
ORACLE®

MySQLのセキュリティ機能

Yoshiaki Yamasaki / 山崎 由章
MySQL Senior Sales Consultant, Asia Pacific and Japan

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

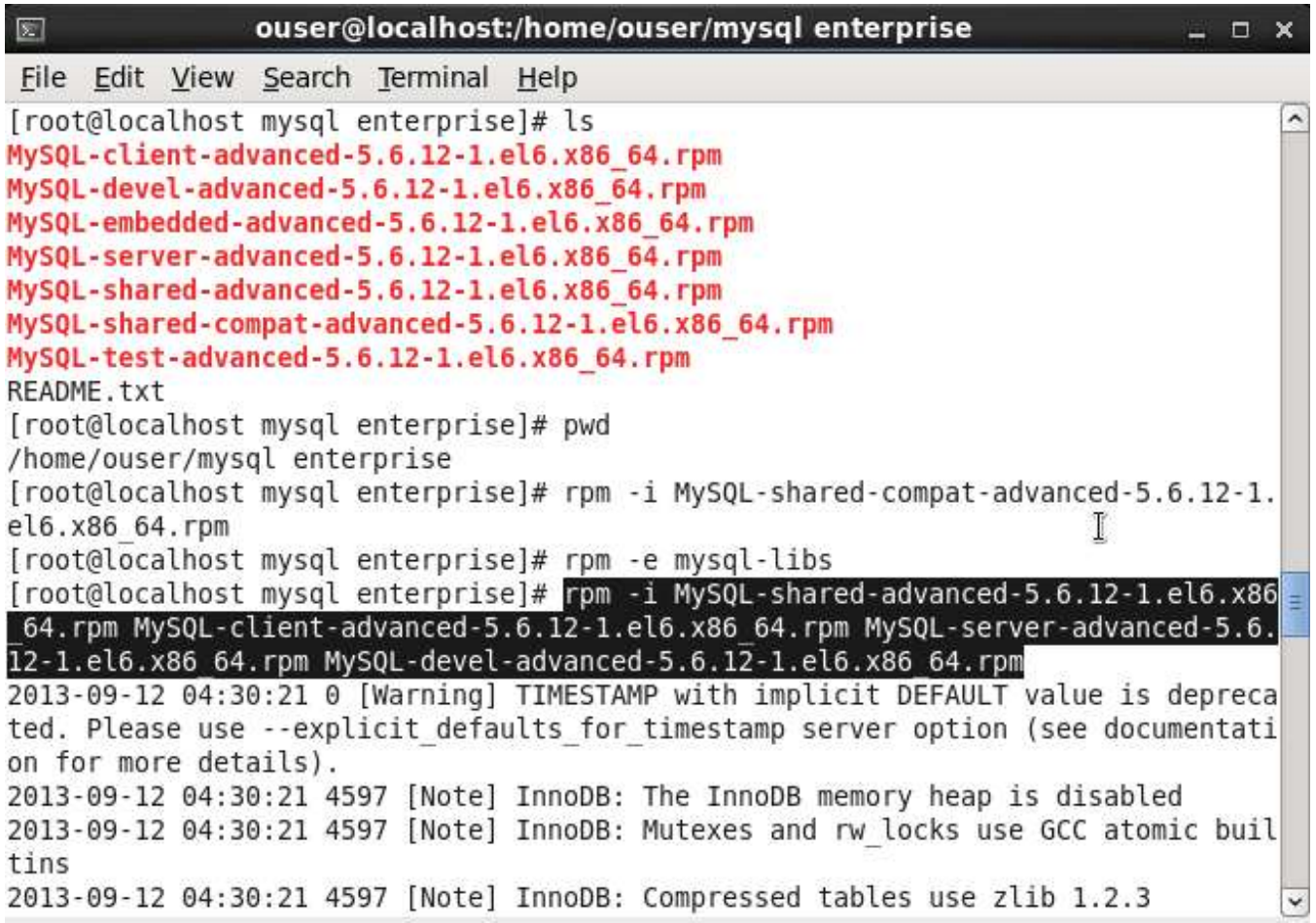
Program Agenda

1. インストール関連
2. ユーザー管理
3. 権限管理
4. 暗号化
5. 監査ログ

Program Agenda

1. インストール関連
2. ユーザー管理
3. 権限管理
4. 暗号化
5. 監査ログ

MySQL 5.6をRPMでインストール



- rootでインストール
