**openldap2.4 的同步&分布式部署方式**

​一、openldap2.4 的同步方式

**1、Syncrepl （全量模式）**：slave服务器用拉的方式同步master数据，使用该方法最大的缺陷在于：当你修改了一个Entry中的任何一个属性，那么该方法会把该条目下所有的属性都同步过来。

2、**Delta-syncrepl（增量模式）**：比syncrepl多了一个基于日志的同步功能。每在master修改一条数据后，就会产生一个日志文件，salve通过master的日志进行相应的修改，这种方式克服了当修改条目中某个属性后要把整个条目都更新过来的缺点；

**3、N-WAY Mutli-Master**:多主Master方式同步LDAP信息

**4、MirrorMode**：該方式是服務器互相以推的方式同步用戶數據。MirrorMode只支持2個主MASTER(並不是說鏡像模式只能做2台LDAP，而是只有2個MASTER起作用可以推送數據出去，其他的LDAP服務器也會同步更新，只要把提供者指定到這2個MASTER任意一台即可),當你設定超過2台的時候，該模式只有最開始設定的那2台是MASTER，能主動互相推送數據。後面超過的如第三台LDAP3或LDAP4時，這些自動全部變成單向同步，即只有那2個主MASTER修改用戶數據后可以同步到下面的第三台或第四台LDAP上， LDAP3，LDAP4做任何動作都無法將數據同步到主master上。也不會同不到其他LDAP服務器上,有點類似老版本slurp的效果。

**5.Syncrepl Proxy**：代理同步。將保留用戶信息的MASTER主機隱藏起來，而代理機上面的LDAP通過Syncrepl從MASTER主機以拉的方式同步maser用戶數據，當代理主機發生改變時，代理主機的LDAP又以推的方式將數據更新到更下層的slave LDAP服務器上。而slave LDAP是沒有權限去更改代理服務為那台LDAP用戶信息，只有讀取權限，什麽，這種情況類似老版本的slurp單向同步功能，並且和老版本slurp一樣可以建立一個快捷方式(這個快捷方式不保留任何數據，數據全部保留在你去指定的那台LDAP服務器上，只是說你可以通過這個快捷方式在slave LDAP服務器上也可以修改數據。該快捷方式具體應用可以去查看RPM包方式當中安裝方法里有說明。)

**二、安装**

**1.编译安装**

为了使用openldap的同步协议，必须在编译阶段强制开启如下的编译选项，

./configure --prefix=/usr/local/openldap --enable-debug --enable-modules --enable-ldap --enable-relay --enable-accesslog --enable-auditlog --enable-syncprov

其中--enable-overlays --enable-ldap --enable-accesslog  --enable-syncprov必不可少。

* --enable-ldap 选项用于支持ldap代理，在同步中用来推送数据；
* --enable-accesslog 选项用于记录用户操作，在同步中用于记录服务端的数据修改；
* --enable-syncprov 选项用于支持数据同步引擎

**2.yum安装**

Yum –y install openldap\* compat-openldap

3.日志配置

mkdir /var/log/slapd

chmod 755 /var/log/slapd/

chown ldap:ldap /var/log/slapd/

vi /etc/rsyslog.conf添加如下配置

local4.\* /var/log/slapd/openldap.log

4. openldap服务器安装证书

[root@openldap-master ~]# vi /etc/openldap/ldap.conf

BASE dc=unfgroup,dc=com

URI ldaps://192.168.16.19 ldap://ldap-master.example.com:666

TLS\_CACERTDIR /etc/openldap/certs

TLS\_REQCERT never

[root@openldap-master ~]#vi /etc/openldap/slapd.conf

TLSCACertificatePath /etc/openldap/certs

TLSCertificateFile /etc/openldap/certs/server.crt

TLSCertificateKeyFile /etc/openldap/certs/server.key

TLS\_REQCERT never

[root@openldap-master ~]# chown ldap.ldap /etc/openldap/cacerts/

[root@localhost ~]# vi /etc/sysconfig/ldap

# Run slapd with -h "... ldap:/// ..."

# yes/no, default: yes

SLAPD\_LDAP=yes

# Run slapd with -h "... ldapi:/// ..."

# yes/no, default: yes

SLAPD\_LDAPI=no

# Run slapd with -h "... ldaps:/// ..."

# yes/no, default: no

SLAPD\_LDAPS=yes

[root@openldap-master ~]# service slapd restart

停止 slapd：[确定]

这里我们采用这种方式来启动ldap，这样可以监听加密和非加密的端口，

[root@openldap-master ~]# slapd -h "ldap:/// ldaps:///"

如果只想监听加密的

[root@openldap-master ~]# slapd -h "ldaps:///"

