

オープンソースの「今」を伝える

オープンソースカンファレンス2009 Tokyo/Fall

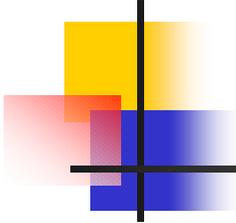
知っておきたい、

OpenLDAPサポートツール

日本LDAPユーザ会

伊藤忠テクノソリューションズ株式会社

菊池研自



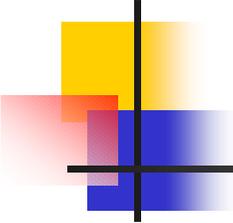
はじめに

- OpenLDAPにはslapXXX、Berkeley DBにはdb_XXXといった、使いどころを理解していると便利なツールがあります。これらのツールの役割を十分理解し、行った操作が正しいことを管理者が自ら確認できれば、効率的な運用が促進され負担は軽減されることでしょう

本資料でのコマンド例の表記は、

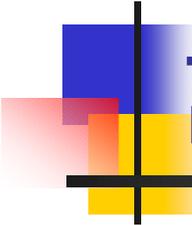
- Cent OS 5.x 、
- OpenLDAP 2.4.x及び、
- Berkeley DB 4.6.x を

ベースにしております。



目次

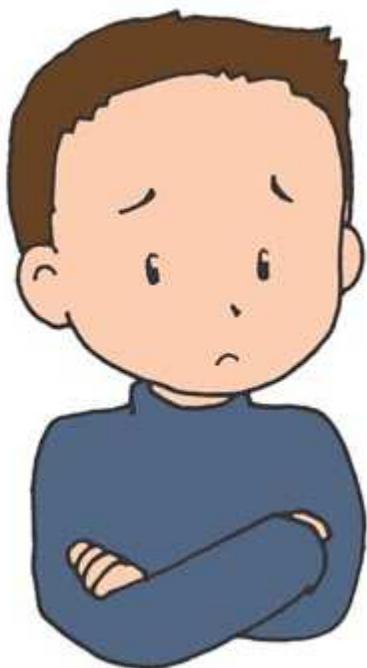
- **OpenLDAPサーバ管理**
 - 設定ファイル
 - アクセス権
 - インデックス管理
 - バックアップ、リカバリ
 - ログ管理
- バックエンドDB(Berkeley DB)管理
- GUI管理ツール



設定ファイル

-slaptest

設定ファイル



- OpenLDAP (ディレクトリサーバ)は、勤怠システムや、メールサーバ、ファイルサーバなど、企業の業務上必要なシステムと連携していることがある。管理者は
 - OpenLDAPサーバを再起動する前に、設定に問題がないかを確認したい
 - 意図した内容が反映されることを、再起動する前に確認したい

slaptest

- slaptest を利用したslapd.confの確認
 - slapd.confに設定した内容をOpenLDAPサーバがどのように解釈するかを確認可能
 - 再起動することなく、OpenLDAPサーバ起動中に、変更する設定が正しく解釈されることを確認可能

```
# slaptest -f ./etc/openldap/slapd.conf -d config
```

```
reading config file ./etc/openldap/slapd.conf
```

```
line 5 (include /usr/local/openldap-2.4.11/etc/openldap/schema/core.schema)
```

```
reading config file /usr/local/openldap-2.4.11/etc/openldap/schema/core.schema
```

```
...[略]...
```

```
line 84 (rootdn "cn=Manager,dc=my-domain,dc=com")
```

```
line 88 (rootpw ***)
```

```
...[略]...
```

```
config file testing succeeded
```

slapd.confの基本ルール

■ OpenLDAPが解析する基本ルール

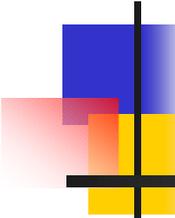
slapd.conf

ルール1. シャープで始まる行は、コメントとして無視
コメント行

ルール2. 空白で始まる行は、継続行
syncrepl rid=123

空白 provider=ldap://provider.example.com:389
type=refreshOnly

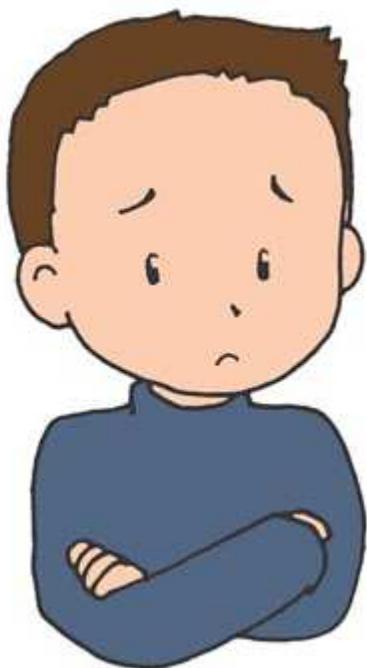
...
ルール3. それ以外は、パラメータと値の組合せ
パラメータ 値



アクセス権

-slapacd

アクセス権



- OpenLDAP (ディレクトリサーバ)は、ネットワーク上にディレクトリのエントリ情報を提供している為、セキュリティ上は、エントリ情報へのアクセス権を必要最低限に絞っておきたい
- 意図した通りのアクセス権が設定されることを、再起動する前に確認したい
- 再起動し、設定を恒久的に反映させる前に、問題がないことを確認したい

解決

slapacl

- slapacl を利用したACL確認
 - 再起動することなく、OpenLDAPサーバ起動中に、変更した場合の振る舞いを確認可能

```
# slapacl -b "uid=test1003,ou=people,dc=my-domain,dc=com" "userPassword/auth" -d acl
```

```
...[略]...
```

```
<= check a_dn_pat: anonymous
```

```
...[略]...
```

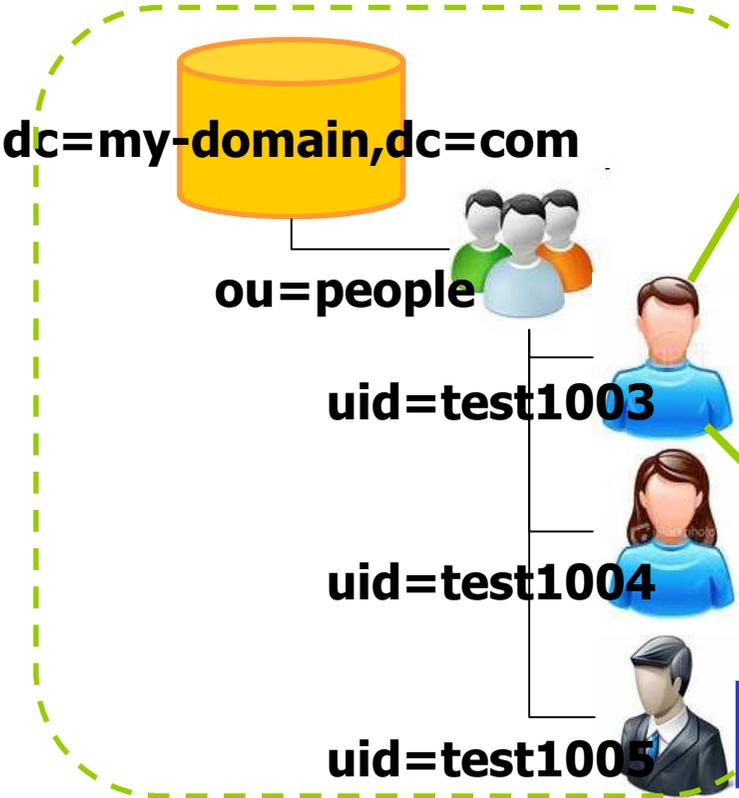
```
=> access_allowed: auth access granted by auth(=xd)
```

```
auth access to userPassword: ALLOWED
```

参考

slapaclの使い所

```
# slapacl -b "uid=test1003,ou=people,dc=my-domain,dc=com" "userPassword/auth" -d acl
```



```
dn:uid=test1003  
cn:...  
sn:...  
uid:...  
userPassword:...  
XXX:...
```

-D オプション



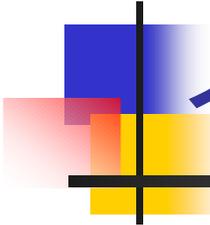
-b オプション

認証処理の為の
アクセスは可能か？

slapaclの使い方

- -bオプション
 - 検証対象のエントリ。“誰の“に相当する部分
- -Dオプション
 - 検証対象のユーザ。“誰に“に相当する部分
 - 省略時は、匿名(Anonymous)ユーザとなる
- 検証対象の属性値/検証対象の処理

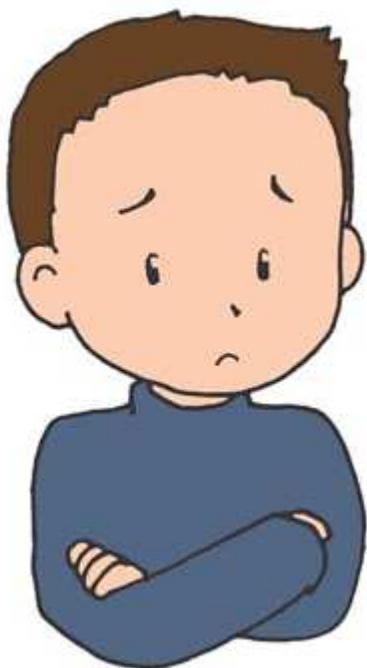
```
# slapacl -b "uid=test1003,ou=people,dc=my-domain,dc=com" "userPassword/auth" -d acl
```



インデックス管理

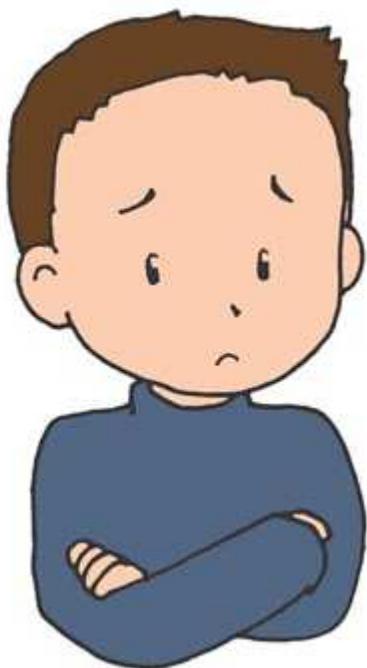
-slapindex

インデックス管理



- OpenLDAP (ディレクトリサーバ)は、大量のエントリ情報を蓄積することもある。また、検索される方式に対応できるようにしっかりとインデックス用意しておきたい
- 設定ファイル上のインデックス設定を変更したけど、それだけで良いの？
- 利用していないインデックスファイルが残っているけど、どうすれば良いの？

インデックス管理



- OpenLDAPの設定ファイル上のインデックス設定を変更したけれども、既存のインデックスファイルは変更されていないし、また、該当の検索処理のスピードもアップしていない

既存データに対し、**slapindex**コマンドを利用し、**OpenLDAP**の設定ファイルに指定された通りのインデックスの再構築が可能になる！

解決

slapindex

- slapindex を利用したインデックス再構築
 1. OpenLDAPサーバの停止
 2. slapd.confの index を更新
 3. slapindexを実行

```
# slapindex -b dc=my-domain,dc=com -v
```

```
indexing id=00000001
```

```
indexing id=00000002
```

```
indexing id=00000003
```

```
indexing id=00000004
```

```
...[略]...
```