- shared-compatをインストール後、mysql-libsを削除
- test、embeddedをインストールしない

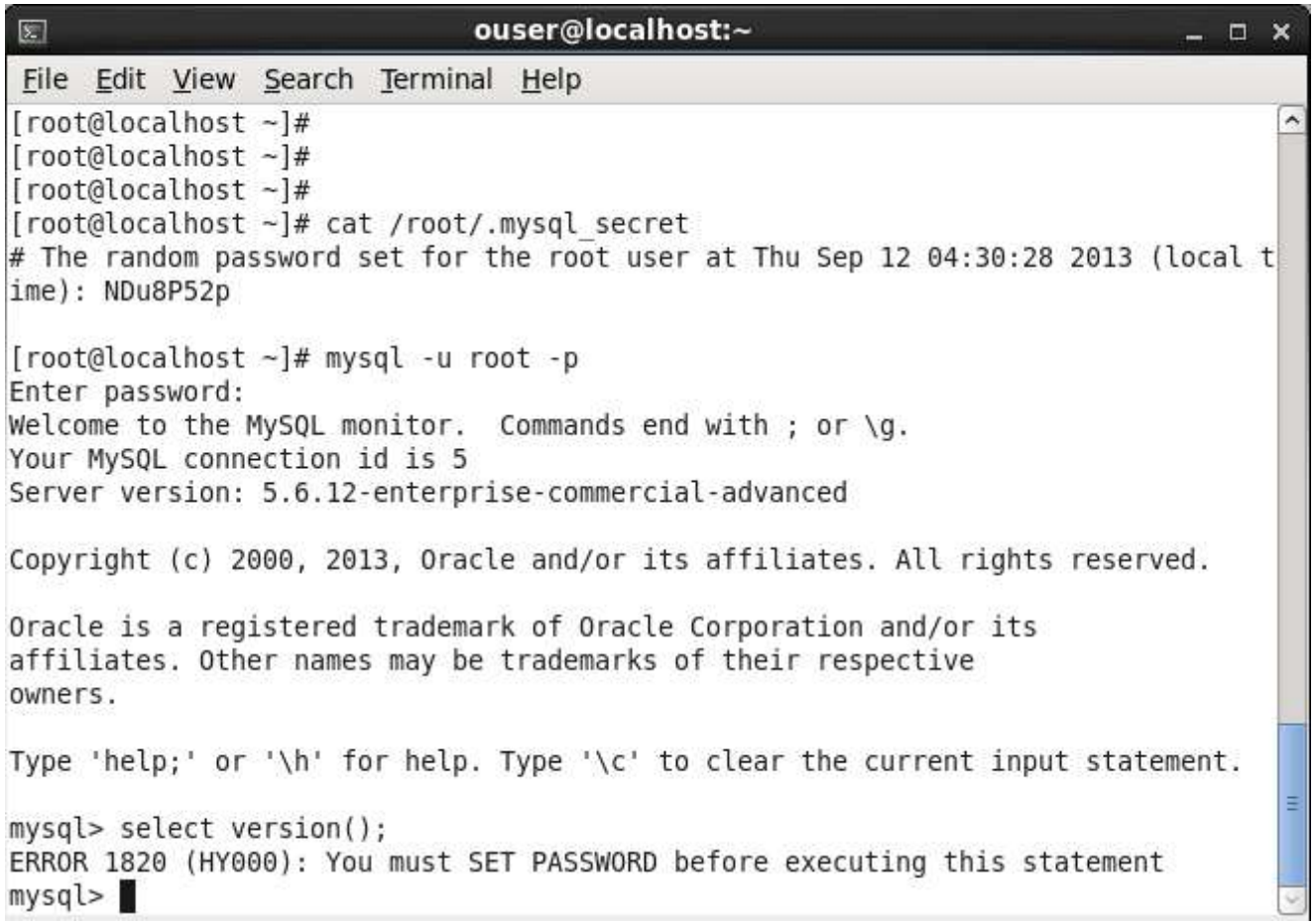
MySQL 5.6をRPMでインストール

- MySQL 5.6をrpmでインストールした場合、rootのパスワードは自動的に設定され、後で変更する必要がある。
  - パスワードは $HOME/. mysql_secret ファイルに記載されている
  - パスワードを変更するまではrootユーザで何も実行できない
  - "SET PASSWORD"コマンドでパスワードを設定
- セキュリティを向上するために、追加で"mysql_secure_installation"を実行可能

