

資料表自動 GrantSelect

Metadata

- 檔案所在 Server: 10.25.1.183
- 檔案所在資料夾：/opt/GrantSelect.sh
- 檔案執行時間：每日執行兩次(00:00, 12:00)
- 檔案執行身分：root
- crontab 位置：/etc/crontab

主程式 `GrantSelect.sh`

```
#!/bin/bash
#####
# Project: Grant the new tables if created on routine
# Branch: Privilege attained
# Author: Gok, the DBA
# Created: 2022-08-15
# Updated: 2022-08-16
# Note: focus on RD relevant account
#####

## parameter setting
mysql_user="root"
mysql_password="1qaz@WSX"
key_db="global_3rd_db"
key_user="rd"

## Get the new-made table list
get_tables="
    select table_name
    from information_schema.tables
    where table_schema = '$key_db'
        and create_time >= date(now() - interval 1 day)
    ;"
echo ''
echo [Get the new-made-table list]
echo $get_tables
table_list=`mysql -u $mysql_user -p$mysql_password -e "$get_tables"`
echo ''
echo $table_list
```

```

for table in $table_list;
do
    ## Find out the users with grant syntax
    grant_sql="
        select
            concat('GRANT SELECT ON $key_db.$table TO ', quote(user), '@', quote(host), ';')
        from mysql.user
        where user REGEXP '$key_user'
            and user <> 'gcprds'
        ;"
    echo ''
    echo [Find out the users with grant syntax]
    echo $grant_sql
    # Must check the list carefully if the some users jump into with the keyword randomly
    mysql -u $mysql_user -p$mysql_password -e "$grant_sql" >> grant.sql
    sed -i '/table_name/d' grant.sql
    sed -i '/concat/d' grant.sql
done

## see whether the grant.sql exists
if [ -f grant.sql ];
then
    echo ''
    echo [New table found! Source the grant syntax]
    cat grant.sql
    mysql -u $mysql_user -p$mysql_password -e "source grant.sql"
else
    echo ''
    echo "There is no new table to grant!"
fi

## remove the working file grant.sql
echo ''
echo [remove the working file grant.sql]
rm -f grant.sql

```

Note

- 只針對 global_3rd_db 新增的資料表進行 Grant
- Grant 的權限只有 Select
- Grant 的對象只有 '%rd%' 的 user, 'gcprds' 這帳號不更動(它有 Grant Select *.*)