属性名.bdb

cn.bdb

ou.bdb

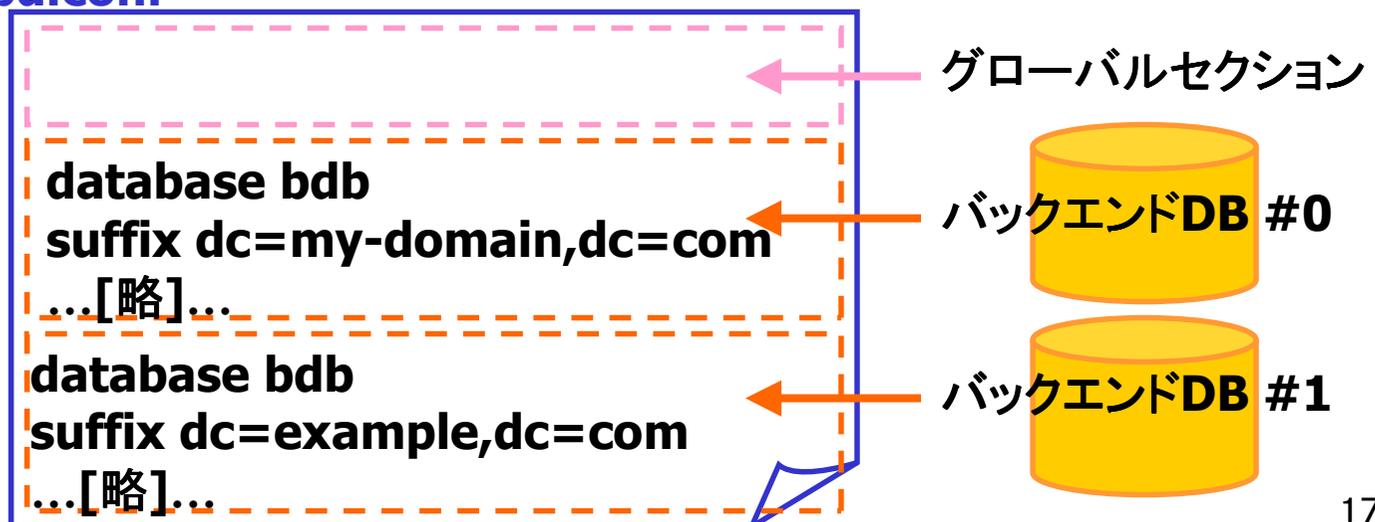
xx.bdb

yy.bdb

slapindexの使い勝手

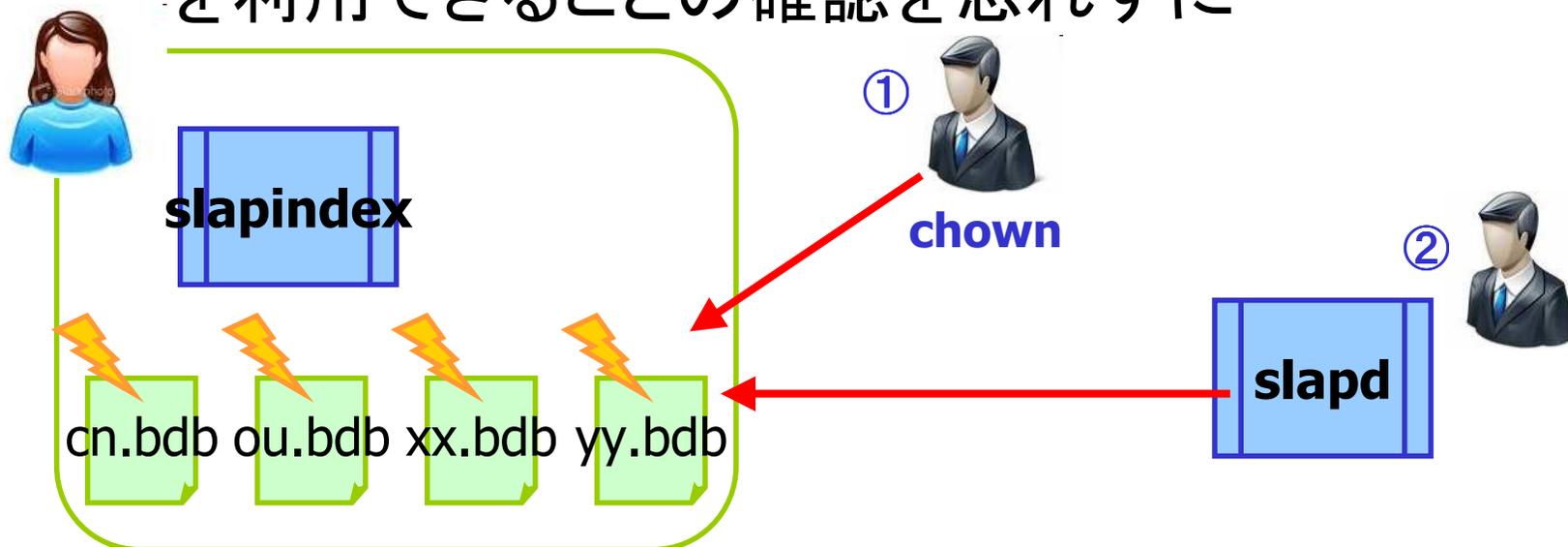
- slapindexのデフォルト動作は、slapd.confに記述された最初に利用可能なバックエンドDBを対象にインデックスを構築
- -bオプションでのsuffix指定が、明示的で安心

slapd.conf



slapindexの使い勝手 (2)

- slapindexは、slapindexの実行ユーザでインデックスファイルを作成
- OpenLDAP実行ユーザが、インデックスファイルを利用できることの確認を忘れずに

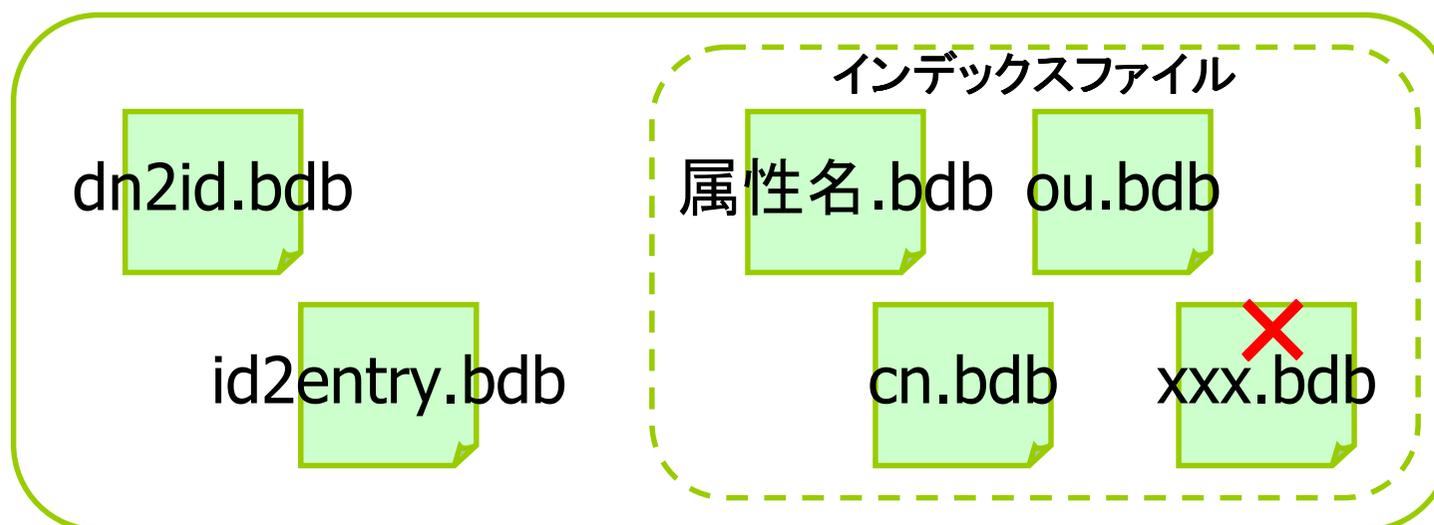


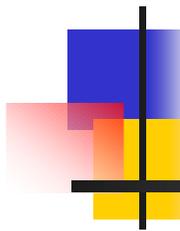
slapindexでは、“-u ユーザ”オプションが利用できない

解決

利用しなくなったインデックス ファイルのメンテナンス

- 不要なインデックスファイルの削除
 1. OpenLDAPサーバを停止
 2. slapd.confの index の更新
 3. 不要なインデックスファイルの削除

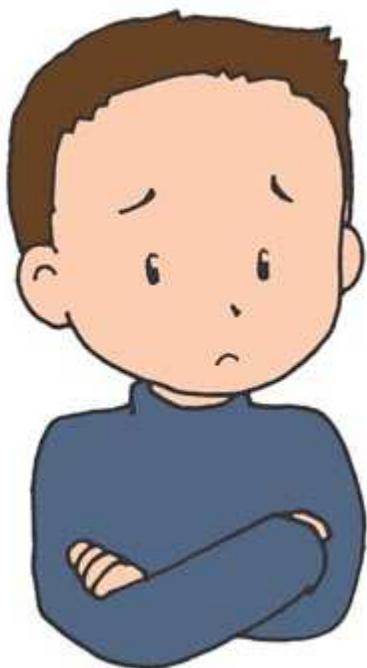




バックアップ、リカバリ

- slapcat
- slapadd

バックアップ、リカバリ



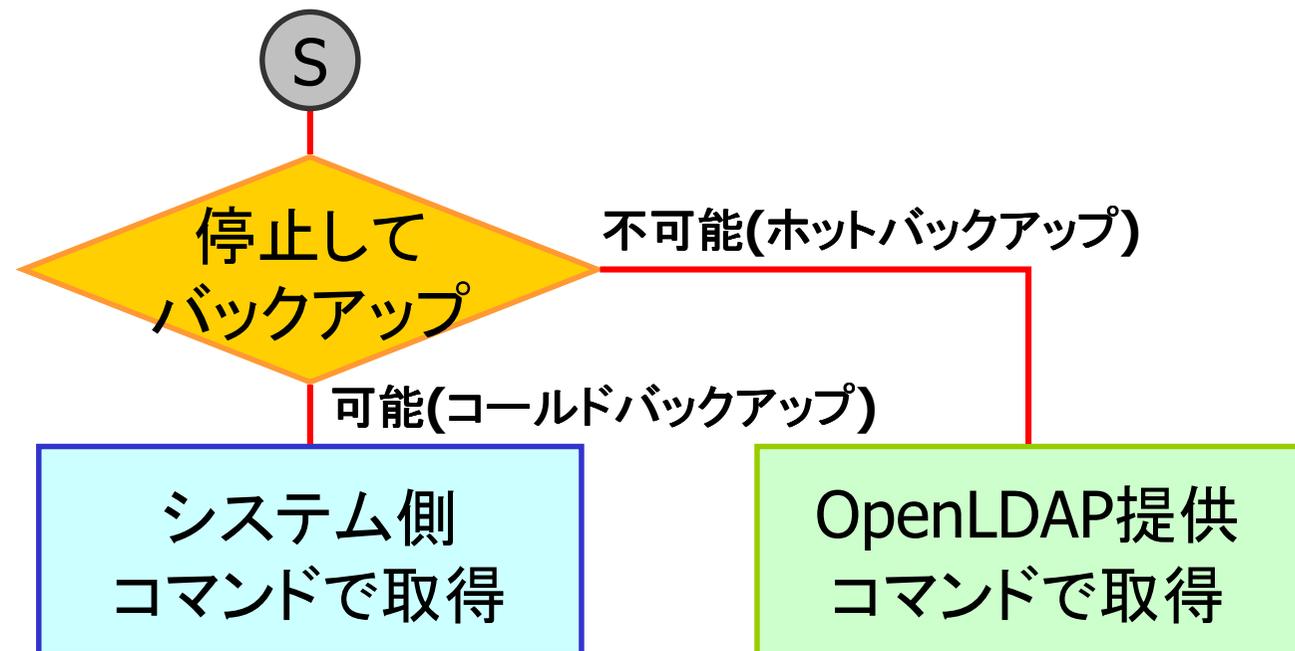
- OpenLDAP (ディレクトリサーバ)は、企業内で様々なシステムと連携する大切なデータが蓄積されている為、万が一に備えてバックアップ、リカバリ手法を確立しておきたい
- ある時点のデータを、2次媒体に保存しておきたい
- 随時更新されるレプリケーション構成でなく、ある時点のデータに戻せるようにしておきたい

背景

バックアップ、リカバリ



- OpenLDAPを運用している環境、提供するサービスレベルに合わせたバックアップ、リカバリ手法が確立したい



参考

コールドバックアップする Berkeley DBファイルの目安

必須	ファイル名	役割
◎	DB_CONFIG	Berkeley DBの設定ファイル
×	__db.[00X]	Berkeley DBが共有利用するメモリ領域がマップされたファイル
○	alock	OpenLDAPがBerkeley DBの重複利用や正常停止を管理するファイル
◎	dn2id.bdb、id2entry.bdb	OpenLDAPのエントリ情報を蓄積するデータファイル。OpenLDAPではメインのデータファイル
◎	log.[000000000X]	Berkeley DBのトランザクションログファイル。最新の1ファイルは必須
○	[インデックス指定属性名].bdb	OpenLDAPのインデックス情報を蓄積するデータファイル

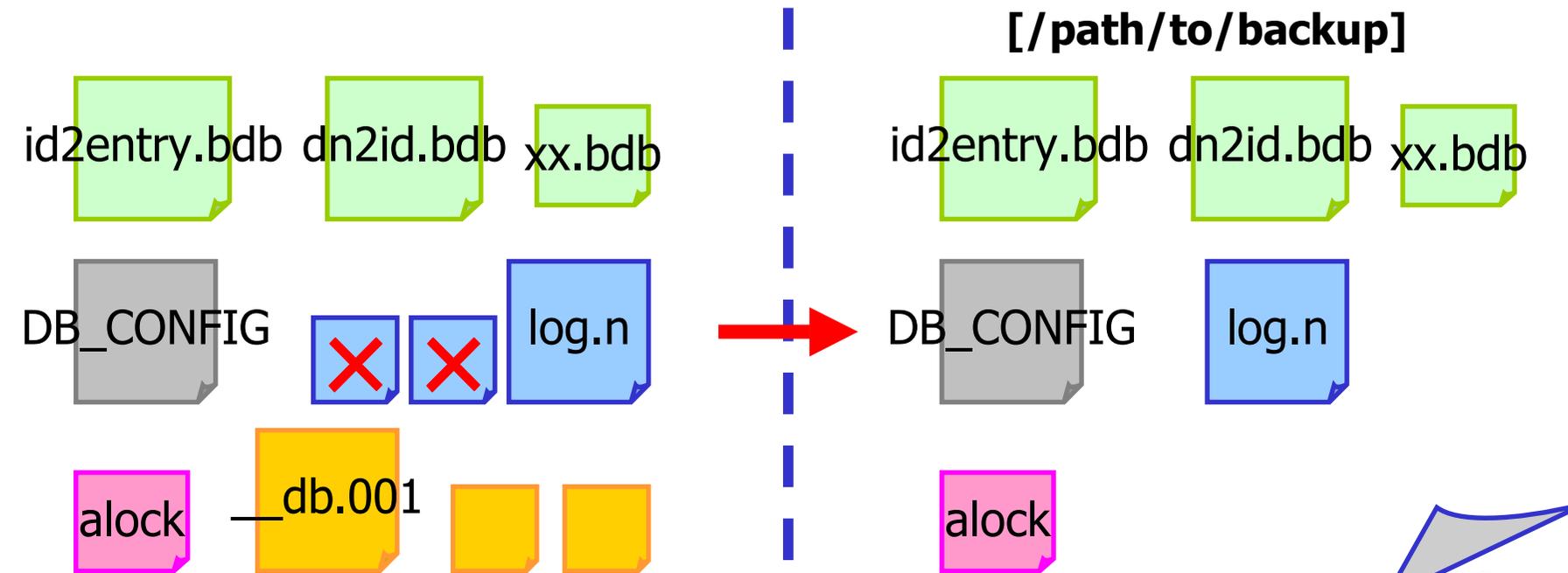
- OpenLDAPの設定ファイルslapd.conf、変更があればスキーマファイルも忘れずに 23

解決

Berkeley DB関連ファイルの コールドバックアップ

- OpenLDAPを停止してバックアップ

```
# cp -p DB_CONFIG alock *.bdb log.* /path/to/backup
```