MySQL 5.6をRPMでインストール

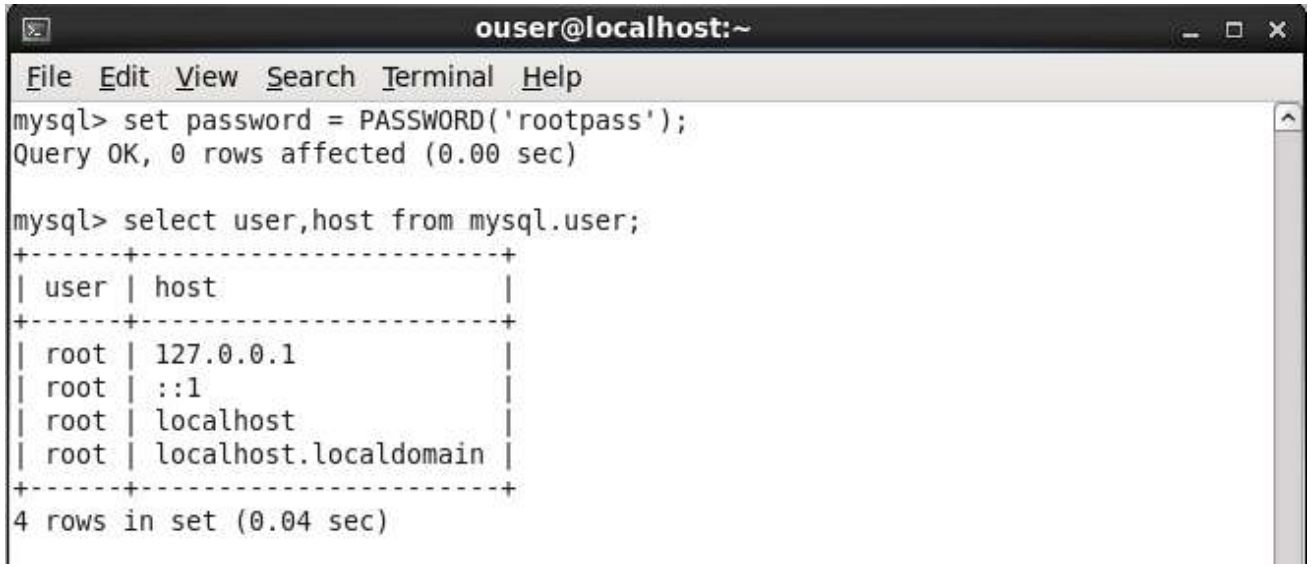
- rootで実行
- 自動起動の設定

MySQL 5.6をRPMでインストール



- rootユーザーのパスワードは有効期限が切れている
- “SET PASSWORD”コマンドのみ実行可能

MySQL 5.6をRPMでインストール



- rootユーザーのパスワードを最初に変更

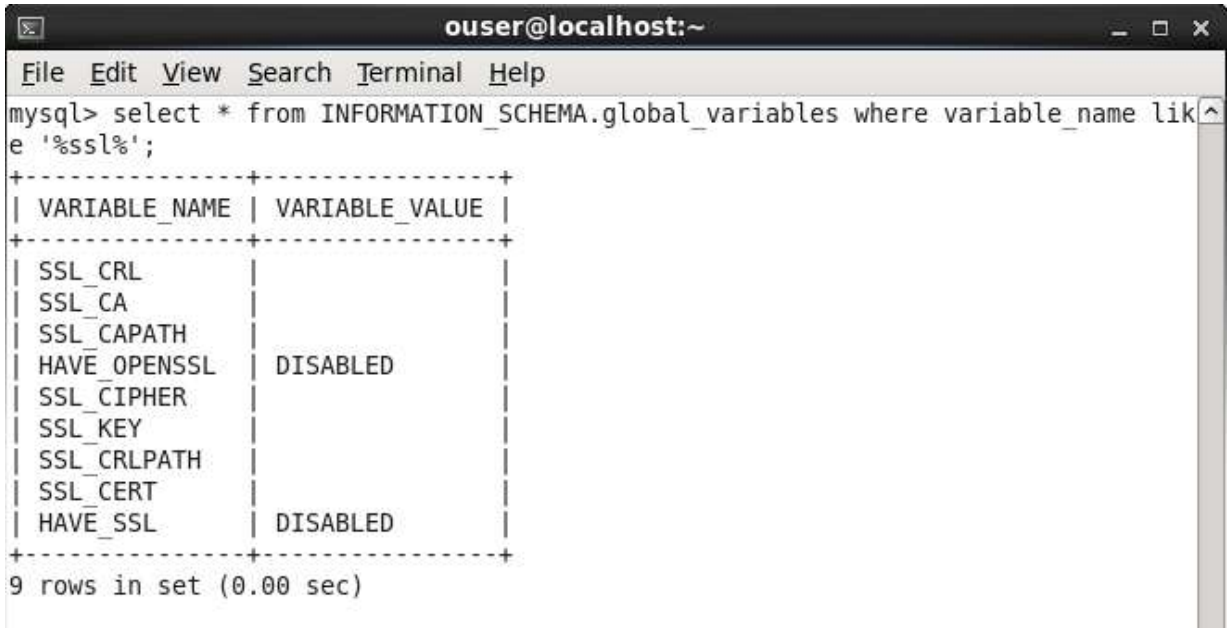
mysql_secure_installation

- MySQLインストール後のデフォルト状態からセキュリティを向上させるスクリプト
  - rootアカウントのパスワードを設定
  - localhost以外からrootアカウントでのアクセスを無効化
  - anonymous(匿名)ユーザアカウントを削除
  - デフォルトでアノニマスユーザがアクセス可能なtestデータベースを削除

MySQL 5.6をTARでインストール

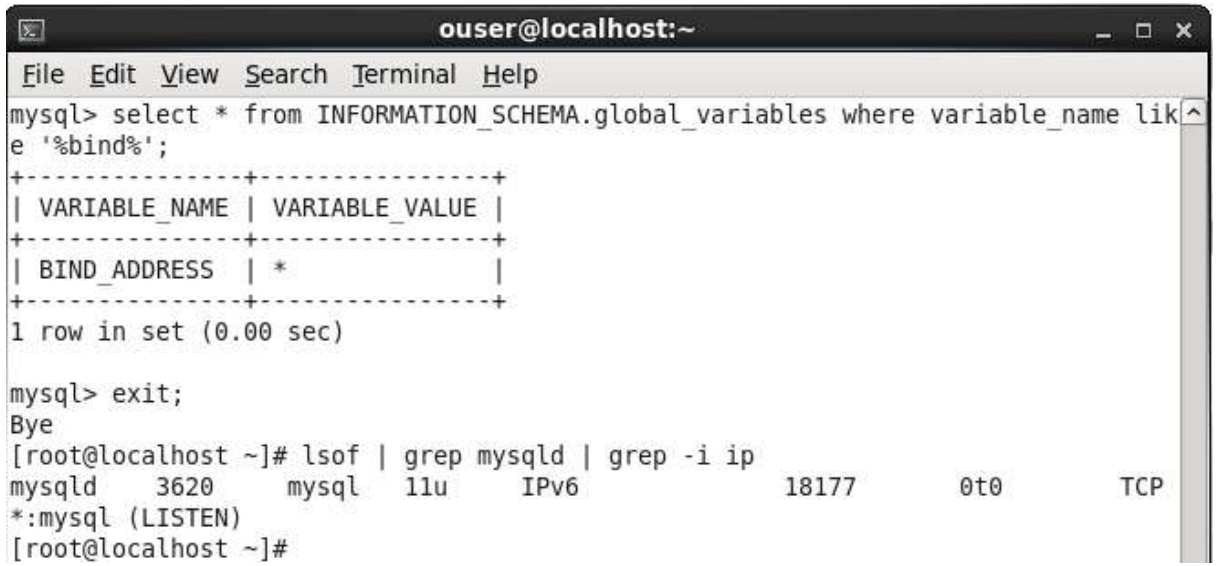
- MySQL 5.6の場合、mysql_install_db に--random-password が指定でき、DB作成時に合わせて以下の操作を実行可能
  - rootユーザにランダムなパスワードを設定
    - パスワードの設定ファイル、パスワードを変更するまでの操作制限は上記と同様
  - anonymousユーザを削除