[root@openldap-master ~]# netstat -ntpl |grep slapd

tcp 0 0 0.0.0.0:636 0.0.0.0:\* LISTEN 25671/slapd

tcp 0 0 0.0.0.0:389 0.0.0.0:\* LISTEN 25671/slapd

tcp 0 0 :::636 :::\* LISTEN 25671/slapd

tcp 0 0 :::389 :::\* LISTEN 25671/slapd

[root@23 openldap]# cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG

[root@23 openldap]# cp /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf

slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d/

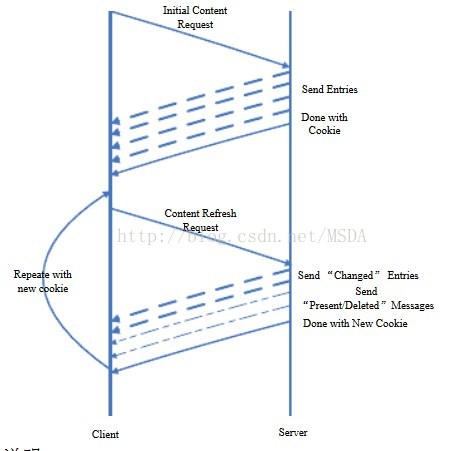
三、ldap数据同步协议传递

3.1 同步模式

* refreshOnly和refreshAndPersist。这两种模式中，同步均由客户端发起，所不同的是同步完成后的操作：refreshOnly模式下，后续操作由客户端轮询完成
* refreshAndPersist模式下，在后续操作中，服务端负责发送相应的改变数据而客户端负责接受并处理本地ldap条目

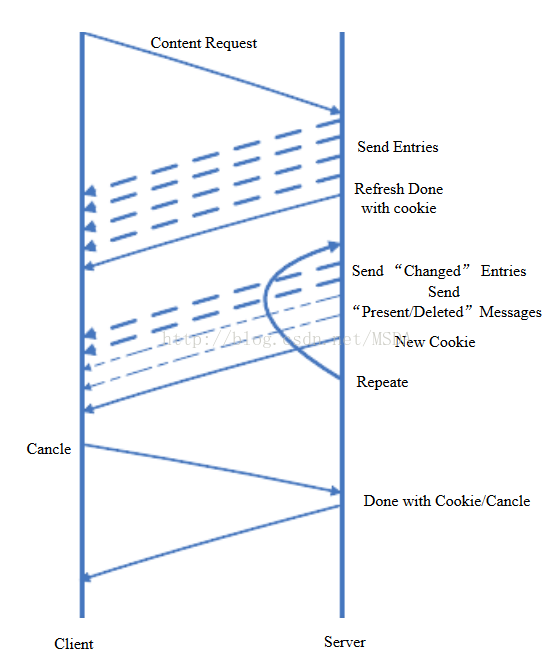
      为了提高性能和减少网络传输，ldap数据同步协议要求客户端发起同步请求时，提供一个cookie(最开始的请求除外)。服务端根据此cookie来决定发送给客户端的数据，客户端根据接收到的数据来处理本地的ldap条目。在同步完成之后，客户端必须更新cookie，用于下次同步。Cookie是服务端计算（查询本地条目）的依据。在每种模式中，都涉及到如何计算数据的变化，包括：添加的数据、修改的数据以及删除的数据。Ldap的每个条目包含了时间信息，包括生成时间戳(createTimestamp)和修改时间戳（modifyTimestamp）。对于添加和修改的数据，服务端根据客户端传送来的cookie（包含时间信息）计算得到，并将这些数据发送给客户端，每个数据标记是添加的还是修改的。当服务端有修改日志时，服务端可以较容易地根据cookie来计算被删除的条目，并将这些条目的DN或者UUID发送给客户端。客户端收到后删除本地的条目。此种情况下，删除条目的计算在服务端完成。当服务端无记录修改日志时，服务端无法计算哪些条目被删除，它只能提供当前还存在的数据。服务端将这些还存在的条目DN或者UUID[2]发送给客户端，由客户端来计算已删除条目。

  3.2 refreshOnly模式



1. Initial Content Request(初始请求)中，客户端不提供cookie，服务端返回所有符合查询条件的条目，结束时客户端得到一个cookie;
2. Content Refresh Request(内容更新请求)与初始化请求的查询条件必须一致，并且包含一个cookie
3. 内容更新阶段，“Changes Entries”包括新添加的条目和修改的条目（基于cookie计算得出）；对于已删除的条目，有两种方式来通知客户端。“Present Messages”用于返回当前还存在的条目；“Deleted?Messages”用于明确告知客户端已删除的条目。这两种消息仅包含条目的名称（DirectoryName）或者UUID。

 3.3  refreshAndPersist模式



1）refreshAndPersist模式包括两个阶段：refresh和persist。Refresh阶段用来保证客户端与服务端内容一致，persist阶段由服务端循环发送数据改变给客户端；