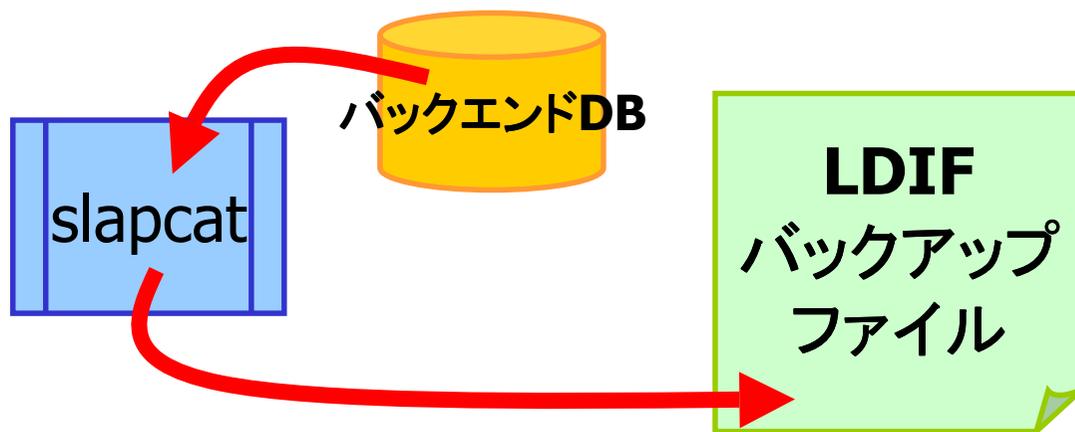


解決

slapcat (ホットバックアップ)

- OpenLDAP起動中にバックアップ
 - ディレクトリデータをLDIF(LDAPでのデータ交換用フォーマット)形式でファイルへ抽出

```
# slapcat -b suffix -l /path/to/backup.ldif
```



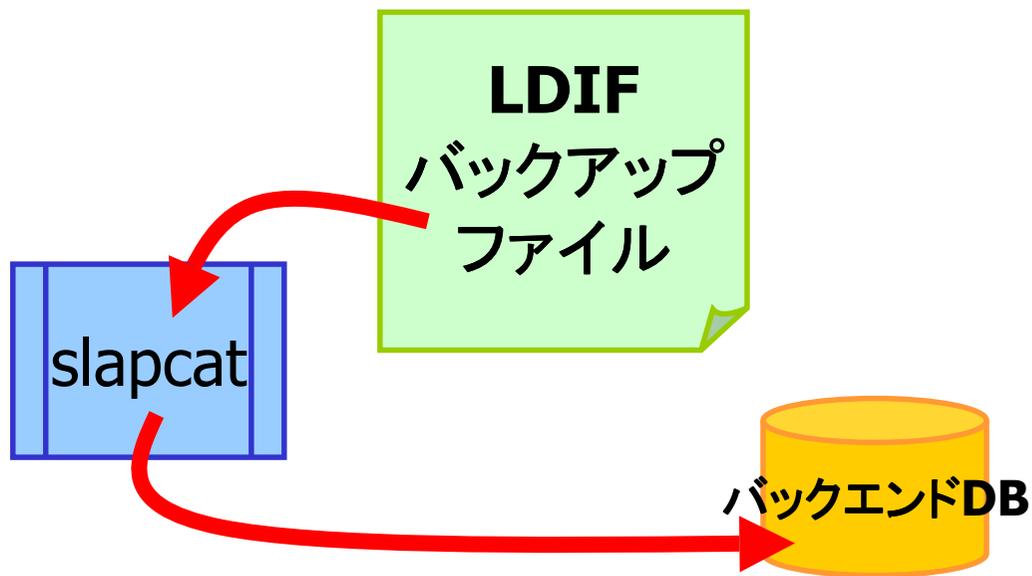
- slapd.conf、DB_CONFIGに加え、変更があった場合スキーマファイルも忘れずに

解決

slapadd (ホットバックアップからのリストア)

- OpenLDAPを停止してリストア
 - LDIF形式のディレクトリデータをリストア

```
# slapadd -b suffix -l /path/to/backup.ldif
```



- slapd.conf、DB_CONFIG、スキーマファイルを、slapaddの実行より先にリストア

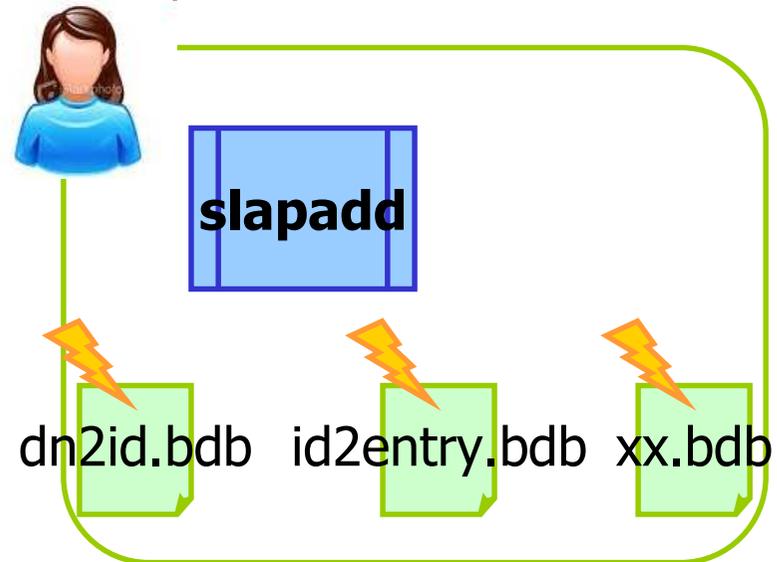
slapcat、slapaddの使い勝手

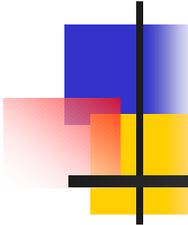
- slapcat、slapaddでは、-bオプションでのsuffix指定が、明示的で安心
- slapaddの実行後は、ファイルの所有権に注意

slapd.conf

```
database bdb  
suffix dc=my-domain,dc=com  
...[略]...
```

```
database bdb  
suffix dc=example,dc=com  
...[略]...
```

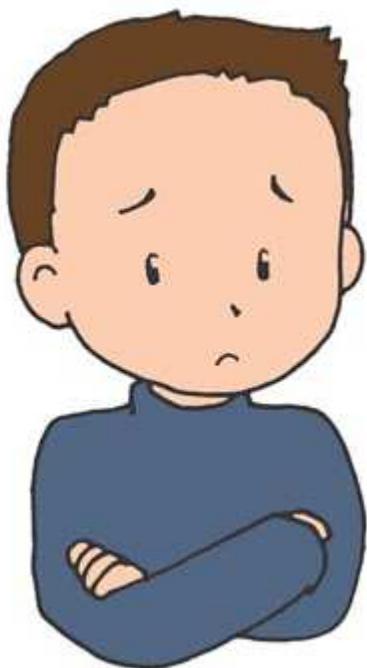




ログ管理

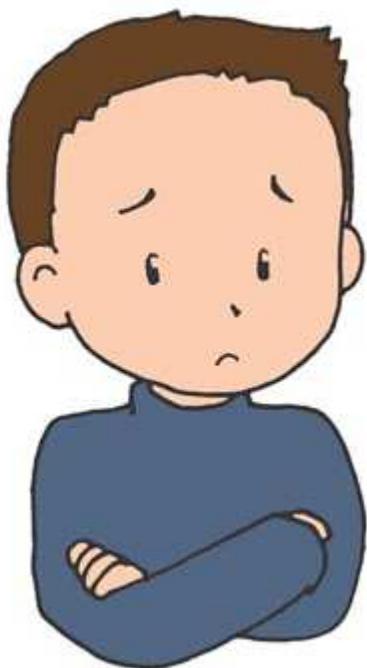
- syslog
- logrotate

ログ出力



- OpenLDAP (ディレクトリサーバ)は、企業内で様々なシステムと連携する大切なサーバの1つ。大切なサーバだからこそ、不都合がないかを把握できるようにしておきたい
 - 不都合があっても、ものを言わないサーバだからこそログを出力させ管理したい
 - デフォルトでは、どこにログが出力されているか分からない

ログ出力



- OpenLDAPの設定ファイル上でログ(loglevel)の設定を行ったけれど、どこにもログが出力されていない
 - ログ出力されないのは正しい動作？

OpenLDAPでは、デフォルトではログが記録されない為、ログを記録させる為の設定が必要！

Step 1. ログ取得の準備

- OpenLDAPは、デフォルトでLOCAL4ファシリティを用いてログメッセージを送付
- syslog側で、LOCAL4ファシリティログを受け取る設定が必要
 - # vi /etc/syslog.conf

...[略]...

```
local4.*                /var/log/ldap.log
```

...[略]...

- syslog 再起動

解決

Step 2. ログ送信の準備

- ログの出力内容(レベル)を設定
 - # vi slapd.conf

グローバル
セクション

```
include...  
...[略]...  
loglevel 256  
...[略]...
```

loglevelディレクティブを指定
しない場合でも、デフォルトの
256(0x100、stats)となる。

バックエンドDB
セクション

- slapd 再起動

参考

ログ出力内容(レベル)一覧

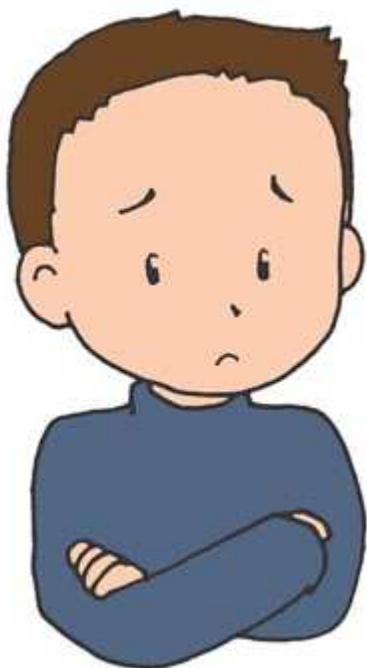
Level (10進数)	Level (16進数)	Level (文字列)	説明
✓ -1		any	enable all debugging
0	0x0		no debugging
1	0x1	trace	trace function calls
2	0x2	packet	debug packet handling
4	0x4	args	heavy trace debugging (function args)
8	0x8	conns	connection management
16	0x10	BER	print out packets sent and received
32	0x20	filter	search filter processing

参考

ログ出力内容(レベル)一覧(2)

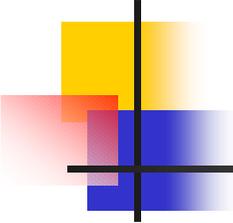
Level (10進数)	Level (16進数)	Level (文字列)	説明
✓ 64	0x40	config	configuration file processing
✓ 128	0x80	ACL	access control list processing
✓ 256	0x100	stats	stats log connections/operations/results
512	0x200	stats2	stats log entries sent
1024	0x400	shell	print communication with shell backends
2048	0x800	parse	entry parsing
16384	0x4000	sync	LDAPSync replication
32768	0x8000	none	only messages that get logged whatever log level is set

ログの活用



- ログが記録されるようになったけど、活用しなければ、ディスク容量を圧迫し、また、時間のかかるディスクI/Oを伴い性能を劣化させるだけ
- ログを見る時のポイントは？

OpenLDAPのログを見るコツを理解すれば、トラブル対応時にも役立ちます！



loglevel 256 でのログ出力

- Idapsearchを実行しログ出力を確認
 - Idapsearch -x -D DN -w passwd filter attr

```
# Idapsearch -x -D uid=test1001,ou=people,dc=my-domain,dc=com -w 3edcvfr4 uid=test1001 dn -LLL  
dn: uid=test1001,ou=People,dc=my-domain,dc=com
```

- tail -f /var/log/ldap.log

```
Feb 14 04:39:44 CentOSa slapd[9733]: conn=5 fd=13 ACCEPT from IP=127.0.0.1:38379 (IP=0.0.0.0:389)  
Feb 14 04:39:44 CentOSa slapd[9733]: conn=5 op=0 BIND dn="uid=test1001,ou=people,dc=my-domain,dc=com" method=128  
Feb 14 04:39:44 CentOSa slapd[9733]: conn=5 op=0 BIND dn="uid=test1001,ou=People,dc=my-domain,dc=com" mech=SIMPLE ssf=0  
Feb 14 04:39:44 CentOSa slapd[9733]: conn=5 op=0 RESULT tag=97 err=0 text=  
Feb 14 04:39:44 CentOSa slapd[9733]: conn=5 op=1 SRCH base="dc=my-domain,dc=com" scope=2 deref=0 filter="(uid=test1001)"  
Feb 14 04:39:44 CentOSa slapd[9733]: conn=5 op=1 SRCH attr=dn  
Feb 14 04:39:44 CentOSa slapd[9733]: conn=5 op=1 SEARCH RESULT tag=101 err=0 nentries=1 text=  
Feb 14 04:39:44 CentOSa slapd[9733]: conn=5 op=2 UNBIND  
Feb 14 04:39:44 CentOSa slapd[9733]: conn=5 fd=13 closed
```

