NSD DBA1 DAY04

1 MySQL管理工具

1.1 问题

- 部署LAMP+phpMyAdmin平台

1.2 方案

1. 安装httpd、mysql、php-mysql及相关包
2. 启动httpd服务程序
3. 解压phpMyAdmin包，部署到网站目录
4. 配置config.inc.php，指定MySQL主机地址
5. 创建授权用户
6. 浏览器访问、登录使用

今天课程需要使用1台RHEL7虚拟机，其中一台作为数据服务器（192.168.4.6）、另外一台作为测试用的Linux客户机（192.168.4.254），如图-1所示。

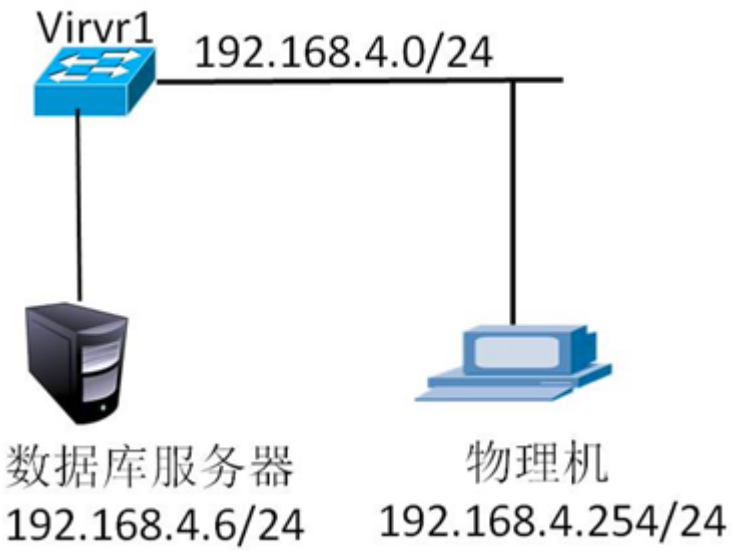

图-1

1.3 步骤

Top

实现此案例需要按照如下步骤进行。

步骤一：准备软件的运行环境 lamp

```
[root@mysql6~]# rpm -q httpd  php  php-mysql   //检测是否安装软件包
未安装软件包 httpd
未安装软件包 php
未安装软件包 php-mysql
[root@mysql6~]# yum  -y  install  httpd   php   php-mysql  //装包
[root@mysql6~]# systemctl  start  httpd     //启动服务
[root@mysql6~]# systemctl  enable httpd     //设置开机自启
Created symlink from /etc/systemd/system/multi-user.target.wants/htt
```

步骤二：测试运行环境

```
[root@mysql6~]# vim  /var/www/html/test.php    //编辑页面测试文件
[root@mysql6~]# cat /var/www/html/test.php     //查看页面测试文件
<?php
$x=mysql_connect("localhost","root","123456");
if($x){   echo "ok";   }else{   echo "no";   };
?>
[root@mysql6~]# yum  -y  install  elinks    //安装测试网页工具
[root@mysql6~]#  elinks  --dump  http://localhost/test.php
   Ok                                  //验证测试页面成功
```

步骤三：安装软件包

1）物理机传输解压包给虚拟机192.168.4.6

```
[root@room9pc桌面]# scp phpMyAdmin-2.11.11-all-languages.tar.gz 19
root@192.168.4.6's password:
phpMyAdmin-2.11.11-a 100% 4218KB 122.5MB/s   00:00
```

2）虚拟机192.168.4.6解压phpMyAdmin-2.11.11-all-languages.tar.gz压缩包

Top

```
[root@mysql6~]# tar -zxf phpMyAdmin-2.11.11-all-languages.tar.gz -C /v
[root@mysql6~]# cd /var/www/html/
[root@mysql6~]# mv phpMyAdmin-2.11.11-all-languages phpmyadmin
[root@mysql6~]# chown -R apache:apache phpmyadmin/ //改变phpr
```

步骤四：修改软件的配置文件定义管理的数据库服务器

切换到部署后的phpmyadmin程序目录，拷贝配置文件，并修改配置以正确指定MySQL服务器的地址

```
[root@mysql6html]# cd phpmyadmin
[root@mysql6 phpmyadmin]# cp config.sample.inc.php config.inc.php
//备份主配置文件
[root@mysql6 phpmyadmin]# vim config.inc.php //编辑主配置文件
17 $cfg['blowfish_secret'] = 'plj123'; //给cookie做认证的值，可以随
31 $cfg['Servers'][$i]['host'] = 'localhost'; //指定主机名，定义连接哪台
:wq
```