インストール後の作業：SSLの設定



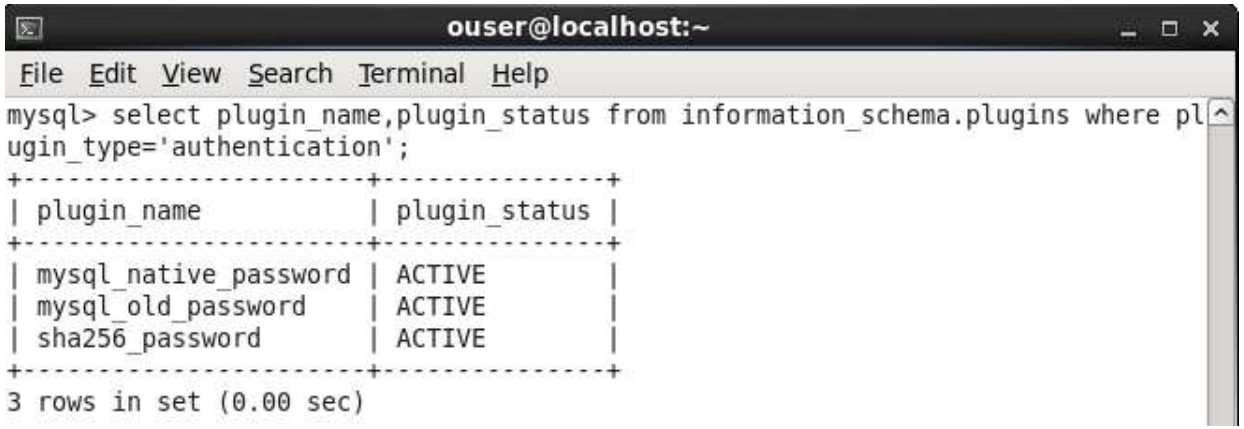
- 設定を強く推奨
- デフォルトでは設定されていない

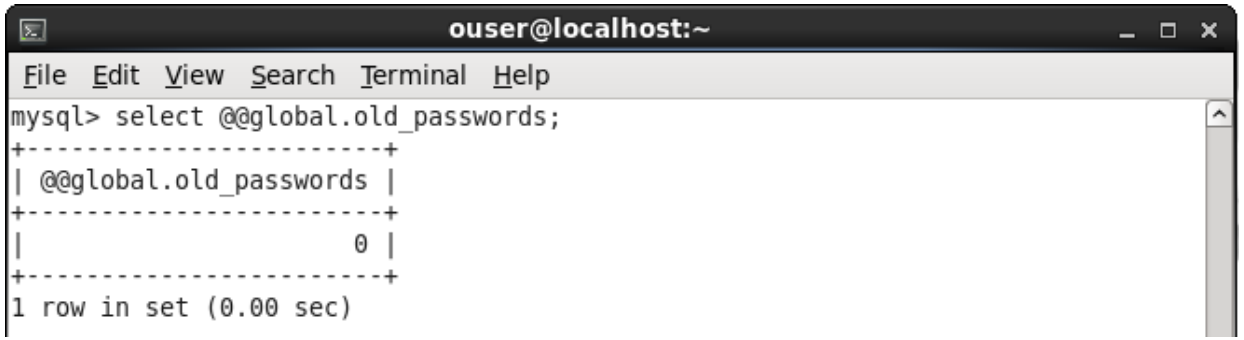
インストール後の作業：接続インターフェースの制御



- 全てのインターフェースがデフォルトで有効になっている(IPv6 も含めて)
- OS側のアクセス制御も確認

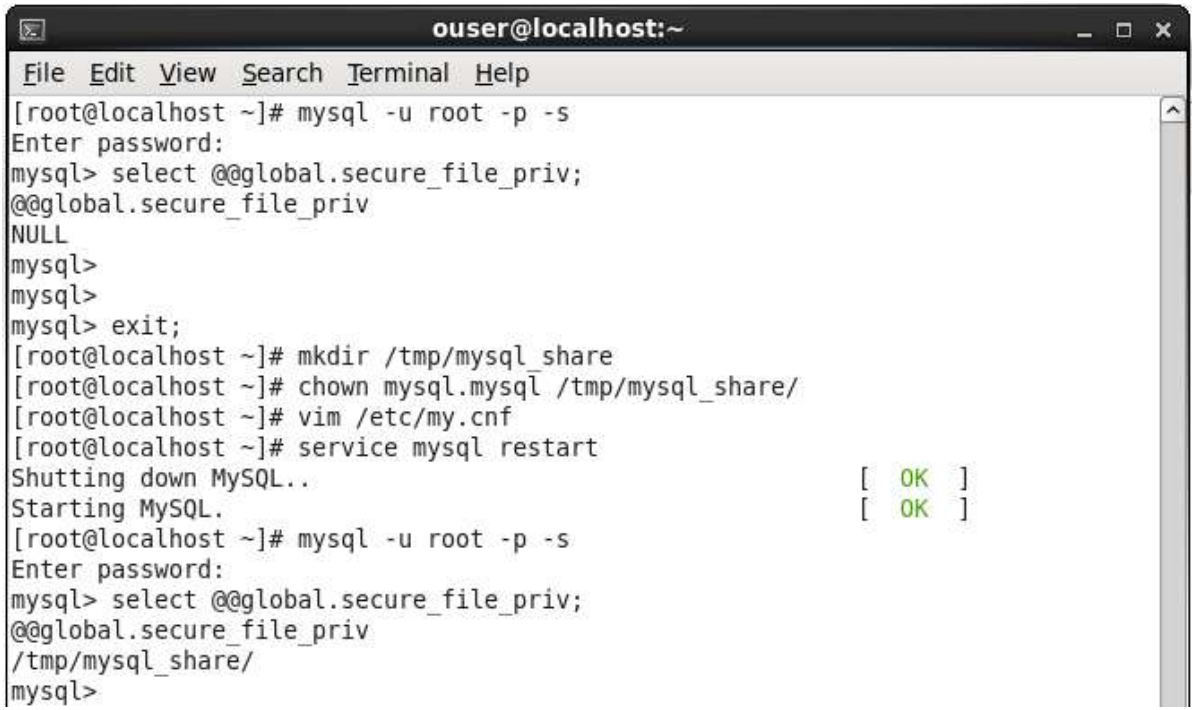
インストール後の作業：認証方式の確認





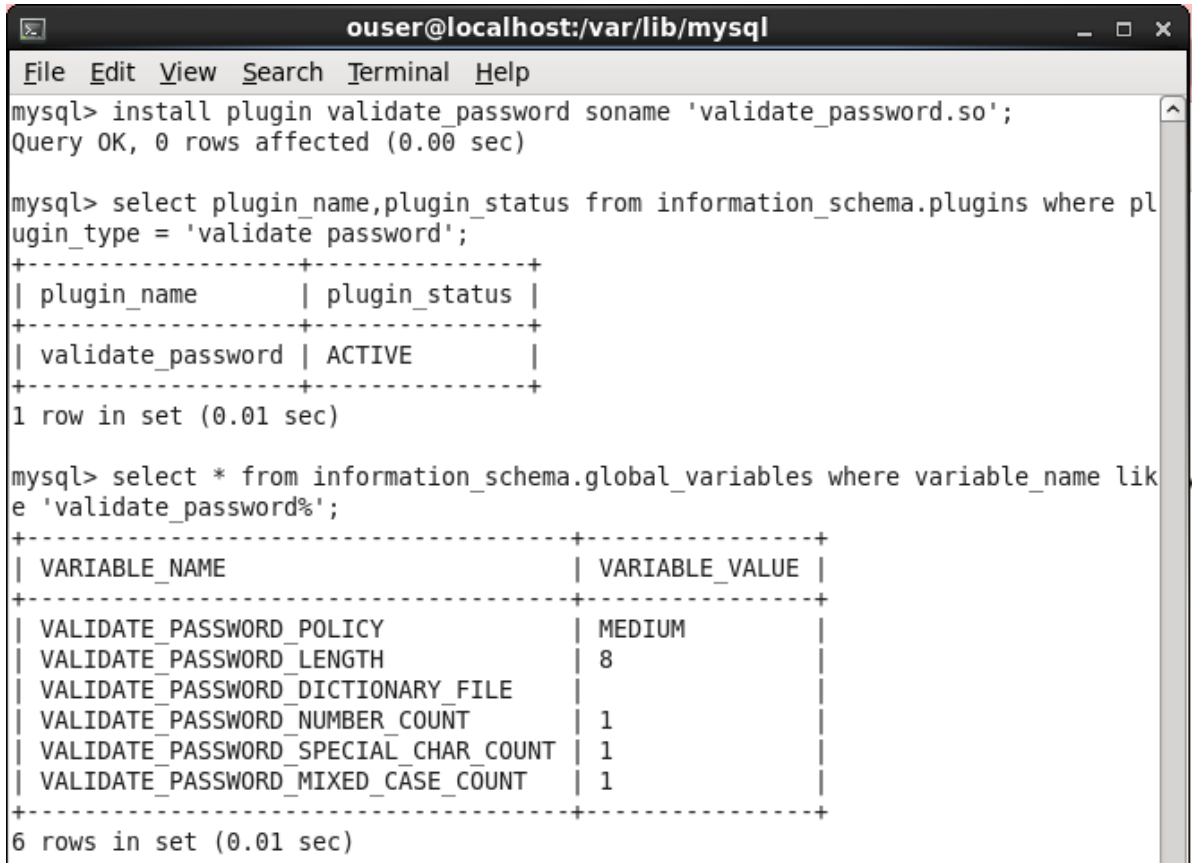
- 3つの方式が有効になっている (mysql_old_passwordは非推奨)
- 他の方式も追加可能
- 正しい方式のパスワードが生成されているか確認

インストール後の作業：OS上のファイルへのアクセスを制限



- 専用のディレクトリを作る /tmp/mysql_share
- “mysql”をオーナーにする
- my.cnfの[mysqld]セクションに “secure-file-priv=/tmp/mysql_share“ を設定
- MySQLサーバー再起動

インストール後の作業：パスワードポリシーのインストール



- validate_password プラグインをインストール
- 英数字の混在を強制する、文字数を〇文字以上にする、特定のキーワードはパスワードに指定できなくする、といった対応が可能

Program Agenda

1. インストール関連
2. ユーザー管理
3. 権限管理
4. 暗号化
5. 監査ログ

ユーザー作成

- CREATE USER コマンドで作成
- ユーザーは、ユーザー名と接続元ホストの組合わせで定義される
(同じユーザー名でも、ホストが違えば別のユーザーとして扱われる)
- ホストの指定はホスト名またはIPアドレス、およびワイルドカード(%)を使用する方法がある
  - 例）'10.0.%‘, '%.domain.com‘