解決

Step 1. 処理フローの把握

■ ログの左側部分に着目

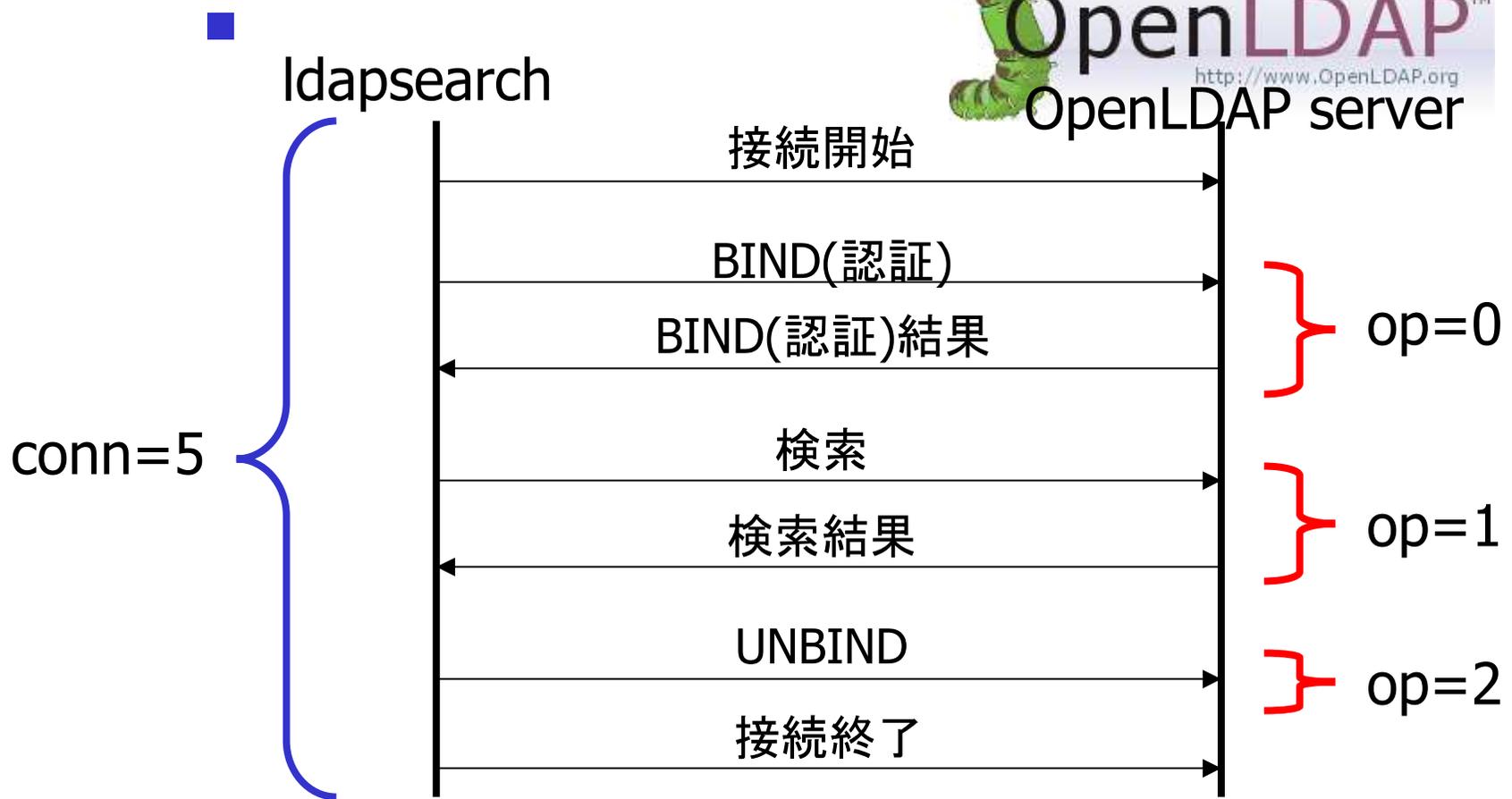
日時	ホスト	プロセス	conn=5	fd=13
Feb 14 04:39:44	CentOSa	slapd[9733]	conn=5	fd=13
Feb 14 04:39:44	CentOSa	slapd[9733]	conn=5	op=0 BIND ...
Feb 14 04:39:44	CentOSa	slapd[9733]	conn=5	op=0 BIND ...
Feb 14 04:39:44	CentOSa	slapd[9733]	conn=5	op=0 RESULT
Feb 14 04:39:44	CentOSa	slapd[9733]	conn=5	op=1 SRCH ...
Feb 14 04:39:44	CentOSa	slapd[9733]	conn=5	op=1 SRCH ...
Feb 14 04:39:44	CentOSa	slapd[9733]	conn=5	op=1 SEARCH
Feb 14 04:39:44	CentOSa	slapd[9733]	conn=5	op=2 UNBIND
Feb 14 04:39:44	CentOSa	slapd[9733]	conn=5	fd=13 closed ...

① conn# (connection 番号) が同一の出力をピックアップし、追跡すること

② 同一conn# 中で増加する op# (operation 番号) より処理フローの概要を掴むこと

解決

Step 1. で確認できた処理フロー



解決

Step 2. 処理内容と結果の把握

■ ログの右側部分に着目

```
fd=13 ACCEPT from IP=127.0.0.1:38379 (IP=0.0.0.0)
-----
op=0 BIND dn="uid=test1001,ou=people,dc=my-domain,dc=com" method=128
op=0 BIND dn="uid=test1001,ou=People,dc=my-domain,dc=com" mech=SIMPLE ssf=0
op=0 RESULT tag=97 err=0 text=
-----
op=1 SRCH base="dc=my-domain,dc=com" scope=2 deref=
op=1 SRCH attr=dn
op=1 SEARCH RESULT tag=101 err=0 nentries=1 text=
-----
op=2 UNBIND
-----
fd=13 closed
```

③カテゴリ分けした処理内容の詳細を把握すること

④各処理毎に、対応する結果を確認すること

解決

Step 2.で確認できた処理と結果



参考

今すぐ使える 便利ツール、statslog

- ログを整形する便利ツール
 - contrib/slapd-tools ディレクトリにあるperlスクリプト
 - loglevel 256 (stats)で出力されたログをコネクション番号をベースにソートし直す便利ツール
 - コネクションが入り乱れているログで便利
 - 正規表現を用いて、欲しいログを選択可能
- 使い方は、

```
# cd openldap-2.4.XX/contrib/slapd-tools  
# ./statslog --usage
```

参考

今すぐ使える 便利ツール、statslog

- 例) 2月に認証に失敗しているTLS接続は...

```
# cd openldap-2.4.XX/contrib/slapd-tools
```

```
# ./statslog -i ^Feb.*err=49 -i TLS /var/log/ldap.log
```

```
Feb 7 00:28:51 CentOSa slapd[7376]: conn=3 fd=15 ACCEPT from IP=127.0.0.1:52996 (IP=0.0.0.0:636)
```

```
Feb 7 00:28:52 CentOSa slapd[7376]: conn=3 fd=15 TLS established tls_ssf=256 ssf=256
```

```
Feb 7 00:28:52 CentOSa slapd[7376]: conn=3 op=0 BIND dn="cn=Manager,dc=my-domain1,dc=com" method=128
```

```
Feb 7 00:28:52 CentOSa slapd[7376]: send_ldap_result: conn=3 op=0 p=3
```

```
Feb 7 00:28:52 CentOSa slapd[7376]: conn=3 op=0 RESULT tag=97 err=49 text=
```

```
Feb 7 00:28:52 CentOSa slapd[7376]: connection_closing: readying conn=3 sd=15 for close
```

```
Feb 7 00:28:53 CentOSa slapd[7376]: conn=3 fd=15 closed (connection lost)
```

```
Feb 14 05:57:14 CentOSa slapd[9978]: conn=0 fd=15 ACCEPT from IP=127.0.0.1:50294 (IP=0.0.0.0:636)
```

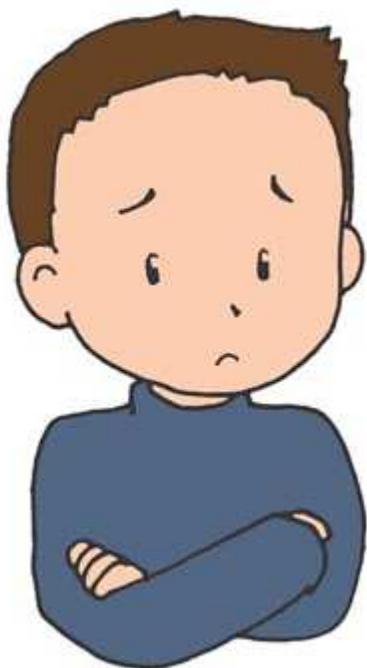
```
Feb 14 05:57:14 CentOSa slapd[9978]: conn=0 fd=15 TLS established tls_ssf=256 ssf=256
```

```
Feb 14 05:57:14 CentOSa slapd[9978]: conn=0 op=0 BIND dn="uid=test1001,ou=people,dc=my-domain,dc=com" method=128
```

```
Feb 14 05:57:14 CentOSa slapd[9978]: conn=0 op=0 RESULT tag=97 err=49 text=
```

```
Feb 14 05:57:14 CentOSa slapd[9978]: conn=0 fd=15 closed (connection lost)
```

ログ削除



- 日々延々と増えるOpenLDAPログは、ディスクを圧迫している要因に
- syslogに送ったログは、どうするの？

OpenLDAPがsyslogに送ったログは、そのままでは削除されない為、何らかの方法で定期的なメンテナンスを行う必要がある！

logrotate

- 例えば、logrotateに任せる

```
# vi /etc/logrotate.d/syslog
```

```
/var/log/ldap.log /var/log/messages ... /var/log/cron {
```

```
sharedscripts
```

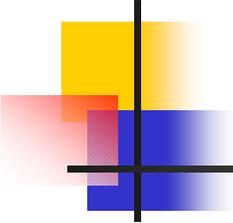
```
postrotate
```

```
    /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> ...
```

```
    /bin/kill -HUP `cat /var/run/rsyslogd.pid 2> /dev/null` 2> ...
```

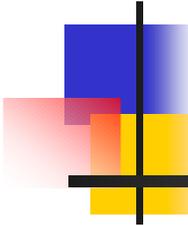
```
endscript
```

```
}
```



目次

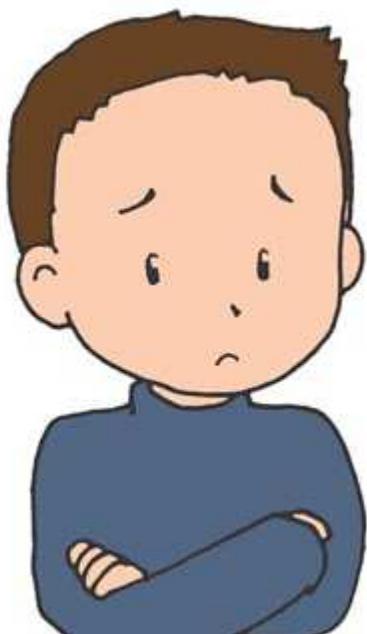
- OpenLDAPサーバ管理
- バックエンドDB(**Berkeley DB**)管理
 - 設定ファイル
 - 統計情報
 - トランザクションログ管理
 - バックアップ、リカバリ
- GUI管理ツール



Berkeley DB 設定ファイル

- DB_CONFIG

Berkeley DB 設定ファイル



- バックエンドデータベース Berkeley DB の設定ファイルが見当たらない
 - Berkeley DB の設定ファイルがないと、OpenLDAP 起動時に、毎回、警告が出力される
 - Expect poor performance って... 不安

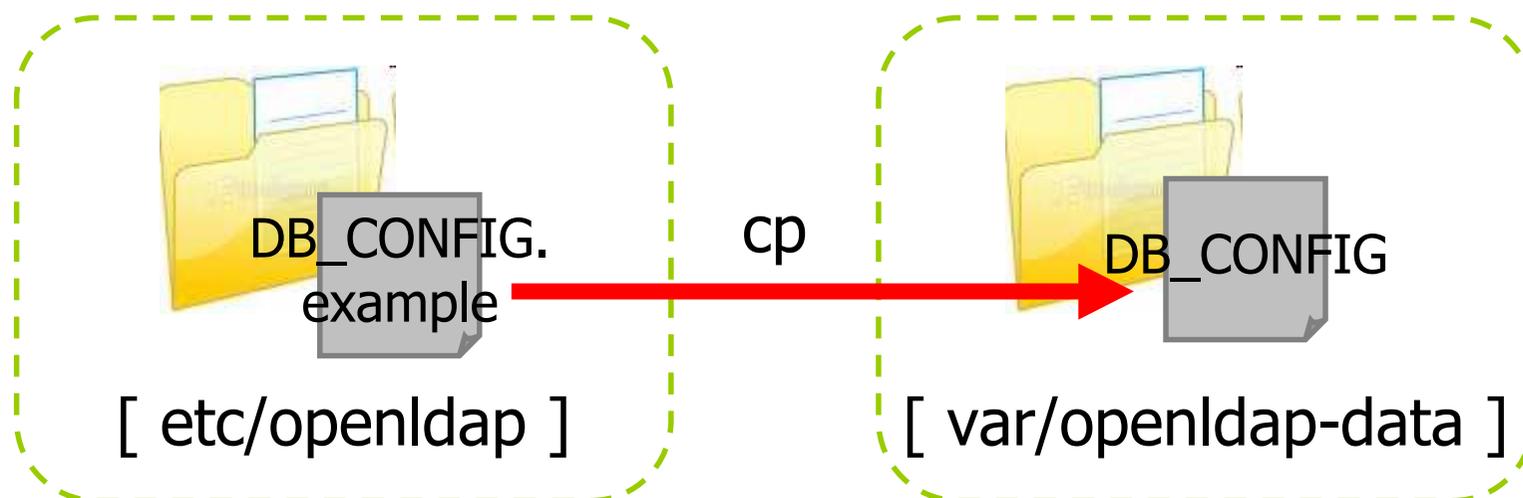
```
# tail -f /var/log/ldap.log
```

```
Oct 14 01:57:59 CentOS53a slapd[24651]: bdb_db_open: warning - no  
DB_CONFIG file found in directory /usr/local/openldap-2.4.16/var/openldap-data:  
(2). Expect poor performance for suffix "dc=my-domain,dc=com".
```