步骤五：在客户端访问软件 管理数据库服务器

1）在客户端访问软件,打开浏览器输入http://192.168.4.6/phpmyadmin(数据库服务器地址) 访问软件，如图-2所示，用户名是root，密码是123456

Top

图-2

2）登入成功后，如图-3示，即可在授权范围内对MySQL数据库进行管理。

/

图-3

2 密码恢复及设置

2.1 问题

本案例要求密码恢复及设置，完成以下任务操作：

- 恢复MySQL管理列表
- 正常设置管理密码

2.2 步骤

实现此案例需要按照如下步骤进行。

步骤一：重置MySQL管理密码 Top

1）首先停止已运行的MySQL服务程序

```
[root@dbsvr1 ~]# systemctl  stop mysqld.service          //停止服务
[root@dbsvr1 ~]# systemctl  status mysqld.service        //确认状态
mysqld.service - MySQL Server
   Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled)
   Active: inactive (dead) since 五 2017-04-07 23:01:38 CST; 21s ago
     Docs: man:mysqld(8)
           http://dev.mysql.com/doc/refman/en/using-systemd.html
  Process: 20260 ExecStart=/usr/sbin/mysqld --daemonize --pid-file=/v
  Process: 20238 ExecStartPre=/usr/bin/mysqld_pre_systemd (code=ex
 Main PID: 20262 (code=exited, status=0/SUCCESS)
```

2）然后跳过授权表启动MySQL服务程序

这一步主要利用mysqld的 --skip-grant-tables选项

修改my.cnf配置，添加 skip_grant_tables=1启动设置：

```
[root@dbsvr1 ~]# vim /etc/my.cnf
[mysqld]
skip_grant_tables=1
.. ..
[root@dbsvr1 ~]# systemctl  restart mysqld.service
[root@dbsvr1 ~]# service mysql status
mysqld.service - MySQL Server
   Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled)
   Active: active (running) since 五 2017-04-07 23:40:20 CST; 40s ago
     Docs: man:mysqld(8)
           http://dev.mysql.com/doc/refman/en/using-systemd.html
  Process: 11698 ExecStart=/usr/sbin/mysqld --daemonize --pid-file=/v
  Process: 11676 ExecStartPre=/usr/bin/mysqld_pre_systemd (code=ex
 Main PID: 11701 (mysqld)
   CGroup: /system.slice/mysqld.service
           └─11701 /usr/sbin/mysqld --daemonize --pid-file=/var/run/m
```

Top

3）使用mysql命令连接到MySQL服务，重设root的密码

由于前一步启动的MySQL服务跳过了授权表，所以可以root从本机直接登录

```
[root@dbsvr1 ~]# mysql -u root
Enter password:                         //直接回车即可
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.17 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statemer

mysql>
```

进入 mysql> 环境后，通过修改mysql库中user表的相关记录，重设root用户从本机登录的密码：

```
mysql> UPDATE mysql.user SET authentication_string=PASSWORD('123
    -> WHERE user='root' AND host='localhost';          //重设root的密
Query OK, 1 row affected, 1 warning (0.00 sec)
Rows matched: 1  Changed: 1  Warnings: 1
mysql> FLUSH PRIVILEGES;                            //刷新授权表
Query OK, 0 rows affected (0.01 sec)
mysql> exit                                         //退出mysql> 环境
Bye
```

通过执行“FLUSH PRIVILEGES;”可使授权表立即生效，对于正常运行的MySQL服务，也可以用上述方法来修改密码，不用重启服务。本例中因为是恢复密码，最好重启MySQL服务程序，所以上述“FLUSH PRIVILEGES;”操作可跳过。

4）重新以正常方式启动MySQL服务程序，验证新密码

如果前面是修改/etc/my.cnf配置的方法来跳过授权表，则重置root密码后，应去除相应的设置以恢复正常：

Top

```
01.  [root@dbsvr1 ~]# vim /etc/my.cnf
02.  [mysqld]
03.  #skip_grant_tables=1                    //注释掉或删除此行
04.  .. ..
```

