エンタープライズID基盤におけるLDAPの活用

～ OpenLDAPの高速化と技術トレンドについて ～

OSSTech

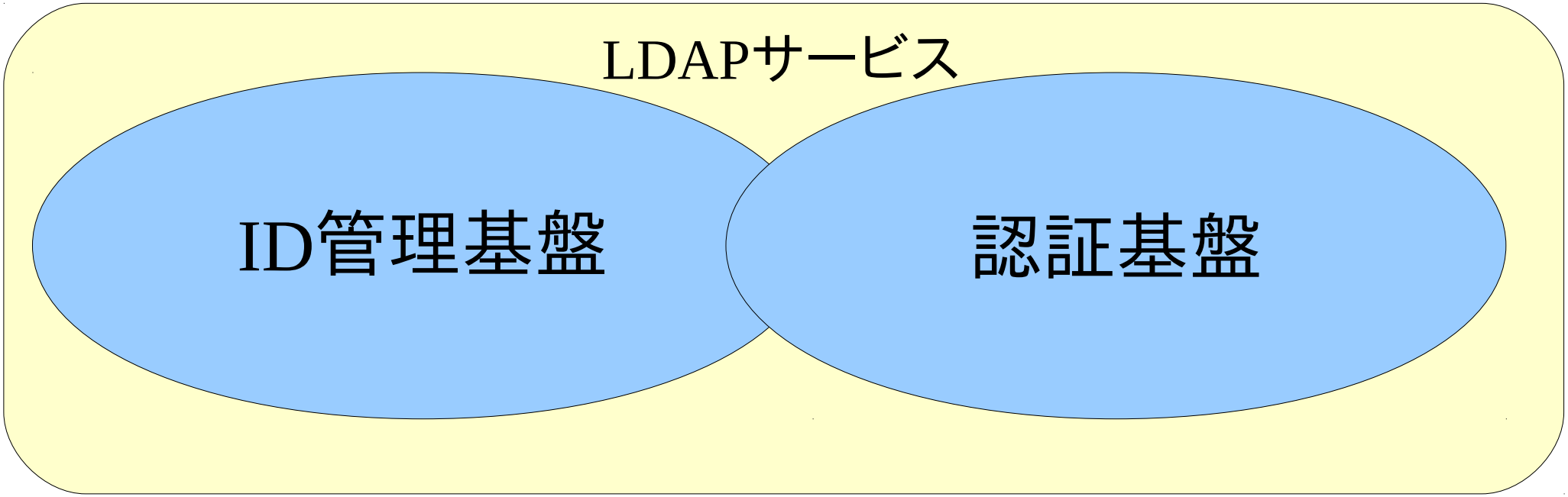
2015年6月26日

オープンソース・ソリューション・テクノロジ株式会社
http://www.osstech.co.jp/
お問い合わせ info@osstech.co.jp

目次

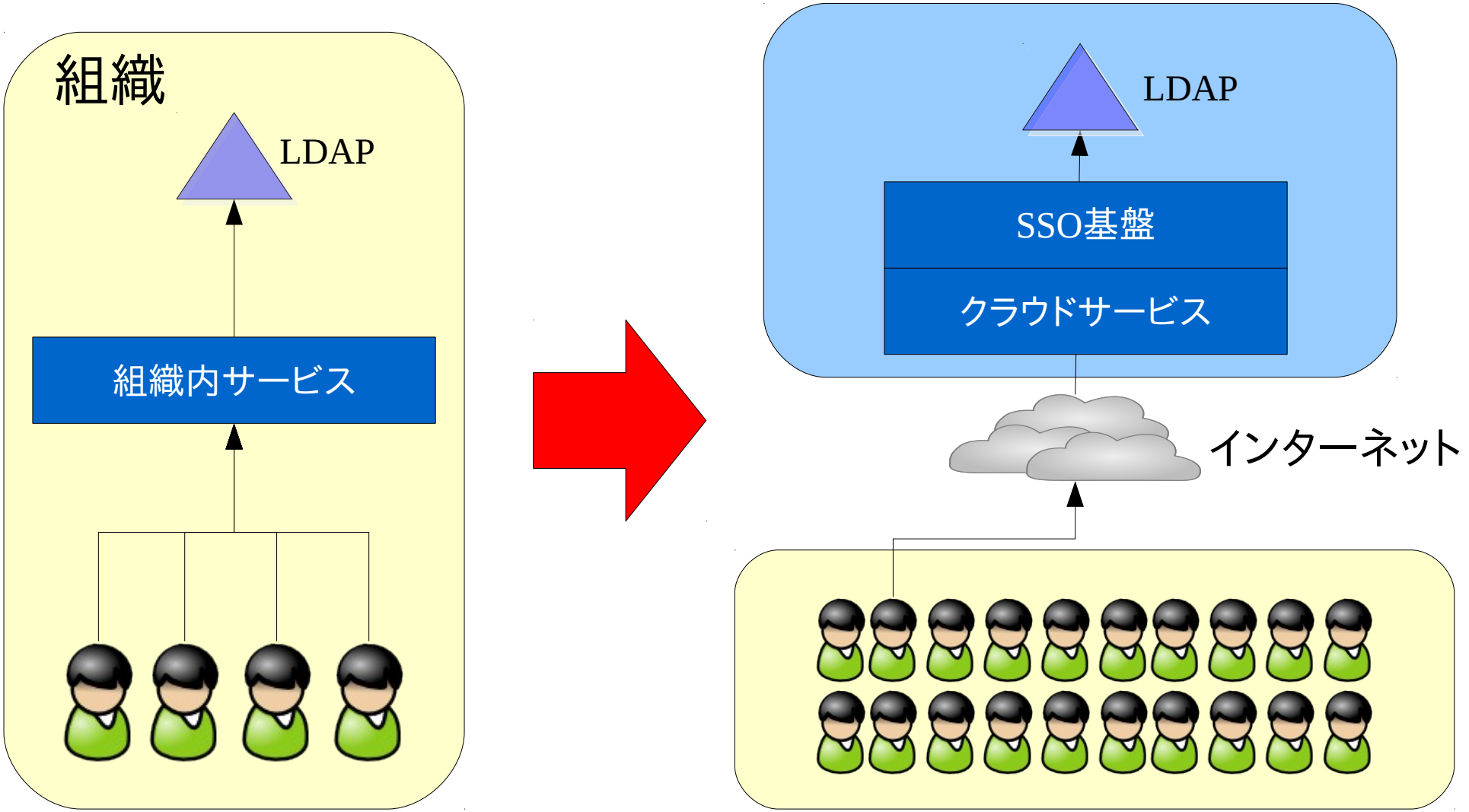
- OpenLDAPの高速化
- OpenLDAPのパスワード管理

LDAPの活用領域



- 認証・検索に特化
- 標準プロトコルとして普及

クラウドサービスとLDAP



社員等：数万人程度

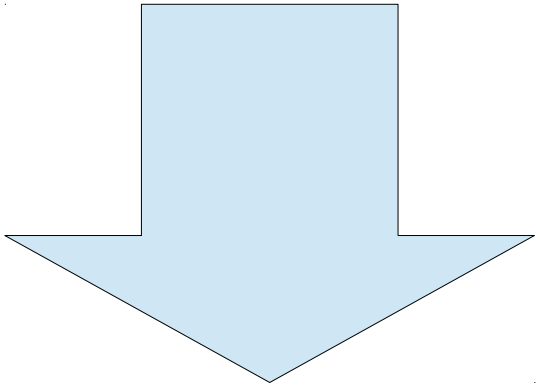
利用ユーザー：数十万人～数百万人

Why OpenLDAP?

- オープンソースソフトウェア
  - Core Team　: OpenLDAP Foundation
  - License　　: OpenLDAP Public License
- 1998年開発開始～
  - 2007年 OpenLDAP 2.4 リリース
- LDAPサービスの系統
  - OpenLDAP およびその仲間
  - Netscape Directory Server系列
  - その他商用製品

大規模環境で顕在化する問題

- エントリが100万件を超える環境では...
  - エントリの頻繁な更新 … 性能低下
  - 初期登録、障害復旧時の全件登録 … 処理時間増大



OpenLDAPの更新性能の不足

原因は?

- BerkleyDB(back-bdb, back-hdb)に起因
  - OpenLDAPの標準的なストレージエンジン
  - ファイルベースのKey-Value型

- OpenLDAP と BerkleyDB の関係
  - OpenLDAP 2.1 (2002年)から利用可能
  - エントリ、インデックス等の格納に利用

BerkleyDBのライセンス問題

- Sleepycat Software
  - Version 4.8.30まで　Sleepycat License
- Oracle BerkleyDB
  - Version 5.0.32～5.3.28 まで　Sleepycat License
  - Version 6.0.20 (12.1.6.0)以降　AGPLv3
    - リモート接続経由で利用しているユーザーへのソースコード公開義務

BDBの代替を探せ!!