解決

サンプルファイルのコピー

- デフォルトでは、Berkeley DBの設定ファイルは存在しない
- サンプルファイルで提供されるDB_CONFIG.exampleをコピーして利用可能

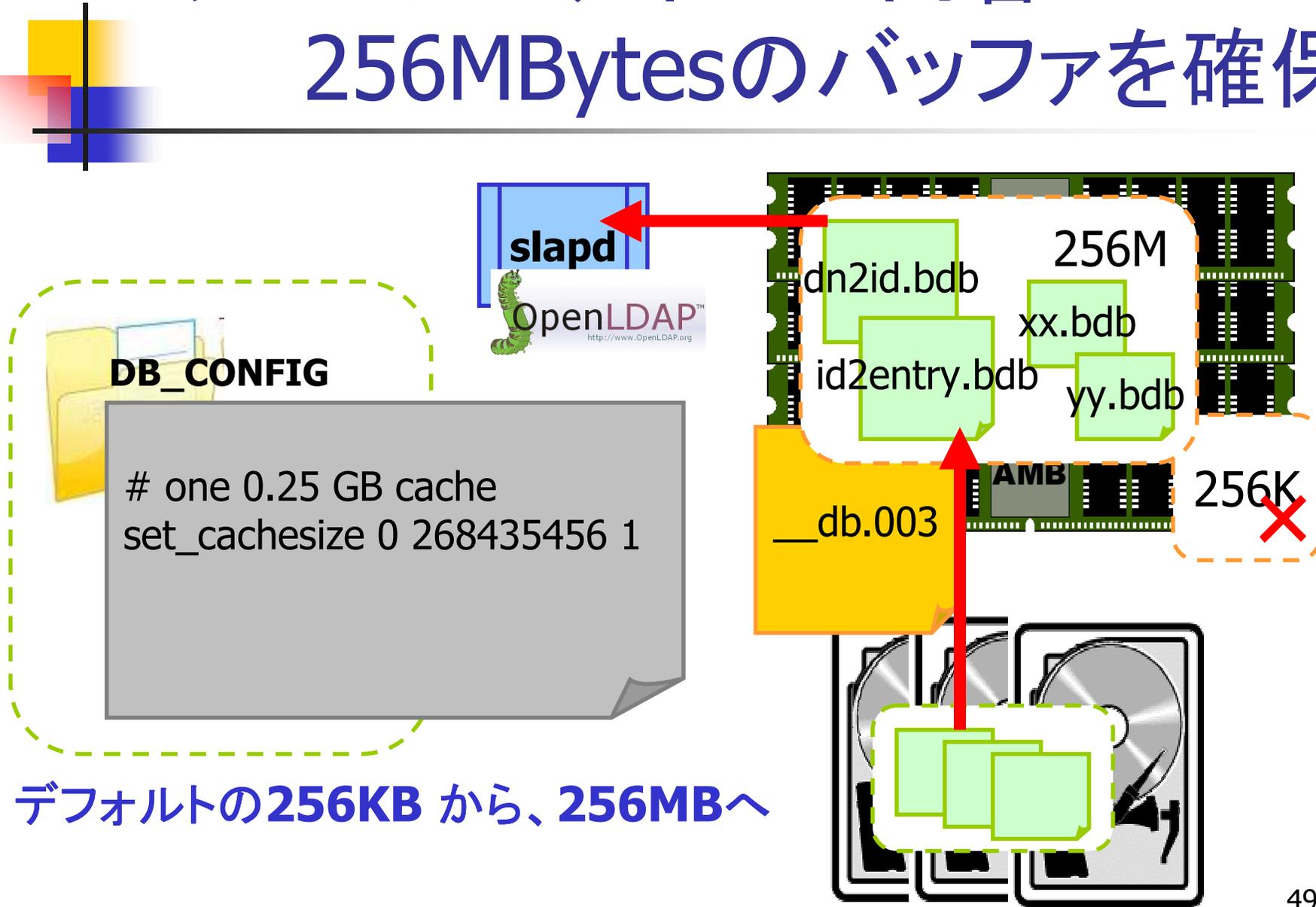


- cp後、slapd実行ユーザがDB_CONFIGファイルを利用できるよう所有権にも注意

解決

サンプルファイルの内容

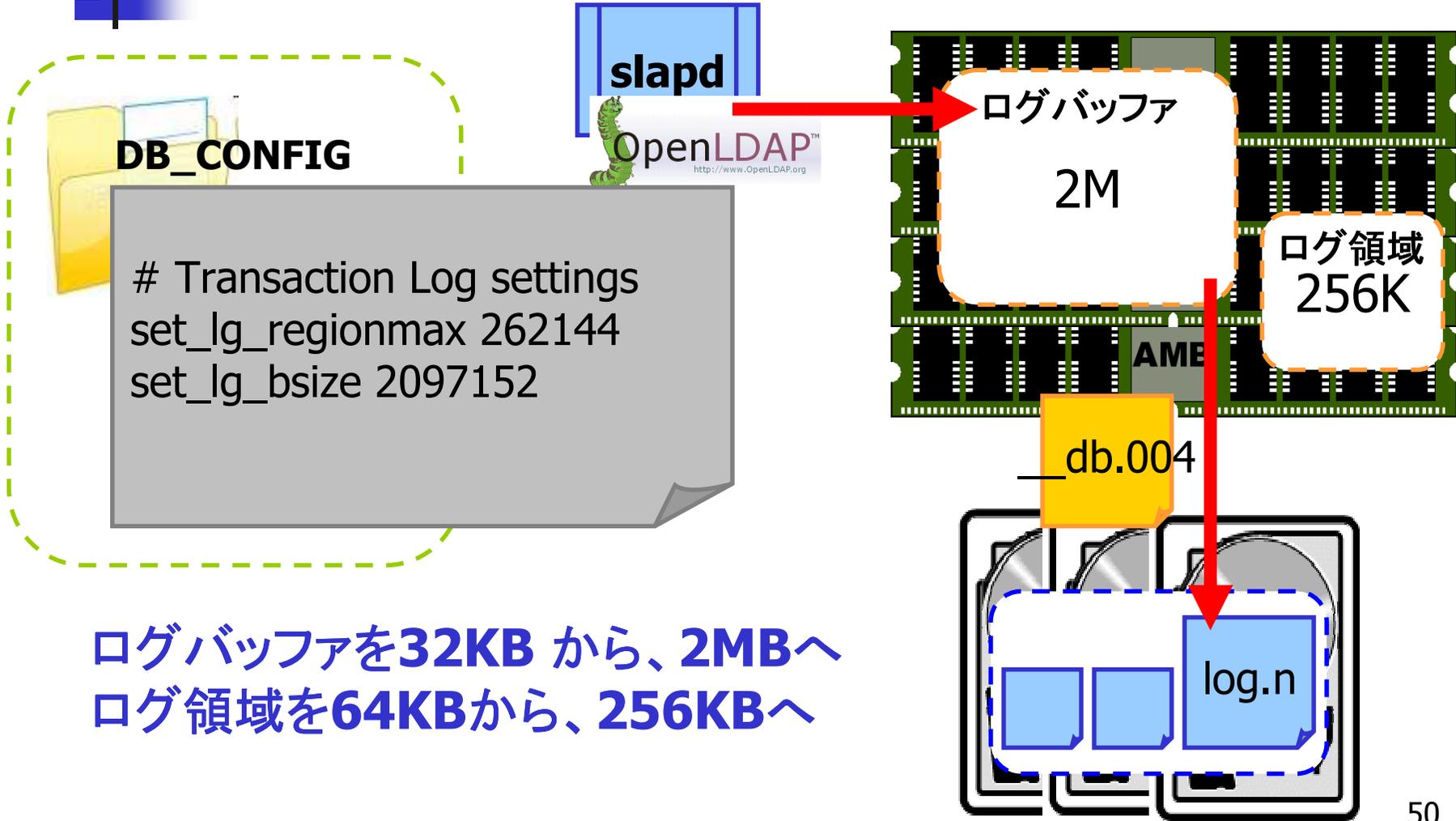
256MBytesのバッファを確保



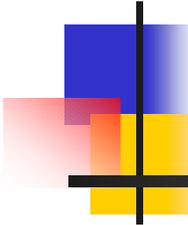
デフォルトの**256KB** から、**256MB**へ

参考

サンプルファイルの内容(2) 2MBのログバッファを確保



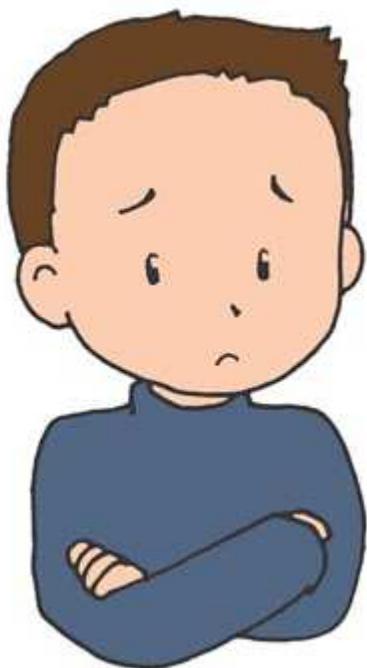
ログバッファを**32KB** から、**2MB**へ
ログ領域を**64KB**から、**256KB**へ



Berkeley DB 統計情報

- db_stat

Berkeley DB 統計情報

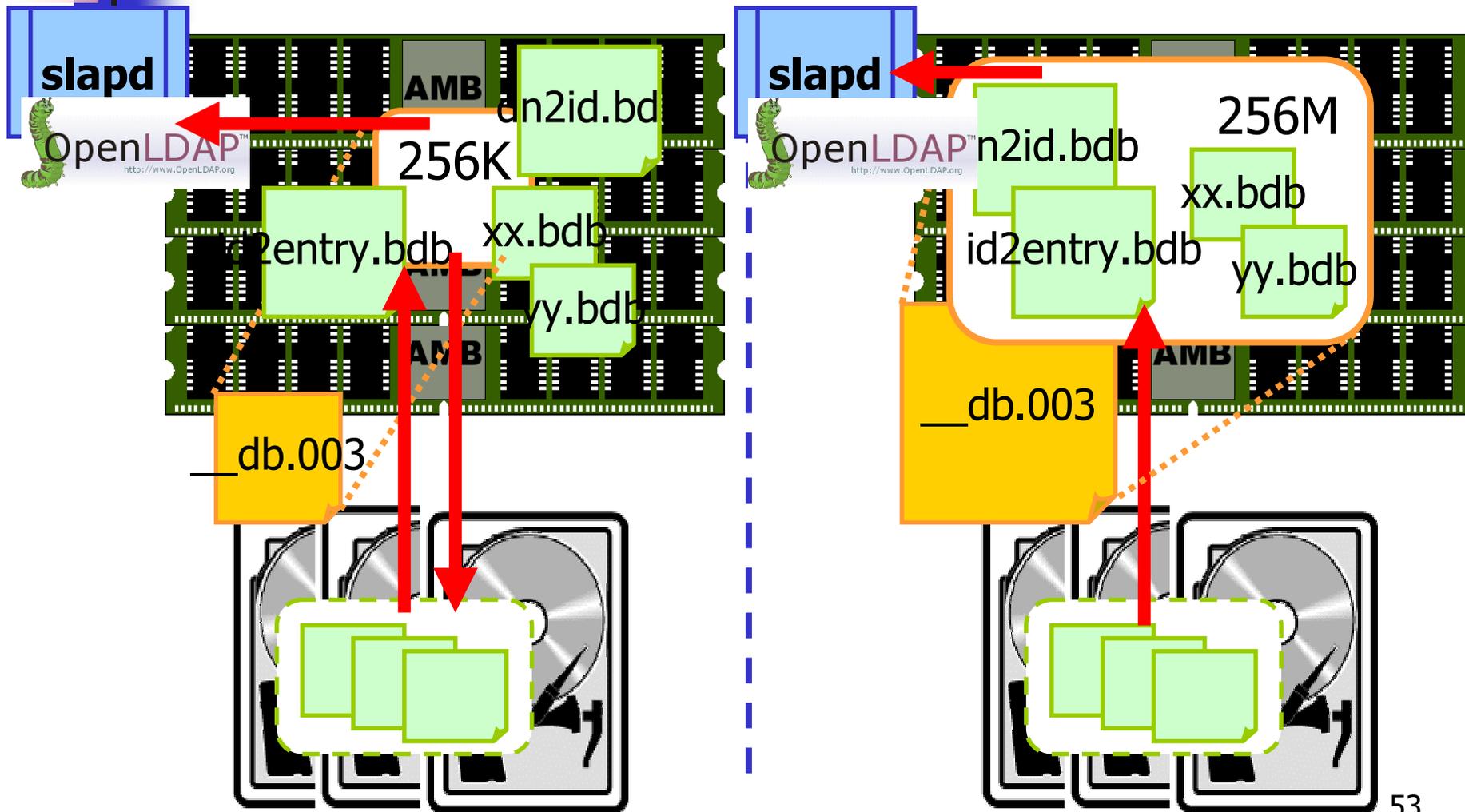


- サンプルのBerkeley DB設定ファイルをコピーしたけど、それでいいの？
 - サンプルファイルの値で大丈夫？
 - ハード資源をしっかりと利用できてる？

Berkeley DBに付属するツールを利用して、Berkeley DBの運用状況を把握することが可能！

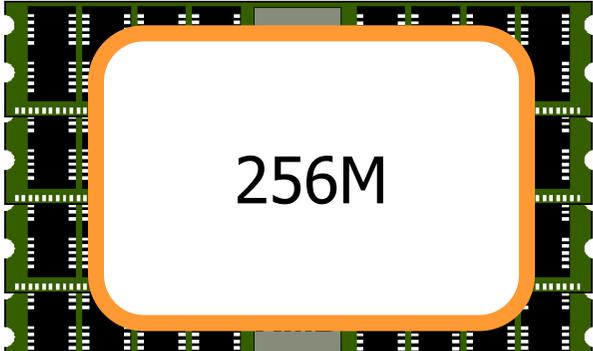
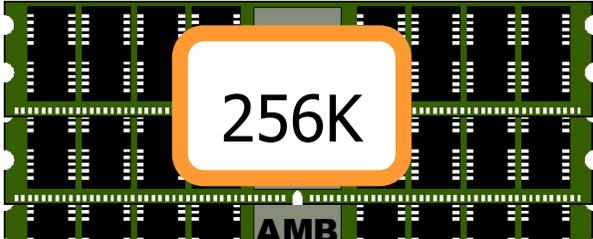
参考