按正常方式，通过mysql脚本重启服务即可：

```
01.  [root@dbsvr1 ~]# systemctl  restart mysqld.service
```

验证无密码登录时，将会被拒绝：

```
01.  [root@dbsvr1 ~]# mysql -u root
02.  Enter password:                    //没有跳过授权表回车会报错
03.  ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using
```

只有提供重置后的新密码，才能成功登入：

```
01.  [root@dbsvr1 ~]# mysql -u root –p
02.  Enter password:
03.  Welcome to the MySQL monitor.  Commands end with ; or \g.
04.  Your MySQL connection id is 4
05.  Server version: 5.7.17 MySQL Community Server (GPL)
06.
07.  Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved
08.
09.  Oracle is a registered trademark of Oracle Corporation and/or its
10.  affiliates. Other names may be trademarks of their respective
11.  owners.
12.
13.  Type 'help;' or '\h' for help. Type '\c' to clear the current input statemer
14.
15.  mysql>
```

Top

步骤二：正常设置MySQL管理密码

正常的前提是：已知当前MySQL管理用户（root）的密码。

1）方法1，在Shell命令行下设置

使用mysqladmin管理工具，需要验证旧的密码。比如，以下操作将会把root的密码设置为 1234567：

```
01.  [root@dbsvr1 ~]# mysqladmin -u root -p password '1234567'
02.  Enter password:                          //验证原来的密码
03.  mysqladmin: [Warning] Using a password on the command line interface
04.  Warning: Since password will be sent to server in plain text, use ssl con
```

2）方法2，以root登入mysql> 后，使用SET PASSWORD指令设置

这个与新安装MySQL-server后首次修改密码时要求的方式相同，平时也可以用：

```
01.  mysql> SET PASSWORD FOR root@localhost=PASSWORD('1234567');
02.  Query OK, 0 rows affected, 1 warning (0.00 sec)
```

3）方法3，以root登入mysql> 后，使用GRANT授权工具设置

这个是最常见的用户授权方式（下一节会做更多授权的练习）：

```
01.  mysql> GRANT all ON *.* TO root@localhost IDENTIFIED BY '1234567';
02.  Query OK, 0 rows affected, 1 warning (0.00 sec)
```

4）方法4，以root登入mysql> 后，使用UPDATE更新相应的表记录

这种方法与恢复密码时的操作相同：

Top

```
mysql> UPDATE mysql.user SET authentication_string=PASSWORD('123
    -> WHERE user='root' AND host='localhost';        //重设root的密码
Query OK, 0 rows affected, 1 warning (0.00 sec)
Rows matched: 1  Changed: 0  Warnings: 1
mysql> FLUSH PRIVILEGES;                              //刷新授权表
Query OK, 0 rows affected (0.00 sec)
```

在上述方法中，需要特别注意：当MySQL服务程序以 skip-grant-tables 选项启动时，如果未执行“FLUSH PRIVILEGES;”操作，是无法通过SET PASSWORD或者GRANT方式来设置密码的。比如，验证这两种方式时，都会看到ERROR 1290的出错提示：

```
mysql> SET PASSWORD FOR root@localhost=PASSWORD('1234567');
ERROR 1290 (HY000): The MySQL server is running with the --skip-grant

mysql> GRANT all ON *.* TO root@localhost IDENTIFIED BY '1234567';
ERROR 1290 (HY000): The MySQL server is running with the --skip-grant
```

3 用户授权及撤销

3.1 问题

- 允许root从192.168.4.0/24网段 访问，对所有库/表有完全权限，密码为tarena
- 添加一个管理账号dba007，完全控制及授权
- 撤销root从本机访问的权限，然后恢复
- 允许webuser从任意客户机登录，只对webdb库有完全权限，密码为 888888
- 撤销webuser的完全权限，改为查询权限

3.2 方案

使用2台RHEL 7虚拟机，如图-1所示。其中192.168.4.10是MySQL服务器，授权及撤销操作均在此服务器上执行；而192.168.4.120作为测试客户机，需要安装好MySQL-client软件包，以便提供mysql命令。