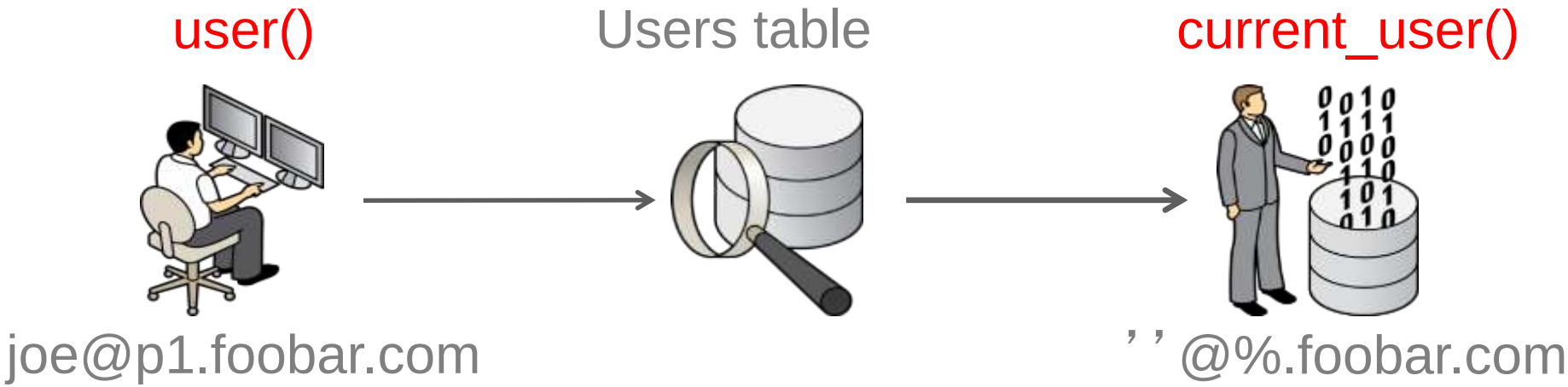
```
mysql> CREATE USER 'oper’@’localhost' IDENTIFIED BY 'sakila';
mysql> CREATE USER 'oper’@’10.1.1.32' IDENTIFIED BY 'sakila’;
```

※推奨(DNSのルックアップを回避)
- IPアドレスを使用
- --skip-name-resolve

"ログインユーザー"と"現在のユーザー"の違い

- joeというユーザが p1.foobar.com というクライアントから接続
- MySQLのユーザテーブルに 'joe'@'p1.foobar.com' が存在せず、別途存在した *''@'%.foobar.com'* で認証
- joeは *''@'%.foobar.com'* の権限にてアクセス

  ⇒想定外のユーザーで接続されないように注意！！

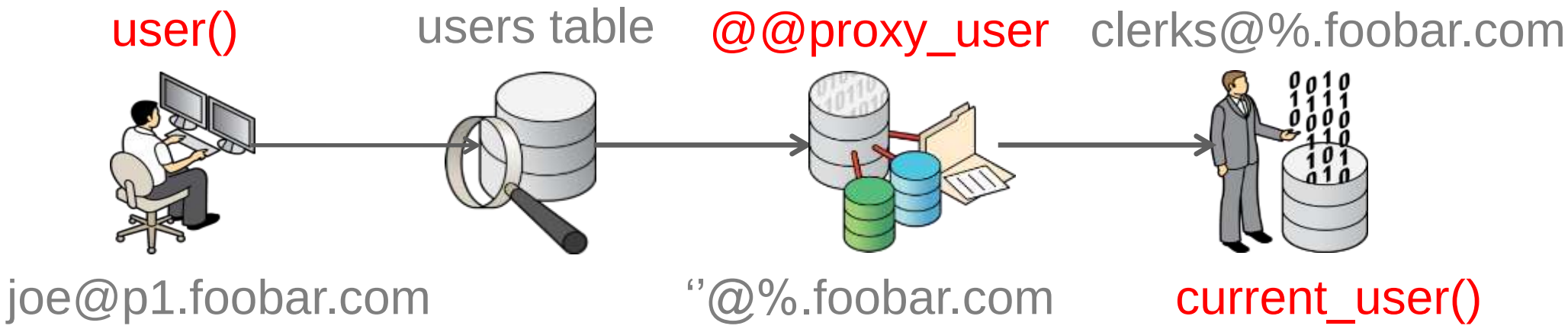


MySQL Enterprise Security
External Authentication

- PAM (Pluggable Authentication Modules)
  - 外部の認証システムを利用
  - 標準的なインターフェース (Unix, LDAP)
- Windows
  - Windowsのネイティブサービスを利用
  - Windowsログイン時に認証済みの情報を利用可能 (Windows Active Directory)
- Pluggable Authentication API

Authentication APIを利用したプラグイン

- joeの接続は ‘’@‘%.foobar.com’ にマッピングされる
- ‘’@‘%.foobar.com’ を使ってプラグインでの認証を行う
- プラグインがjoeを ‘clerks’@‘%.foobar.com’ としてアクセスさせる



パスワードの強制 - SQL_MODE

- デフォルトではパスワードの無いユーザも作成可能
  - セキュリティ向上のために強制可能

```
mysql>  SET GLOBAL sql_mode=NO_AUTO_CREATE_USER;
```

パスワードの無効化：MySQL 5.6の新機能

- ALTER USER コマンドで、パスワードの無効化が可能
- 該当ユーザは、パスワードを変更するまで操作ができなくなる

```
mysql>  ALTER UESR ‘test’@’localhost’ PASSWORD EXPIRE;
```