256Kバッファと 256Mバッファからの読み込み



解決

db_stat -M A、または-m



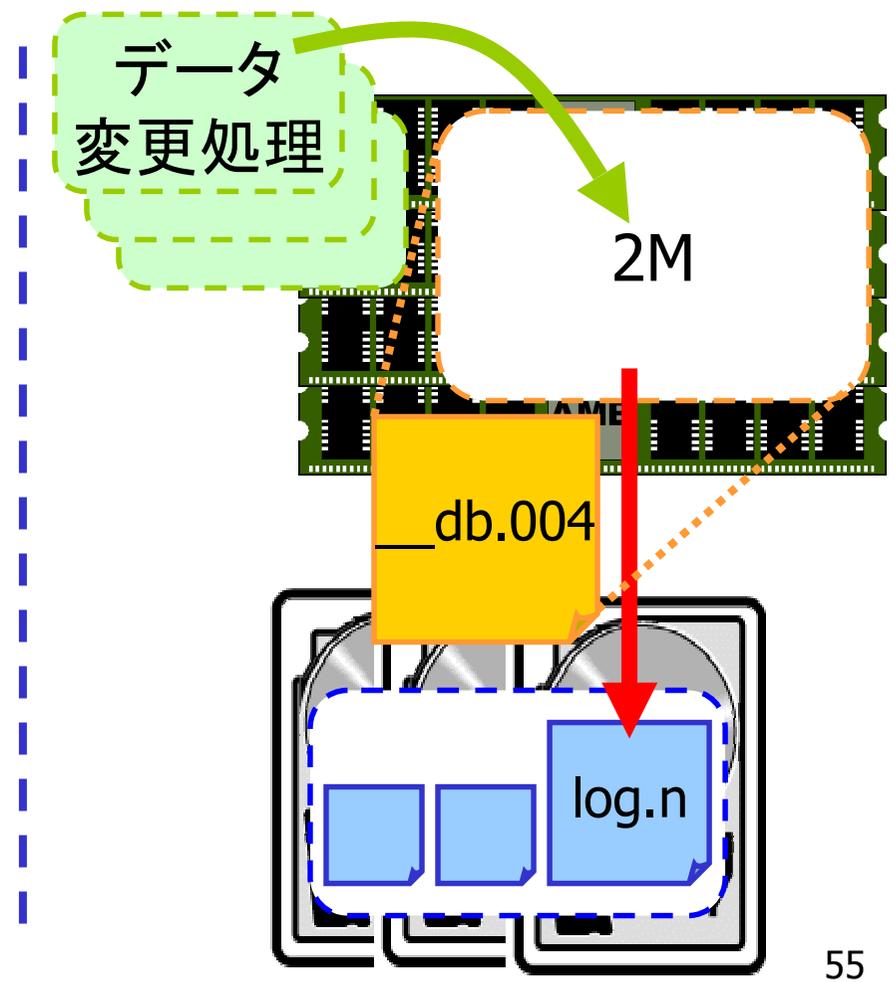
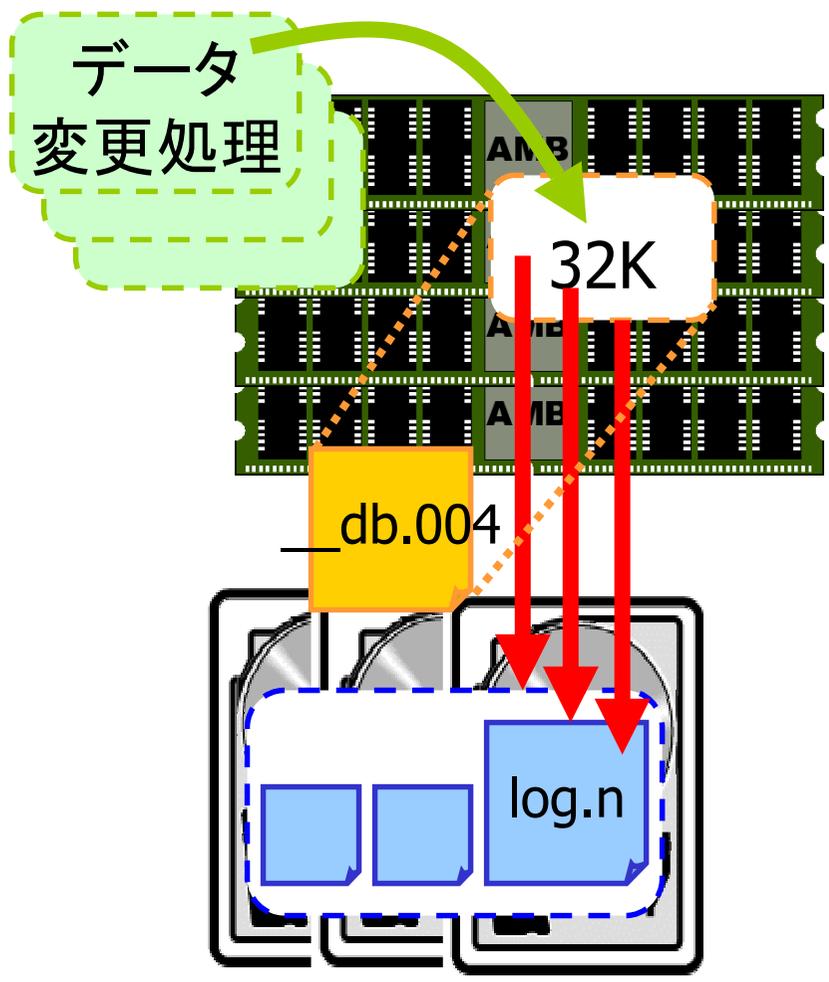
```
Pool File: id2entry.bdb
...[略]...
314017 Requested pages found in the cache (98%)
-----
Pool File: uid.bdb
...[略]...
10 Requested pages found in the cache (3%)
```

```
entry.bdb
...[略]...
Requested pages found in the cache (99%)
-----
db
...[略]...
243 Requested pages found in the cache (85%)
```

バッファヒット率の表示

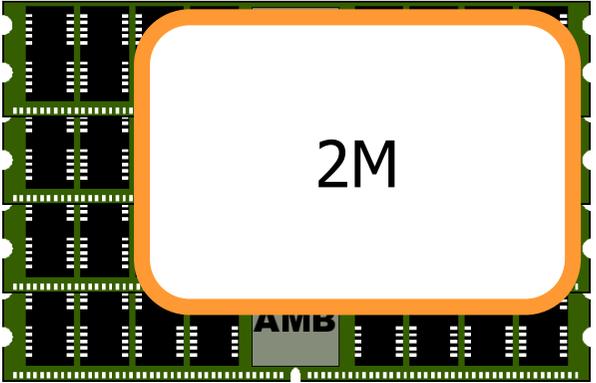
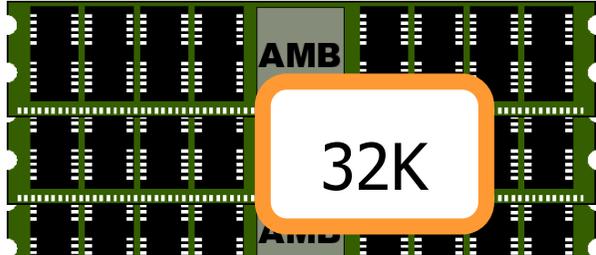
参考

32KBログバッファと 2MBログバッファへの書込み



解決

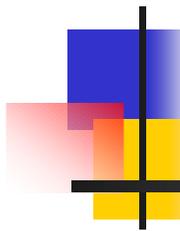
db_stat -L A、または-



```
31KB 256B      Log record cache size
...[略]...
1419374 Records entered into the
...[略]...
20147  Total log file I/O writes
103  Total log file I/O writes
20044  Total log file flushes
```

```
2MB      Log record cache size
...[略]...
1419374 Records entered into the log
...[略]...
20044  Total log file I/O writes
0    Total log file I/O writes due to overflow
20044  Total log file flushes
```

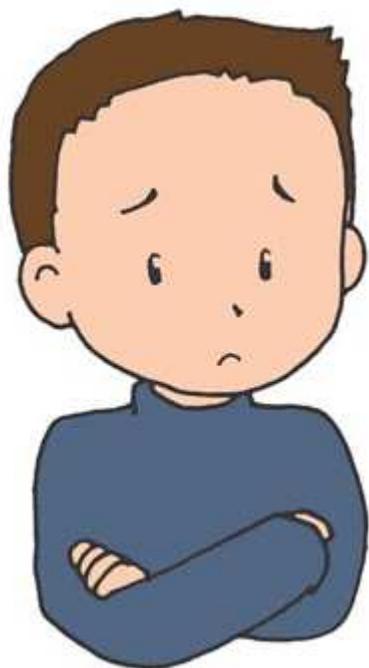
ログバッファのオーバーフローにより発生した書込み数の表示



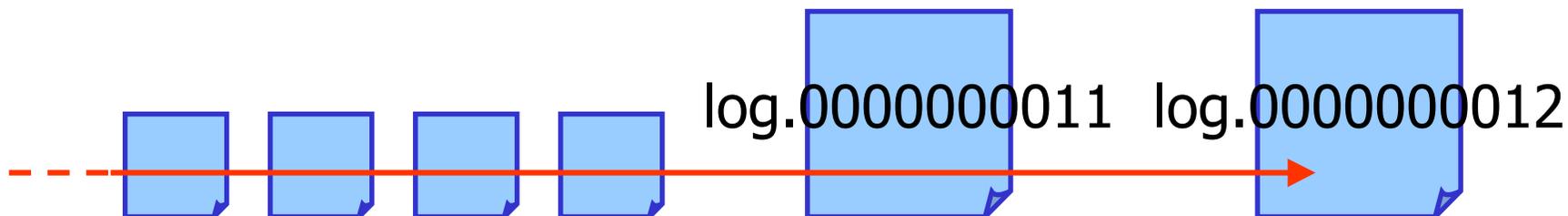
トランザクションログ管理

- db_checkpoint
- db_archive
- DB_CONFIG

トランザクションログ管理



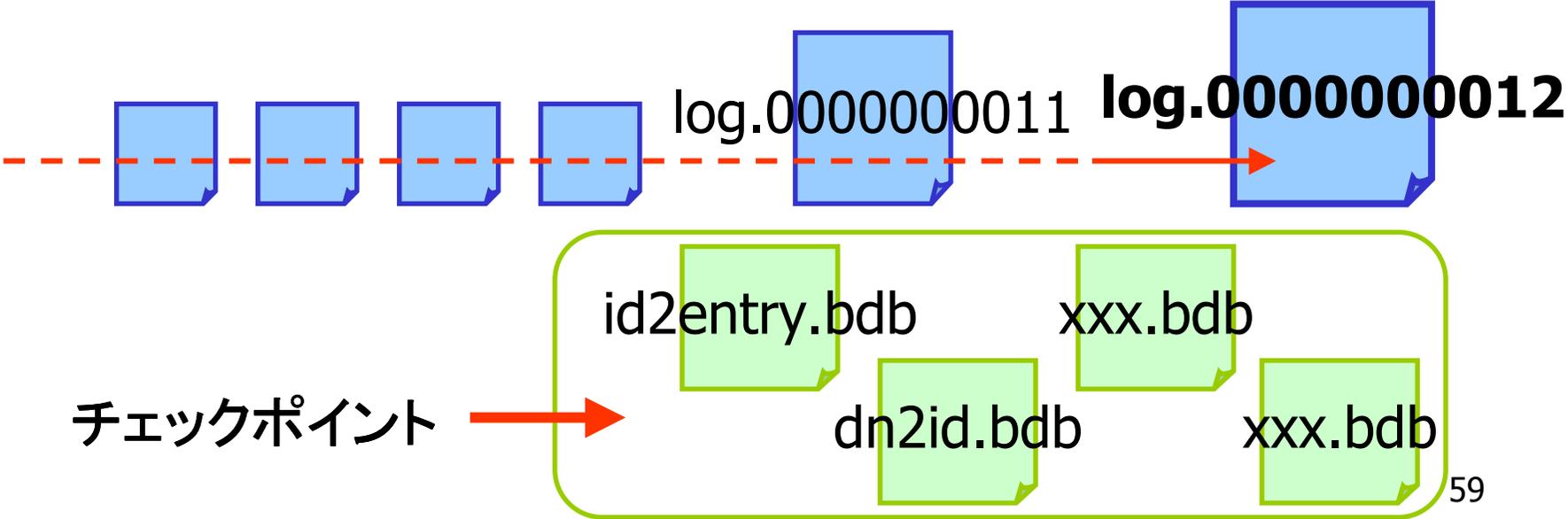
- OpenLDAPへの更新がある度に増えるBerkeley DBのトランザクションログファイルは、ディスクを圧迫している
 - デフォルトでは、削除されない
 - どのファイルを削除して良いか知りたい



参考

トランザクションログファイル 削除の基本ルール

- 次の3つを満たす場合、削除可能
 1. 実行中のトランザクションに関連しない
 2. 次のトランザクションファイルが作成され、チェックポイントが実行されている
 3. 唯一のトランザクションファイルでない



解決

トランザクション ログファイルの削除

- 削除可能なトランザクションログファイルの表示

```
# db_archive
```

- チェックポイントの実行と、削除可能ログの表示

```
# db_checkpoint -1; db_archive
```

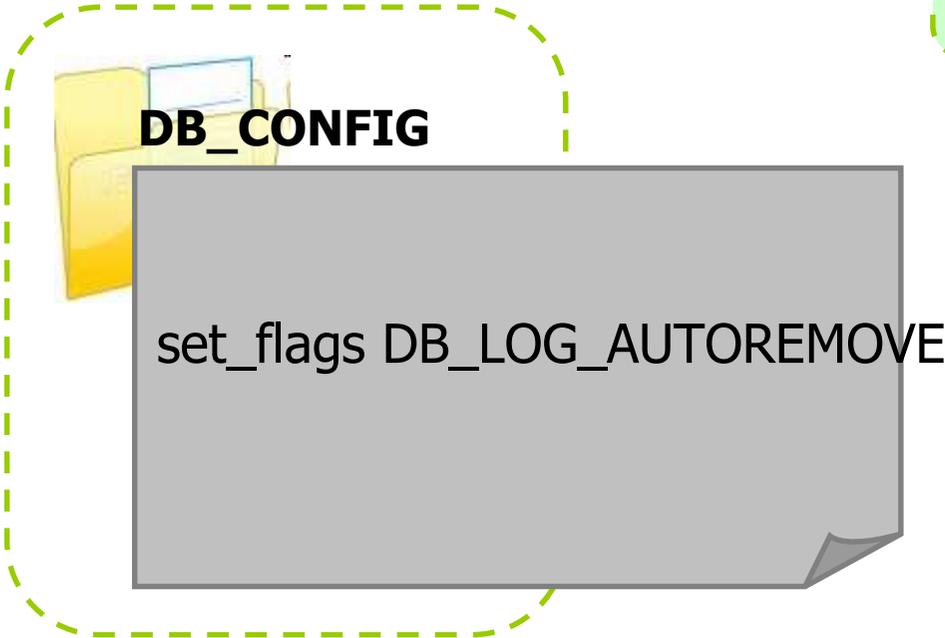
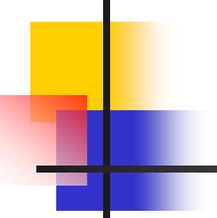
- トランザクションログファイルの削除

```
# db_archive -d
```