Top

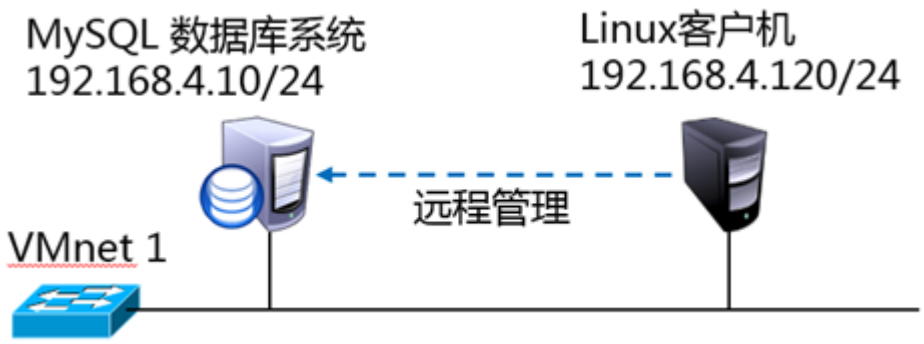

图-1

同时，MySQL服务器本身（192.168.4.10）也可以作为测试客户机。

3.3 步骤

实现此案例需要按照如下步骤进行。

步骤一：用户授权及撤销

1）允许root从192.168.4.0/24访问，对所有库表有完全权限，密码为tarena。

授权之前，从192.168.4.0/24网段的客户机访问时，将会被拒绝：

```
[root@host120 ~]# mysql -u root -p -h 192.168.4.10
Enter password:                          //输入正确的密码
ERROR 2003 (HY000): Host '192.168.4.120' is not allowed to connect
```

授权操作，此处可设置与从localhost访问时不同的密码：

```
mysql> GRANT all ON *.* TO root@'192.168.4.%' IDENTIFIED BY 'tarena
Query OK, 0 rows affected (0.00 sec)
```

再次从192.168.4.0/24网段的客户机访问时，输入正确的密码后可登入：

```
[root@host120 ~]# mysql -u root -p -h 192.168.4.10
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 20
Server version: 5.7.17 MySQL Community Server (GPL)
```

Top

```
06.
07.    Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved
08.
09.    Oracle is a registered trademark of Oracle Corporation and/or its
10.    affiliates. Other names may be trademarks of their respective
11.    owners.
12.
13.    Type 'help;' or '\h' for help. Type '\c' to clear the current input statemer
14.
15.    mysql>
```

从网络登入后，测试新建一个库、查看所有库：

```
01.    mysql> CREATE DATABASE rootdb;                    //创建新库rootdb
02.    Query OK, 1 row affected (0.06 sec)
03.
04.    mysql> SHOW DATABASES;
05.    +--------------------+
06.    | Database           |
07.    +--------------------+
08.    | information_schema |
09.    | home               |
10.    | mysql              |
11.    | performance_schema |
12.    | rootdb             |                    //新建的rootdb库
13.    | sys                |
14.    | userdb             |
15.    +--------------------+
16.    7 rows in set (0.01 sec)
```

2）在Mysql服务器上建立一个管理账号dba007，对所有库完全控制，并赋予其授权的权限

新建账号并授权：

Top

```
01.    mysql> GRANT all ON *.* TO dba007@localhost
```

```
    -> IDENTIFIED BY '1234567'
    -> WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)
```

查看dba007的权限：

```
mysql> SHOW GRANTS FOR dba007@localhost;
+-----------------------------------------------------------------+
| Grants for dba007@localhost                                     |
+-----------------------------------------------------------------+
| GRANT ALL PRIVILEGES ON *.* TO 'dba007'@'localhost' WITH GRANT
+-----------------------------------------------------------------+
1 row in set (0.00 sec)
```

3）撤销root从本机访问的权限，然后恢复

注意：如果没有事先建立其他管理账号，请不要轻易撤销root用户的本地访问权限，否则恢复起来会比较困难，甚至不得不重装数据库。

撤销root对数据库的操作权限：

```
mysql> REVOKE all ON *.* FROM root@localhost;
Query OK, 0 rows affected (0.00 sec)
mysql> SHOW GRANTS FOR root@localhost;
+-----------------------------------------------------+
| Grants for root@localhost                           |
+-----------------------------------------------------+
| GRANT USAGE ON *.* TO 'root'@'localhost' WITH GRANT OPTION  |
| GRANT PROXY ON ''@'' TO 'root'@'localhost' WITH GRANT OPTION |
+-----------------------------------------------------+
2 rows in set (0.00 sec)
```