2）persist阶段中，服务端发送改变数据时，发送cookie给客户端（可选）

* overlay syncprov：后端使用syncprov作为overlay作为组件的扩展
* syncprov-checkpoint 100 1： 同步的满足条件，当满足修改100个条目或者1分钟主动进行推送一次；
* syncprov-sessionlog 100：会话日志条目的最大数量

四、配置方法

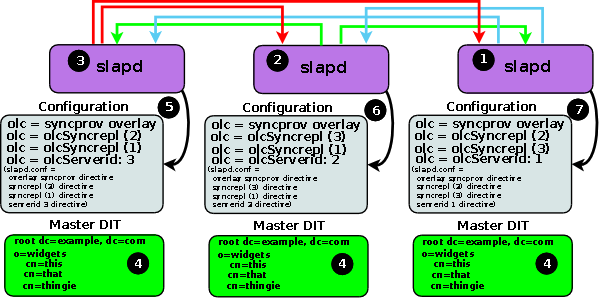
4.1Syncrepl

    该同步方式只支持单向同步，即master---》slave的单向同

4.2 accesslog

4.3 Multi-Master同步，（N-Way）syncrepl

在该同步模式下，每台主机既扮演[provider](http://www.zytrax.com/books/ldap/apd/#provider)又扮演[consumer](http://www.zytrax.com/books/ldap/apd/#provider)的角色



配置示例：有两台ldap服务器：ldap1的端口是 389，ldap2的端口是2001；

ldap1配置：

**[html]** [view plain](http://blog.csdn.net/msda/article/details/42177851) [copy](http://blog.csdn.net/msda/article/details/42177851)

1. include /usr/local/openldap/etc/openldap/schema/core.schema
2. include /usr/local/openldap/my-schema/uc101.schema #自定义的schema
4. pidfile /usr/local/openldap/var/run/slapd.pid
5. argsfile /usr/local/openldap/var/run/slapd.args
7. loglevel -1
9. ServerID 001
10. #######################################################################
11. # BDB database definitions
12. #######################################################################
13. database bdb
14. suffix "dc=nd,dc=com"
15. rootdn "cn=admin,dc=nd,dc=com"
16. rootpw 123456
17. directory /data/ldap/openldap-data389
18. index objectClass eq
20. # syncrepl特有的索引
21. index entryCSN eq
22. index entryUUID eq
24. # syncrepl参数
25. syncrepl rid=203
26. provider=ldap://IP地址:端口 #提供者的IP和端口号
27. bindmethod=simple #认证方式，默认选择简单认证
28. binddn="cn=admin,dc=nd,dc=com" #登陆的ldap账号
29. credentials=登陆密码
30. searchbase="dc=nd,dc=com" #同步的根路径
31. filter="(objectClass=\*)"
32. scope=sub
33. attrs="\*,+"
34. type=refreshAndPersist #同步方式：有refreshAndPersist和
35. retry="5 5 300 +"
36. interval=00:00:00:01 #同步时间间隔 天：小时：分钟：秒
38. mirrormode TRUE
39. #######################################################################
40. # syncprov配置
41. #######################################################################
42. overlay syncprov
43. syncprov-checkpoint 100 1
44. syncprov-sessionlog 100

ldap2配置：

**[html]** [view plain](http://blog.csdn.net/msda/article/details/42177851) [copy](http://blog.csdn.net/msda/article/details/42177851)

1. include /usr/local/openldap2001/etc/openldap/schema/core.schema
2. include /usr/local/openldap2001/my-schema/uc101.schema #自定义的schema
4. # Define global ACLs to disable default read access.
6. # Do not enable referrals until AFTER you have a working directory
7. # service AND an understanding of referrals.
8. #referral ldap://root.openldap.org
10. pidfile /usr/local/openldap2001/var/run/slapd.pid
11. argsfile /usr/local/openldap2001/var/run/slapd.args
13. loglevel -1
15. ServerID 002
16. #######################################################################
17. # BDB database definitions
18. #######################################################################
19. database bdb
20. suffix "dc=nd,dc=com"
21. rootdn "cn=admin,dc=nd,dc=com"
22. rootpw 123456
23. directory /data/ldap/openldap-data-2001
24. index objectClass eq
26. # syncrepl特有的索引
27. index entryCSN eq
28. index entryUUID eq
30. # syncrepl参数
31. syncrepl rid=123
32. provider=ldap://192.168.19.103:389
33. bindmethod=simple
34. binddn="cn=admin,dc=nd,dc=com"
35. credentials=登陆密码
36. searchbase="dc=nd,dc=com"
37. filter="(objectClass=\*)"
38. schemachecking=off
39. scope=sub
40. attrs="\*,+"
41. type=refreshAndPersist
42. retry="5 5 300 +"
43. interval=00:00:00:01
45. mirrormode TRUE
46. #######################################################################
47. # syncprov配置
48. #######################################################################
49. overlay syncprov
50. syncprov-checkpoint 100 1
51. syncprov-sessionlog 100