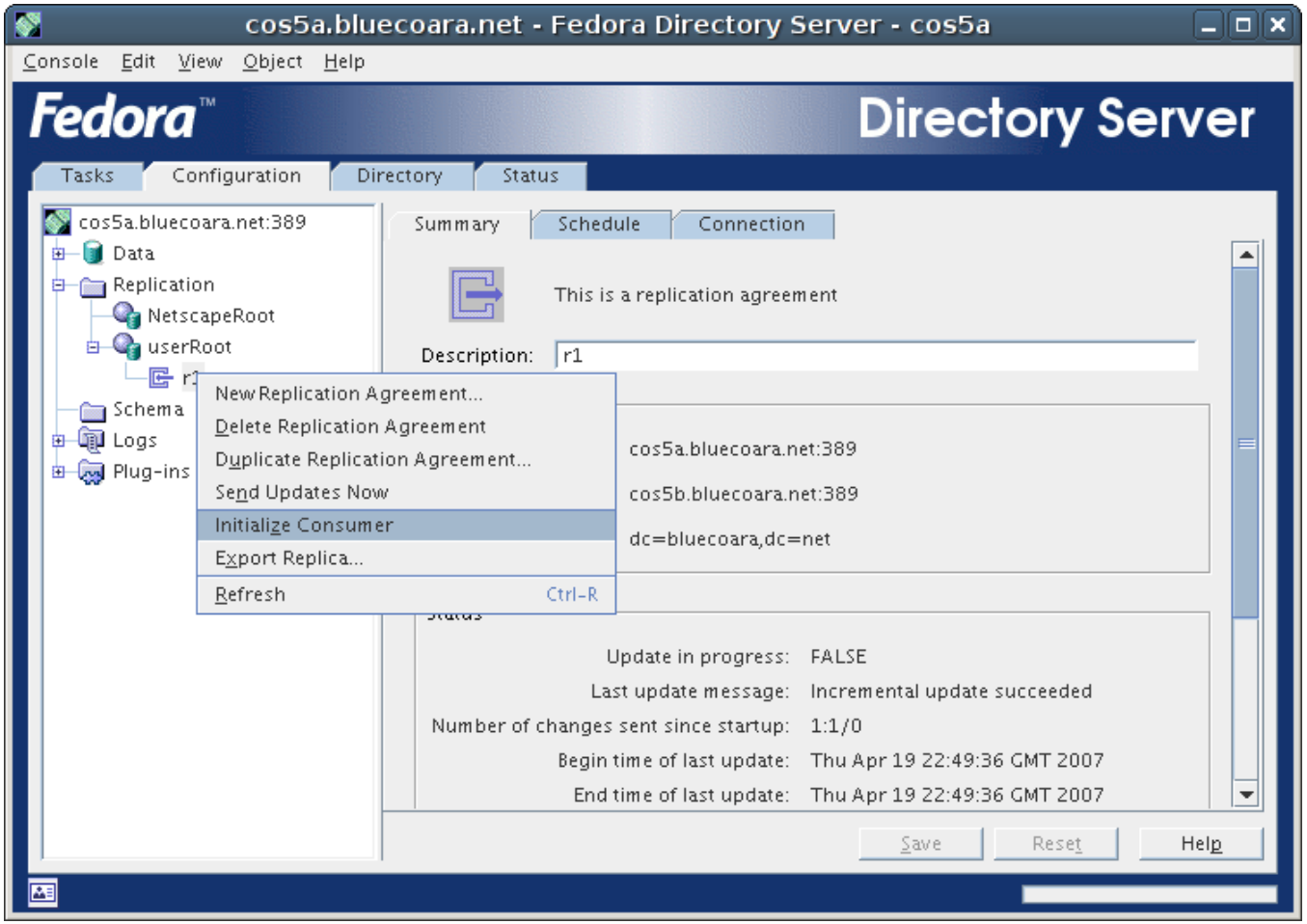


マルチマスタ設定(8)
Agreement設定





マルチマスター設定(9)
イニシャライズ



マルチマスター時のldapadd

- cos5aとcos5bにマルチマスター設定が存在

```
% ldapadd -x -h cos5a -D "cn=Directory Manager" \
  -w abcd1234 -f sample.ldif
```