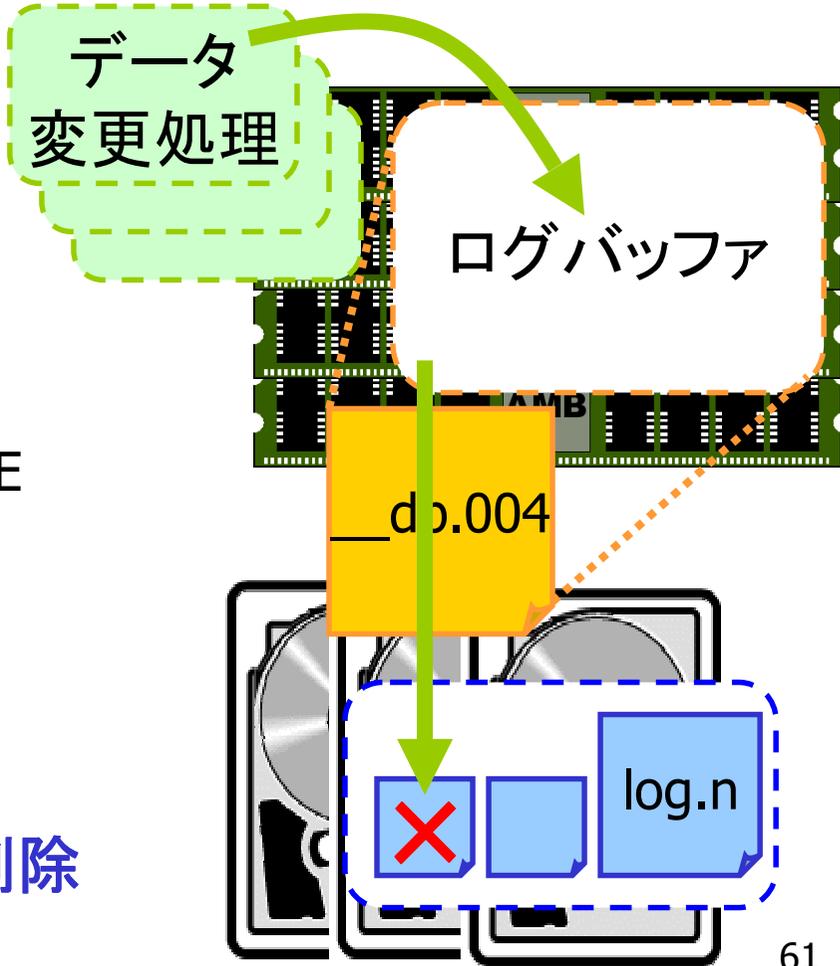
解決

トランザクション

ログファイルの自動削除



条件にマッチするファイルを自動削除





バックアップ、リカバリ

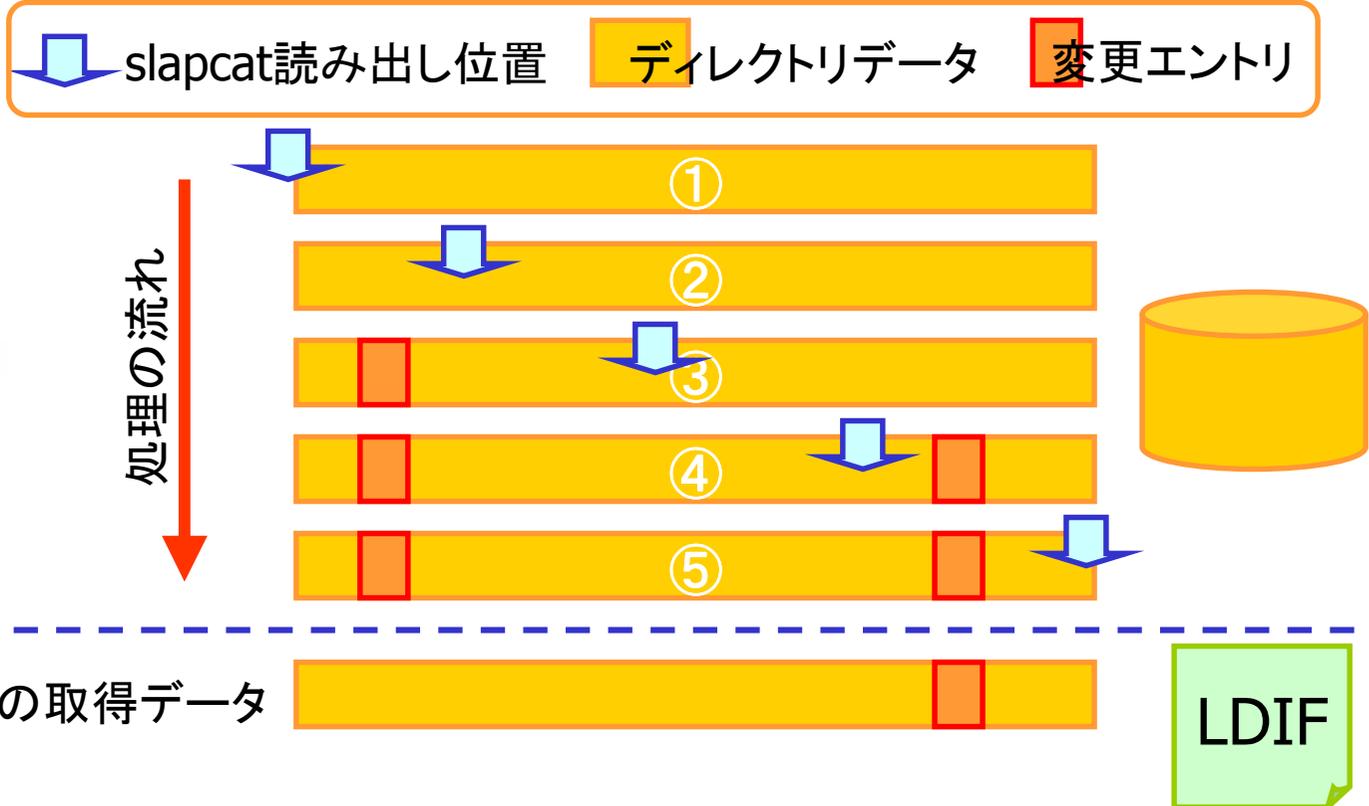
- db_hotbackup
- db_printlog
- db_recover

背景

バックアップ、リカバリ



- slapcatによるホットバックアップに、不満がある

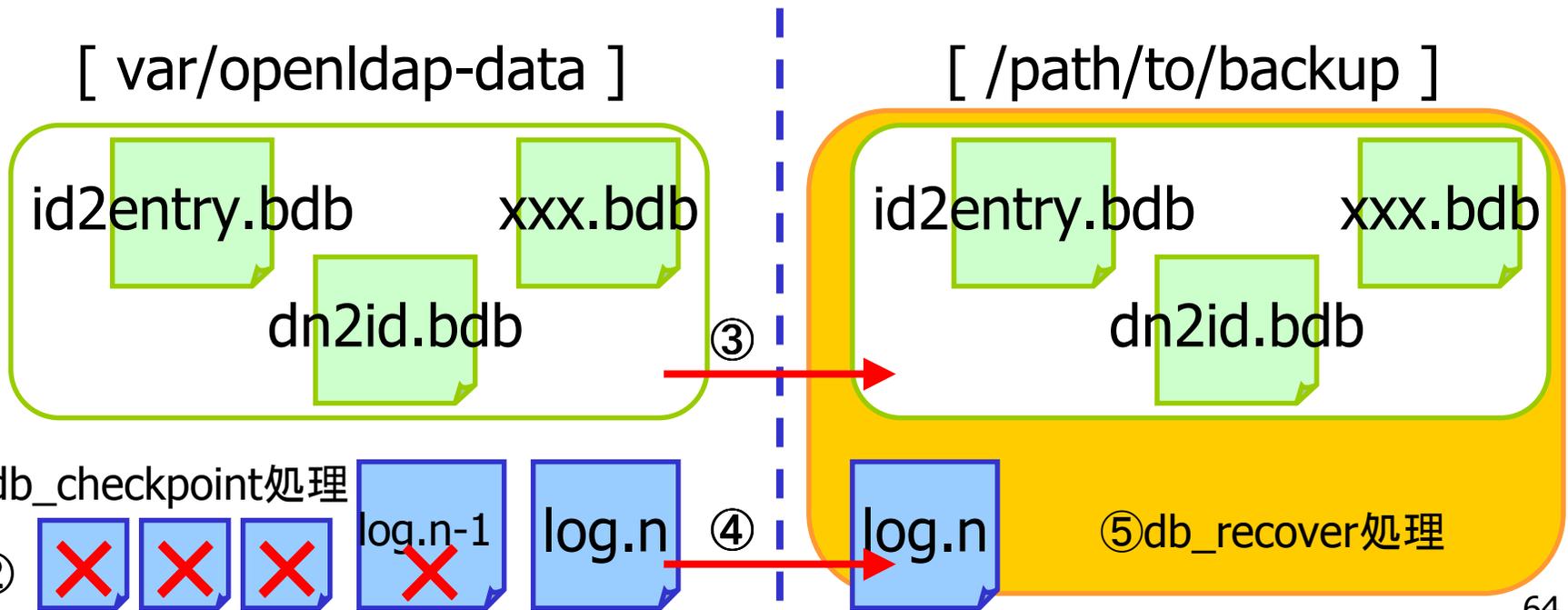


解決

トランザクションログファイル を利用したバックアップ

- Berkeley DB付属ツールを利用したバックアップ

```
# db_hotbackup -cb /path/to/backup
```



解決

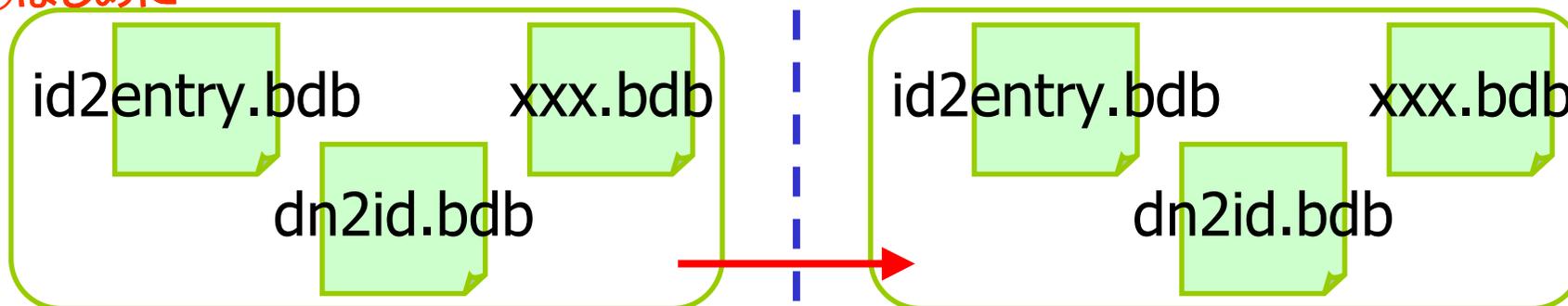
ポイントインタイムリカバリを 目的としたバックアップ

- トランザクションログを繰り返しバックアップ

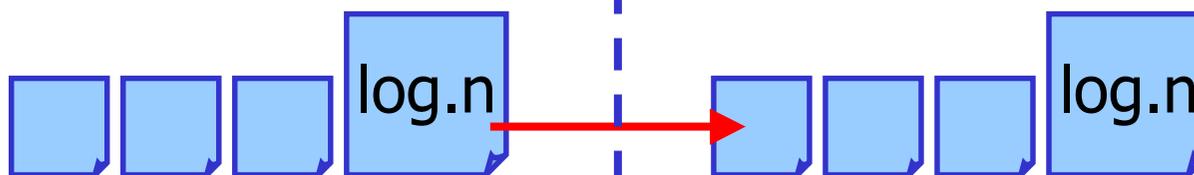
```
# cp -p `db_archive -s` /path/to/backup (はじめに)
```

```
# cp -p `db_archive -l` /path/to/backup (繰り返し)
```

①はじめに



②繰り返し

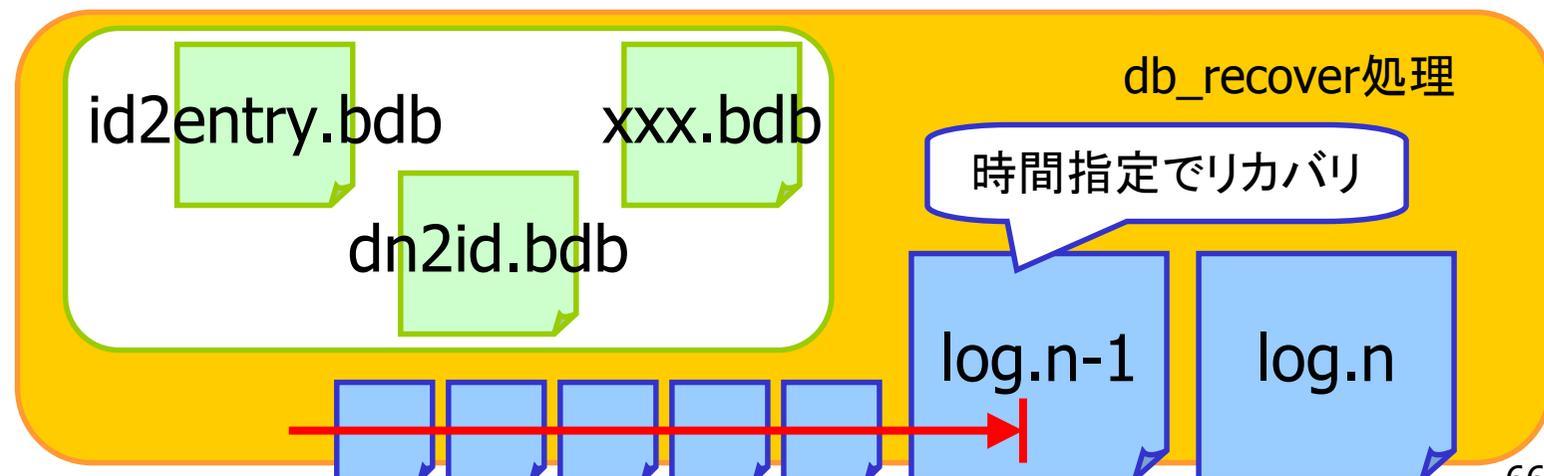


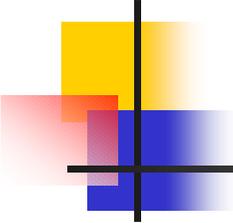
解決

ポイントインタイムリカバリ

- トランザクションログを確認し時間指定でリカバリ

```
# db_printlog > /tmp/recovery_point_check  
# less /tmp/recovery_point_check  
# db_recover -cf -t YYYYMMDDHHMI.SS
```