パスワードのポリシー設定：MySQL 5.6の新機能

- 2つ目のセッション
  「MySQL Enterprise Edition & MySQLによる
  コンプライアンス対応」
  でご紹介します。

Program Agenda

1. インストール関連
2. ユーザー管理
3. **権限管理**
4. 暗号化
5. 監査ログ

権限の種類

- グローバル権限
- データベース権限
- テーブル権限
- カラム権限
- ルーチン権限

グローバル権限

- SUPER (CHANGE MASTER, KILL, PURGE MASTER LOGS, SET GLOBAL)
  - SHOW ENGINE INNODB STATUSの実行にも必要
- SHUTDOWN
- RELOAD
- PROCESS
- FILE
- ALL
- WITH GRANT OPTION

付与されている権限の確認

ユーザに付与されている権限の確認コマンド

```
mysql> SHOW GRANTS [FOR user]
```

http://dev.mysql.com/doc/refman/5.6/en/show-grants.html

付与されている権限の確認

インフォメーションス・キーマからも確認可能

select * from INFORMATION_SCHEMA.*<table>*

Table名	インストール後の状態
USER_PRIVILEGES	rootユーザに権限が付与されている
SCHEMA_PRIVILEGES	testデータベースに対する権限が全員に付与されている
TABLE_PRIVILEGES	Empty
COLUMN_PRIVILEGES	Empty

権限付与(GRANT) / 権限剥奪(REVOKE)

- GRANT文で権限を付与する
  - どのオブジェクトに対する権限： ON *database.table*
  - 誰に権限を付与する： TO *'user'@'host'*
- REVOKE文で権限を剥奪

```
mysql> GRANT SELECT ON db.* TO 'oper'@'10.1.%';
mysql> GRANT INSERT,UPDATE ON db.table TO 'oper'@'localhost';
mysql> REVOKE SELECT ON db.* FROM 'oper@'10.1.%';
```

NOTE: 同一のユーザ名でもホスト毎に権限を変えることが可能

権限が影響するタイミング

- テーブルとカラム：データ参照/変更時
- データベース：USE <dbname> 実行時
- グローバル権限とパスワード：接続時

http://dev.mysql.com/doc/refman/5.6/en/privilege-changes.html

利用するリソースの制限

- MAX_QUERIES_PER_HOUR
- MAX_UPDATES_PER_HOUR
- MAX_CONNECTIONS_PER_HOUR
- MAX_USER_CONNECTIONS

http://dev.mysql.com/doc/refman/5.6/en/user-resources.html
http://dev.mysql.com/doc/refman/5.6/en/grant.html

補足：ネットワークアクセスの制限

TCP/IPアクセスの無効化（localhostのアクセスのみ）

- --skip-networking

他のネットワークアクセスの変更方法

- ポートをデフォルトの3306から変更
- ポートをあけておく場合、root@localhostユーザのみにSUPER権限を付与

Program Agenda

1. インストール関連
2. ユーザー管理
3. 権限管理
4. 暗号化
5. 監査ログ

暗号化 : MySQL Community Edition

- 機密データの暗号化のため、暗号化関数を使用可能
  - AES : AES_ENCRYPT(), AES_DECRYPT()
  - Triple-DES : DES_ENCRYPT(), DES_DECRYPT()

- 暗号化の鍵の強度は、最大256bit(MySQL 5.6の場合)

暗号化：MySQL Enterprise Encryption

NEW

- MySQLの暗号化ライブラリ
  - AES256による対称鍵暗号
  - 公開鍵 / 非対称鍵暗号
- キーの管理
  - 公開鍵および秘密鍵の生成
  - 鍵交換方式: RSA, DSA, DH
- 署名とデータの検証
  - 電子署名、検証、妥当性確認のための暗号学的ハッシュ関数
- Oracle Key Vaultとの統合

※鍵の強度は、最大16,384bit

ORACLE

Program Agenda

1. インストール関連
2. ユーザー管理
3. 権限管理
4. 暗号化
5. 監査ログ

監査ログの出力方法

- MySQL Community Editionには、監査ログの出力機能は無い
- MySQL Enterprise Edition(商用版)では、監査ログの出力機能が使える
- MySQL Enterprise Editionは、Oracle Audit Vault and Database Firewallとの動作保証もされている

MySQL Enterprise Audit

ポリシーベースの監査機能を提供

- ログオン、クエリーの情報を監査可能
- ユーザがポリシーを設定可能：フィルタリング、ログローテーション
- 動的に設定を変更可能：Audit設定時にサーバの再起動が不要
- Oracleの仕様に合わせXMLベースの監査ログを出力
  (Oracle Audit Vaultとの互換性（ログフォーマット))
- サイズに基づいた監査ログファイルの自動ローテーション
- MySQL 5.5のAudit APIを使って実装 / MySQL 5.5.28 以上で使用可能

コンプライアンス対応等で監査が必要なアプリケーションでもMySQLを利用可能

ORACLE

MySQL Enterprise Audit

管理者

```
mysql> INSTALL PLUGIN audit_log SONAME 'audit_log.so';

mysql> SHOW VARIABLES LIKE 'audit_log%';
+--------------------------+--------------+
| Variable_name            | Value        |
+--------------------------+--------------+
| audit_log_buffer_size    | 1048576      |
| audit_log_file           | audit.log    |
| audit_log_flush          | OFF          |
| audit_log_policy         | ALL          |
| audit_log_rotate_on_size | 1044480      |
| audit_log_strategy       | SYNCHRONOUS  |
+--------------------------+--------------+
```

1. DBA enables Audit plugin

Joe (ユーザー)

```
shell> mysql -h joeshost -u joe -p
Enter password: ********

mysql> SELECT * FROM joes_table;
+---------------+--------------+
| FIRST_NAME    | LAST_NAME    |
+---------------+--------------+
| Joe           | User         |
+---------------+--------------+
```