マルチマスター時のログ(1)
cos5a

```
[20/Apr/2007:07:44:34 +0900] conn=19 fd=69 slot=69 connection from 192.168.0.4 to 10.1.0.111
[20/Apr/2007:07:44:34 +0900] conn=19 op=0 BIND dn="cn=Directory Manager" method=128 version=3
[20/Apr/2007:07:44:34 +0900] conn=19 op=0 RESULT err=0 tag=97 nentries=0 etime=0 dn="cn=directory manager"
[20/Apr/2007:07:44:34 +0900] conn=19 op=1 ADD dn="cn=sample,dc=bluecoara,dc=net"
[20/Apr/2007:07:44:34 +0900] conn=19 op=1 RESULT err=0 tag=105 nentries=0 etime=0
csn=4627f0dc000000010000
[20/Apr/2007:07:44:34 +0900] conn=19 op=2 UNBIND
[20/Apr/2007:07:44:34 +0900] conn=19 op=2 fd=69 closed - U1
[20/Apr/2007:07:44:34 +0900] conn=20 fd=70 slot=70 connection from 10.1.0.112 to 10.1.0.111
[20/Apr/2007:07:44:34 +0900] conn=20 op=0 BIND dn="cn=Replication Manager,cn=config" method=128 version=3
[20/Apr/2007:07:44:34 +0900] conn=20 op=0 RESULT err=0 tag=97 nentries=0 etime=0 dn="cn=replication
manager,cn=config"
[20/Apr/2007:07:44:34 +0900] conn=20 op=1 SRCH base="" scope=0 filter="(objectClass=*)"
attrs="supportedControl supportedExtension"
[20/Apr/2007:07:44:34 +0900] conn=20 op=1 RESULT err=0 tag=101 nentries=1 etime=0
[20/Apr/2007:07:44:34 +0900] conn=20 op=2 SRCH base="" scope=0 filter="(objectClass=*)"
attrs="supportedControl supportedExtension"
[20/Apr/2007:07:44:34 +0900] conn=20 op=2 RESULT err=0 tag=101 nentries=1 etime=0
[20/Apr/2007:07:44:34 +0900] conn=20 op=3 EXT oid="2.16.840.1.113730.3.5.3" name="Netscape Replication Start
Session"
[20/Apr/2007:07:44:34 +0900] conn=20 op=3 RESULT err=0 tag=120 nentries=0 etime=0
[20/Apr/2007:07:44:34 +0900] conn=20 op=4 EXT oid="2.16.840.1.113730.3.5.5" name="Netscape Replication End
Session"
[20/Apr/2007:07:44:34 +0900] conn=20 op=4 RESULT err=0 tag=120 nentries=0 etime=0
```

マルチマスター時のログ(1)
cos5b

```
[20/Apr/2007:07:44:45 +0900] conn=21 fd=68 slot=68 connection from 10.1.0.111 to 10.1.0.112
[20/Apr/2007:07:44:45 +0900] conn=21 op=0 BIND dn="cn=Replication Manager,cn=config" method=128 version=3
[20/Apr/2007:07:44:45 +0900] conn=21 op=0 RESULT err=0 tag=97 nentries=0 etime=0 dn="cn=replication
manager,cn=config"
[20/Apr/2007:07:44:45 +0900] conn=21 op=1 SRCH base="" scope=0 filter="(objectClass=*)"
attrs="supportedControl supportedExtension"
[20/Apr/2007:07:44:45 +0900] conn=21 op=1 RESULT err=0 tag=101 nentries=1 etime=0
[20/Apr/2007:07:44:45 +0900] conn=21 op=2 SRCH base="" scope=0 filter="(objectClass=*)"
attrs="supportedControl supportedExtension"
[20/Apr/2007:07:44:45 +0900] conn=21 op=2 RESULT err=0 tag=101 nentries=1 etime=0
[20/Apr/2007:07:44:45 +0900] conn=21 op=3 EXT oid="2.16.840.1.113730.3.5.3" name="Netscape Replication Start
Session"
[20/Apr/2007:07:44:45 +0900] conn=21 op=3 RESULT err=0 tag=120 nentries=0 etime=0
[20/Apr/2007:07:44:45 +0900] conn=21 op=4 ADD dn="cn=sample,dc=bluecoara,dc=net"
[20/Apr/2007:07:44:45 +0900] conn=21 op=4 RESULT err=0 tag=105 nentries=0 etime=0
csn=4627f0dc000000010000
[20/Apr/2007:07:44:47 +0900] conn=21 op=5 EXT oid="2.16.840.1.113730.3.5.5" name="Netscape Replication End
Session"
[20/Apr/2007:07:44:47 +0900] conn=21 op=5 RESULT err=0 tag=120 nentries=0 etime=0
```

Use BIG-IP !!

Appendix

Commands

- start-admin
  - 管理サーバ起動
- stop-admin
  - 管理サーバ停止
- restart-admin
  - 管理サーバ再起動
- startconsole
  - 管理コンソールログイン
- start-slapd
  - slapd起動
- stop-slapd
  - slapd停止
- restart-slapd
  - slapd再起動
- db2ldif
  - LDIFエクスポート
- ldif2db
  - LDIFインポート
- saveconfig
  - 設定ファイルLDIFエクスポート
- restoreconfig
  - 設定ファイルLDIFインポート