OpenLDAPチームの取り組み

- ストレージエンジンとしてLMDBを開発
- LMDBとは?
  - Lightning Memory-mapped DataBase
  - OpenLDAPのために開発されたメモリマップ方式のkey - value型データベース
  - OpenLDAP public License

LMDBの特徴

- No Cashing
  - DBファイルをメモリにマップ
- No Locking / Corruption free
  - Single Writer + N Readers
    - 参照性能はCPU数に比例して向上
  - Copy On Write方式 : デッドロック回避
- Simple Configuration
  - 設定パラメータはMax Sizeのみ

更新性能がCPU数に応じてスケールしない ...

大規模環境のOpenLDAP構成

- 更新用マルチマスター　… 2台
- 参照用スレーブ　　… N台

参照性能	スレーブ台数を増やすことで対処可能
更新性能	CPU、メモリ、ディスクの強化(限界あり) スレーブサーバーも複製時に更新発生

更新性能を向上したい

OSSTechの取り組み

OpenLDAP の WiredTiger バックエンドの開発

… 只今、開発中

http://github.com/osstech-jp/openldap

WiredTigerとは...

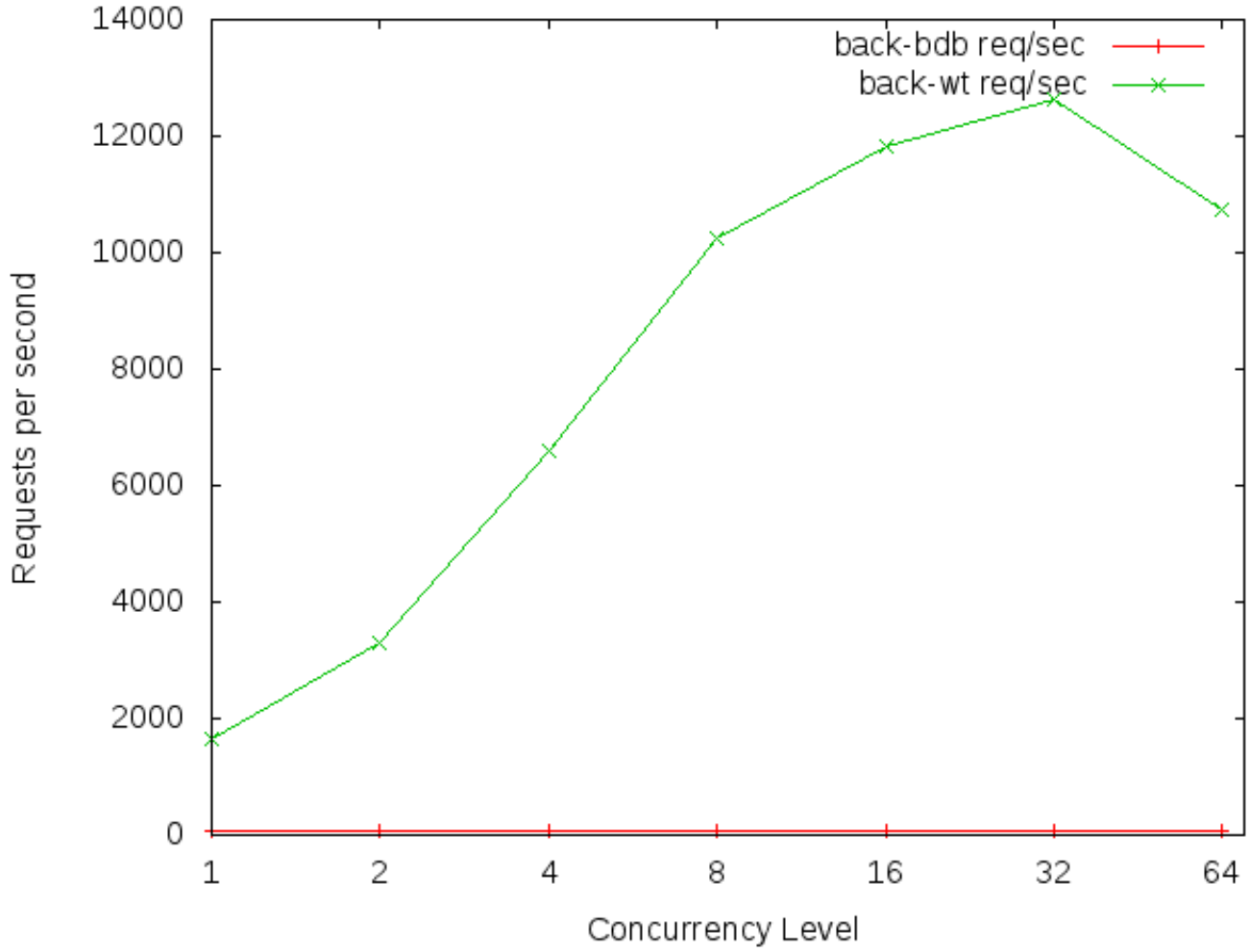
- WiredTiger社開発の新ストレージエンジン
- 開発者
  - Michael Cahill氏、Keith Bostic氏
  - BerkleyDBの開発者(Sleepycat, ORACLE)
- OSS
  - GPL v3 / v2 Dual License