2. User Joe connects and runs a query

3. Joe's connection & query logged

```
<?xml version="1.0" encoding="UTF-8"?>
<AUDIT>
  <AUDIT_RECORD
    TIMESTAMP="2012-08-02T14:52:12"
    NAME="Audit"
    SERVER_ID="1"
    VERSION="1"
    STARTUP_OPTIONS="--port=3306"
    OS_VERSION="i686-Linux"
    MYSQL_VERSION="5.5.28-debug-log"/>
  <AUDIT_RECORD
    TIMESTAMP="2012-08-02T14:52:41"
    NAME="Connect"
    CONNECTION_ID="1"
    STATUS="0"
    USER="joe"
    PRIV_USER="root"
    OS_LOGIN=""
    PROXY_USER=""
    HOST="SERVER1"
    IP="127.0.0.1"
    DB="joes_db"/>
  <AUDIT_RECORD
    TIMESTAMP="2012-08-02T14:53:45"
    NAME="Query"
    CONNECTION_ID="1"
    STATUS="0"
    SQLTEXT="SELECT * FROM joes_table;"/>
</AUDIT>
```

WHO

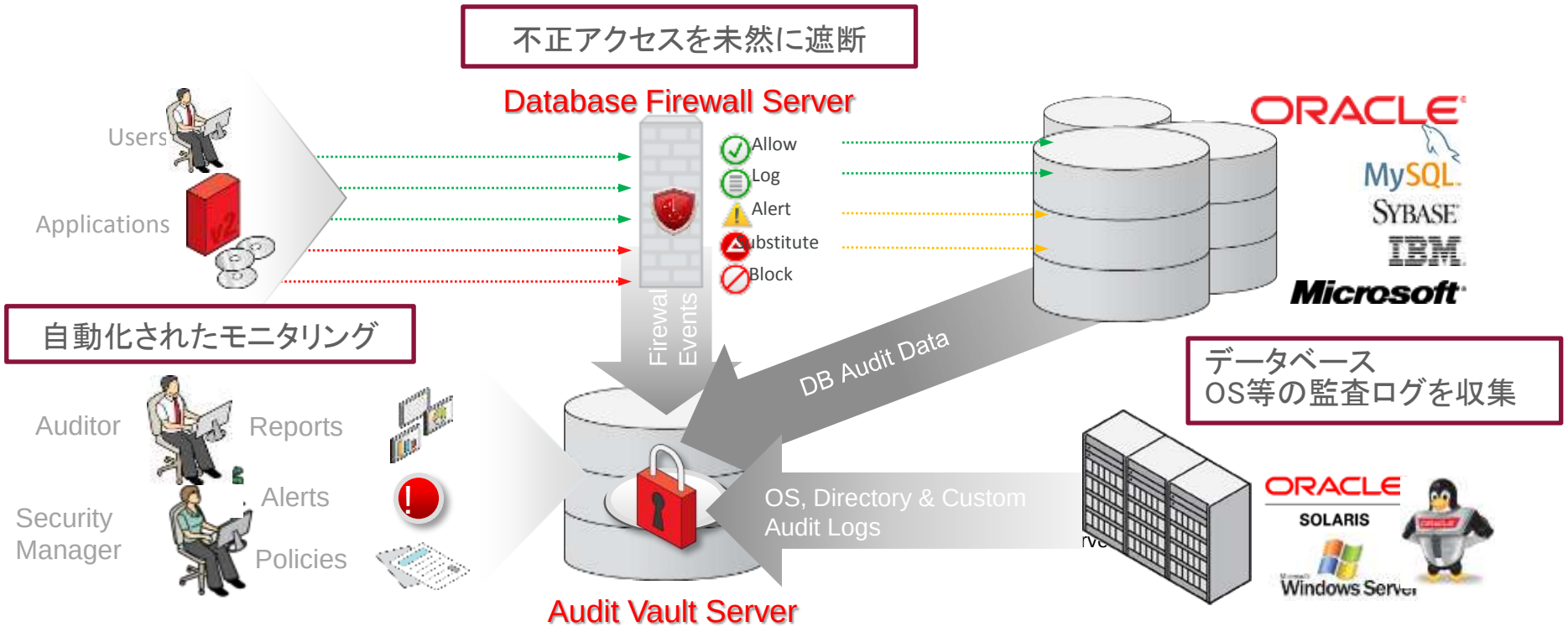
WHERE

WHEN

WHAT

Oracle Audit Vault and Database Firewall

文法解析による正確なブロッキング、DatabaseやOSの監査ログをモニタリング
迅速なセキュリティ対策を可能にするソフトウェア・アプライアンス



Hardware and Software
Engineered to Work Together


ORACLE®

セミナー開催予定

- 2015/1/16(金) 15:00～17:00　　場所：日本オラクル株式会社
  - 【初心者向け】MySQLレプリケーション入門
    「MySQLのレプリケーション機能を使いたいけど、設定方法が分からない」、
    「レプリケーション機能を使っているけど、適切に使いこなせているのか自信が無い」、
    そんな方向けに、初心者向けのMySQLレプリケーション入門セミナーを開催します。
    また、合わせてレプリケーション環境の運用管理に役立つPythonスクリプト
    (MySQL Utilities)のサポートも受けられる、MySQL Enterprise Edition(商用版)の
    詳細もご紹介いたします。

※申込みページは後日公開予定　「日本オラクル　イベント」で検索
http://events.oracle.com/search/search?group=Events&keyword=japan

WiFi

SSID: clear-guest

Userid: guest

Password: NA2RAyg3

ハッシュタグ : mysql_jp