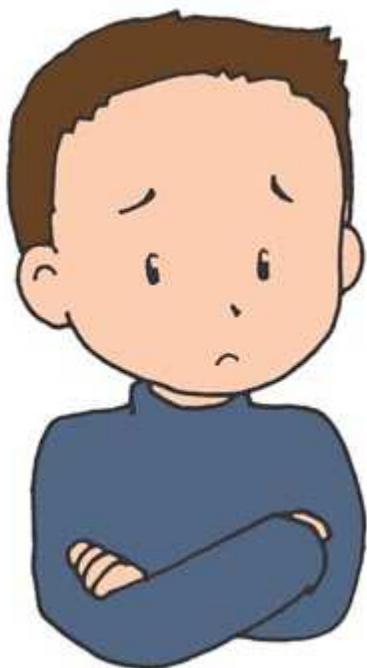




目次

- OpenLDAPサーバ管理
- バックエンドDB(Berkeley DB)管理
- **GUI**管理ツール
 - Apache Directory Studio
 - LDAP Account Manager
 - Ldap Admin
 - phpLDAPadmin
 - その他のGUIツール

GUI管理ツール



- ディレクトリデータの操作はコマンドラインでの操作のみ？ディレクトリツリーのイメージが直感的に把握しづらいし、コマンドラインだけでは作業効率が良くないのでは？

OpenLDAPには、**GUI**でのデータ管理ツールが付属していない。しかし、無償/有償の**GUI**ツールを、別途取得し利用することが可能！

参考

Apache Directory Studio

(<http://directory.apache.org/studio/>)

The screenshot displays the Apache Directory Studio interface. The main window is titled "Apache Directory Studio" and contains several panes:

- LDAP Browser:** Shows a tree view of the LDAP directory structure. The selected entry is "uid=test1000" under "ou=People".
- Entry Editor:** Displays the details of the selected entry. The DN is "uid=test1000,ou=People". The attributes and their values are:

Attribute Description	Value
objectClass	account (structural)
objectClass	posixAccount (auxiliary)
objectClass	shadowAccount (auxiliary)
cn	test1000
gidNumber	1000
homeDirectory	/home/test1000
uid	test1000
uidNumber	1000
gecos	test1000
loginShell	/bin/bash
shadowLastChange	14442
shadowMax	99999
shadowWarning	7
userPassword	SSHA hashed password

- Search Result Editor:** Shows the search results for the selected entry.
- Outline:** Shows the outline of the selected entry, listing attributes like userPassword, loginShell, gidNumber, uidNumber, shadowMax, objectClass, uid, geccos, shadowLastChange, cn, homeDirectory, and shadowWarning.
- Connections:** Shows the connection to the LDAP server, identified as "CentOS53a".
- Modification Logs:** Shows the modification logs for the selected entry.
- Search Logs:** Shows the search logs for the selected entry.
- Progress:** Shows the progress of the search, indicating it is finished at 1:13 and there is an error while processing the search results.

Apache Directory Studio

概要	Apacheプロジェクトから提供される、EclipseベースのLDAPブラウザ&ツール
動作環境	Mac OS X、Linux、Windows
依存プログラム	Java (プラグイン利用は、Eclipseも)
日本語表示	× (英語、フランス語、ドイツ語)
データ操作	○ (エントリデータ操作、スキーマ参照)
バックアップ	LDIF、Excel、(CSV)などで出力可能
ACL設定	× (Apache DSに対して可)
サーバ設定	× (Apache DSに対して可)

参考

LDAP Account Manager

(<http://www.ldap-account-manager.org/>)

LDAP Account Manager

ログアウト

ツリービュー ユーザ グループ ホスト Samba ドメイン

(リフレッシュ | 新しいエントリを作成)

dc=my-domain, dc=com (3)

- cn=Manager
- ou=Group (50+)
- ou=People (72)
 - 新しいエントリを作成
 - uid=test1000
 - 新しいエントリを作成
 - uid=test1001
 - uid=test1002
 - uid=test1003
 - uid=test1004
 - uid=test1005
 - uid=test1006
 - uid=test1007
 - uid=test1008
 - uid=test1009

uid=test1000

DN: uid=test1000,ou=People,dc=my-domain,dc=com

リフレッシュ 内部属性を表示する

削除 エクスポート

ヒント: 属性を削除するには、テキストフィールドを空にして保存してください。

新しいエントリを作成 新しい属性の追加

cn test1000 (値の追加)

gecos test1000

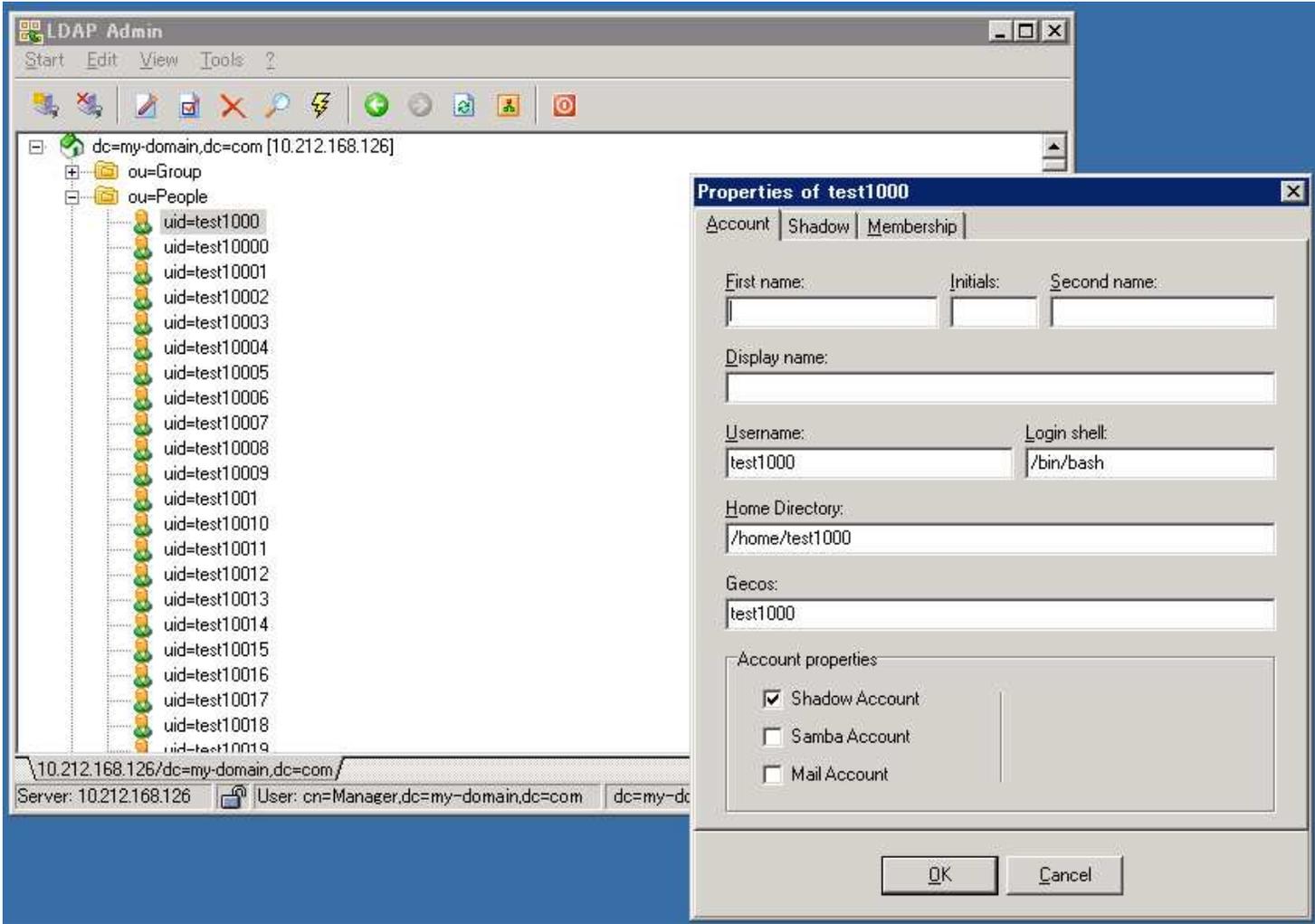
LDAP Account Manager

概要	元々は、Sambaアカウントを管理する 為に開発されたWebベースのツール
動作環境	Linux、(Unix系)
依存プログラム	Apache、PHP、Perl
日本語表示	○ (日本語を含め、15の言語に対応)
データ操作	○ (エントリデータ操作、スキーマ参照)
バックアップ	LDIF、CSV、(PDF)などで出力可能
ACL設定	×
サーバ設定	×

参考

LDAP Admin

(<http://ldapadmin.sourceforge.net/>)



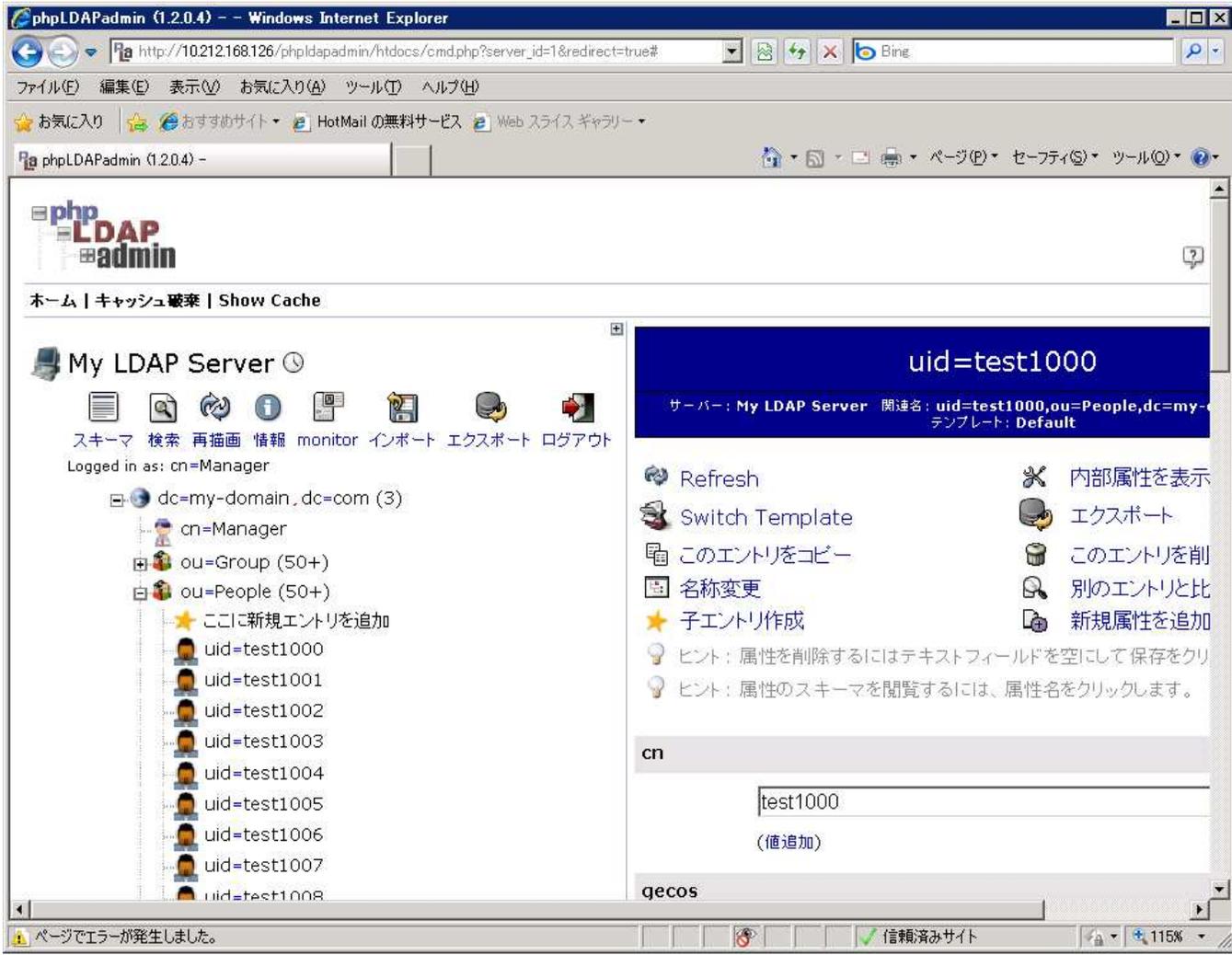
LDAP Admin

概要	Windows上で動作するLDAPサーバ管理ツール
動作環境	Windows
依存プログラム	なし
日本語表示	× (英語のみ)
データ操作	○ (エントリデータ操作、スキーマ参照)
バックアップ	LDIFで出力可能
ACL設定	×
サーバ設定	×

参考

phpLDAPAdmin

(<http://phpldapadmin.sourceforge.net/>)



phpLDAPadmin

概要	WebベースのLDAPサーバ管理ツール (実装の一部はLAMに採用されている)
動作環境	Linux、Unix系
依存プログラム	Apache、PHP
日本語表示	○ (日本語を含め、18の言語に対応)
データ操作	○ (エントリデータ操作、スキーマ参照)
バックアップ	LDIF、CSVなどで出力可能
ACL設定	×
サーバ設定	×

その他のGUI管理ツール

- Coral Directory
 - GQ LDAP client
 - ...
- これらGUI管理ツールの使い勝手は、本カンファレンスの開催中、日本LDAPユーザ会のブースでお楽しみ下さい

ご清聴、ありがとうございました

- 日本LDAPユーザ会は、こちらから
 - <http://www.ldap.jp/>