验证撤销后的权限效果：

Top

```
mysql> exit                             //退出当前MySQL连接
```

```
02.  Bye
03.  [root@dbsvr1 ~]# mysql -u root -p                    //重新以root从本地登入
04.  Enter password:
05.  Welcome to the MySQL monitor.  Commands end with ; or \g.
06.  Your MySQL connection id is 6
07.  Server version: 5.6.15 MySQL Community Server (GPL)
08.
09.  Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved
10.
11.  Oracle is a registered trademark of Oracle Corporation and/or its
12.  affiliates. Other names may be trademarks of their respective
13.  owners.
14.
15.  Type 'help;' or '\h' for help. Type '\c' to clear the current input statemer
16.
17.  mysql> CREATE DATABASE newdb2014;                    //尝试新建库失败
18.  ERROR 1044 (42000): Access denied for user 'root'@'localhost' to data
19.  mysql> DROP DATABASE rootdb;                         //尝试删除库失败
20.  ERROR 1044 (42000): Access denied for user 'root'@'localhost' to data
```

尝试以当前的root用户恢复权限，也会失败（无权更新授权表）：

```
01.  mysql> GRANT all ON *.* TO root@localhost IDENTIFIED BY '1234567';
02.  ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using
```

怎么办呢？

退出当前MySQL连接，以上一步添加的管理账号dba007登入：

```
01.  mysql> exit                                         //退出当前MySQL连接
02.  Bye
03.  [root@dbsvr1 ~]# mysql -u dba007 -p                 //以另一个管理账号登
04.  Enter password:
05.  Welcome to the MySQL monitor.  Commands end with ; or \g.
06.  Your MySQL connection id is 24
```

Top

```
Server version: 5.7.17 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statemer
```

由管理账号dba007重新为root添加本地访问权限：

```
mysql> GRANT all ON *.* TO root@localhost IDENTIFIED BY '1234567';
Query OK, 0 rows affected (0.00 sec)
mysql> SHOW GRANTS FOR root@localhost;          //查看恢复结果
+-----------------------------------------------------------------+
| Grants for root@localhost                                       |
+-----------------------------------------------------------------+
| GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost' WITH GRANT OPT
| GRANT PROXY ON ''@'' TO 'root'@'localhost' WITH GRANT OPTION
+-----------------------------------------------------------------+
2 rows in set (0.00 sec)
```

退出，再重新以root登入，测试一下看看，权限又恢复了吧：

```
mysql> exit                             //退出当前MySQL连接
Bye
[root@dbsvr1 ~]# mysql -u root -p           //重新以root登入
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 25
Server version: 5.7.17 MySQL Community Server (GPL)
                                                          Top
Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved

```

```
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statemer

mysql> CREATE DATABASE newdb2014;              //成功创建新库
Query OK, 1 row affected (0.00 sec)
```

4）允许webuser从任意客户机登录，只对webdb库有完全权限，密码为 888888

添加授权：

```
mysql> GRANT all ON webdb.* TO webuser@'%' IDENTIFIED BY '888888
Query OK, 0 rows affected (0.00 sec)
```

查看授权结果：

```
mysql> SHOW GRANTS FOR webuser@'%';
+-----------------------------------------------+
| Grants for webuser@%                          |
+-----------------------------------------------+
| GRANT USAGE ON *.* TO 'webuser'@'%'           |
| GRANT ALL PRIVILEGES ON `webdb`.* TO 'webuser'@'%' |
+-----------------------------------------------+
2 rows in set (0.00 sec)
```

5）撤销webuser的完全权限，改为查询权限

撤销所有权限：

```
mysql> REVOKE all ON webdb.* FROM webuser@'%';
Query OK, 0 rows affected (0.00 sec)
```

Top

只赋予查询权限：

```
mysql> GRANT select ON webdb.* TO webuser@'%';
Query OK, 0 rows affected (0.00 sec)
```

确认授权更改结果：

```
mysql> SHOW GRANTS FOR webuser@'%';
+-----------------------------------------+
| Grants for webuser@%                    |
+-----------------------------------------+
| GRANT USAGE ON *.* TO 'webuser'@'%'     |
| GRANT SELECT ON `webdb`.* TO 'webuser'@'%' |
+-----------------------------------------+
2 rows in set (0.00 sec)
```

Top