WiredTigerの特徴

- Key – Value方式のストレージエンジン
- 高い並行処理性能
  - マルチコア、大容量メモリ、ディスク環境向け
  - メモリ上のキャッシュ方式を採用
  - Multi Versioned dataによる処理の競合回避
    - トランザクション間のブロックによる処理遅延を防ぐ
- 効率的なディスク利用
- ジャーナリングによるデータ保護
  - Checkpoint / Write ahead logging

OpenLDAP Benchmark

Add性能



https://github.com/osstech-jp/openldap/wiki/back_wt-benchmark

注意：WiredTigerバックエンドは未完成です …

ところで … LDAPのベンチマークは何を使えば?

今までのLDAPベンチマークツール

- slamd
  - Sun Microsystemsが開発したLDAPベンチマークツール
  - 最新版 : slamd 2.0.1 2006年頃リリース
  - Javaベース (slamd 2.0.1 リリース当時 : JDK 1.6)

メンテナンスされていない & 手に入らない

新LDAPベンチマークツール

- lb
  - Apache bench風のツール
  - コマンドラインで計測可能
  - Add / Bind / Searchに対応

https://github.com/hamano/lb

OpenLDAPのユーザーパスワード管理

ユーザーのパスワードの格納方式

- userPassword属性に格納
  - 平文 (cleartext) 、もしくは ハッシュ化して保存
- 対応ハッシュ方式は?
  - CRYPT
  - MD5 / SMD5
  - SHA-1 / SSHA … OpenLDAP 2.4.40調べ

SHA-1 で大丈夫?

新しいハッシュ方式の対応

- SHA-2対応
  - {CRYPT} + OSのSHA2対応
  - pw-sha2モジュール
- PBKDF2対応
  - pw-pbkdf2モジュール

{CRYPT}によるSHA-2対応

- OS(glibc)のcrypt(3)によるパスワードハッシュ化
- glibc 2.7以降でSHA2対応
  - RHEL5.2 以降
- salt-formatによるラウンド回数の指定が可能
  - デフォルト 5000回
- slapd.confの設定例(SHA512)

```
password-hash "{CRYPT}"
password-crypt-salt-format "$6$%.8s"
```

SHA2モジュール

- OpenLDAP 2.4.34以降で対応
- 対応方式
  - SHA512、SSHA512
  - SHA384、SSHA384
  - SHA256、SSHA256
- pw-sha2.soモジュールのロードが必要
  - contrib/slapd-module/passwd/sha2/
- slappasswdではモジュール名とパス指定が必要

```
# slappasswd -h '{SSHA512}' -o module-path=openldapモジュールのパス
   -o module-load=pw-sha2 -s secret
```

PBKDF2モジュール

- ストレッチングによりハッシュ化演算処理時間増大
  - デフォルト : 10000回
  - 約 100倍の処理時間 (BIND操作 : 3ms → 300ms)
- OpenLDAP 2.4.40以降で対応
- 対応方式
  - SSHA512、SSHA256、SSHA (saltサイズ固定)
- pw-pbkdf2.soモジュールのロードが必要
  - contrib/slapd-module/passwd/pbkdf2/
- slappasswdではモジュール名とパス指定が必要

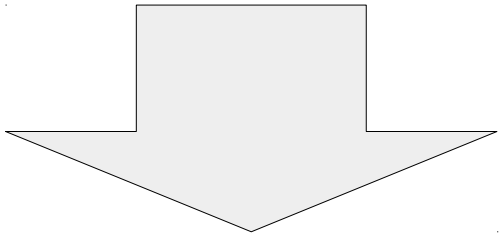
```
# slappasswd -h '{PBKDF2-SHA512}' -o module-path=openldapモジュールのパス
   -o module-load=pw-pbkdf2  -s secret
```

まとめ

- OpenLDAPの大規模環境への導入

OpenLDAPの更新処理の高速化による運用課題の解消へ

ユーザーパスワード保護のための新しいハッシュ方式の対応



OpenID Connectなどの認証基盤のバックエンドとしての
OpenLDAPの活用へ

オープンソース・ソリューション・テクノロジ株式会社
http://www.osstech.co.jp/
お問い合わせ *info@osstech.co.jp*