CPPM & Mysql 对接

Ver 1.1

目录

1. 项目背景

1.1. 客户环境

客户 DOT1x 认证环境-MSChapv2，CPPM 现有情况下只支持 NT hash 与明文两种认证方式
客户 LDAP 环境：Novell LDAP 服务器，只支持 MD5 加密的 LDAP 对接，但支持多种加密方式写入到第三方数据库种

于是需要新增 Mysql/Oracl 数据库，由数据库分别与 LDAP 和 CPPM 对接

写这个文档是方便未来项目如果发生类似情况，可以自建开源 Mysql 做对接测试，或者直接用作与 Oracle 对接的参考

1.2. Mysql

1.2.1.参考链接

https://www.runoob.com/mysql/mysql-administration.html

1.2.2.RDBMS 术语

- **数据库:** 数据库是一些关联表的集合。
- **数据表:** 表是数据的矩阵。在一个数据库中的表看起来像一个简单的电子表格。
- **列:** 一列(数据元素) 包含了相同类型的数据, 例如邮政编码的数据。
- **行：**一行（=元组，或记录）是一组相关的数据，例如一条用户订阅的数据。
- **冗余**：存储两倍数据，冗余降低了性能，但提高了数据的安全性。
- **主键**：主键是唯一的。一个数据表中只能包含一个主键。你可以使用主键来查询数据。
- **外键：**外键用于关联两个表。
- **复合键**：复合键（组合键）将多个列作为一个索引键，一般用于复合索引。
- **索引：**使用索引可快速访问数据库表中的特定信息。索引是对数据库表中一列或多列的值进行排序的一种结构。类似于书籍的目录。
- **参照完整性:** 参照的完整性要求关系中不允许引用不存在的实体。与实体完整性是关系模型必须满足的完整性约束条件，目的是保证数据的一致性。

1.2.3.环境安装（Centos7）

https://www.centos.org/download/

最小化安装+配置完 IP 地址和 DNS 后

通过 yum 命令安装 wget

[root@localhost etc]# yum install wget

Loaded plugins: fastestmirror

Loading mirror speeds from cached hostfile

* base: mirrors.dgut.edu.cn

* extras: mirrors.cn99.com

* updates: mirrors.dgut.edu.cn

Resolving Dependencies

--> Running transaction check

---> Package wget.x86_64 0:1.14-18.el7_6.1 will be installed

--> Finished Dependency Resolution

1.2.4.Mysql 安装

1.get mysql 的安装包

[root@localhost etc]# wget http://repo.mysql.com/mysql-community-release-el7-5.noarch.rpm

--2021-09-07 11:51:37-- http://repo.mysql.com/mysql-community-release-el7-5.noarch.rpm

Resolving repo.mysql.com (repo.mysql.com)... 104.91.72.230

Connecting to repo.mysql.com (repo.mysql.com)|104.91.72.230|:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 6140 (6.0K) [application/x-redhat-package-manager]

Saving to: ‘mysql-community-release-el7-5.noarch.rpm’

100%[==========
==========
=====>] 6,140 --.-K/s in 0s

2021-09-07 11:51:38 (15.0 MB/s) - ‘mysql-community-release-el7-5.noarch.rpm’ saved [6140/6140]

2.安装 mysql rpm

[root@localhost ~]# rpm -ivh mysql-community-release-el7-5.noarch.rpm

Preparing... ## [100%]

Updating / installing...

1:mysql-community-release-el7-5 ## [100%]

3.更新 yum

[root@localhost ~]# yum update

Loaded plugins: fastestmirror

Loading mirror speeds from cached hostfile

* base: ftp.sjtu.edu.cn

* extras: ftp.sjtu.edu.cn

* updates: ftp.sjtu.edu.cn

mysql-connectors-community

| 2.6 kB 00:00:00

mysql-tools-community

| 2.6 kB 00:00:00

mysql56-community

| 2.6 kB 00:00:00

(1/3): mysql-tools-community/x86_64/primary_db

| 91 kB 00:00:03

(2/3): mysql-connectors-community/x86_64/primary_db

| 83 kB 00:00:05

(3/3): mysql56-community/x86_64/primary_db

| 297 kB 00:00:06

Resolving Dependencies

[root@localhost ~]# yum install mysql-server

Loaded plugins: fastestmirror

Loading mirror speeds from cached hostfile

* base: mirrors.dgut.edu.cn

* extras: mirrors.163.com

* updates: mirrors.dgut.edu.cn

Resolving Dependencies

--> Running transaction check

---> Package mysql-community-server.x86_64 0:8.0.26-1.el7 will be installed

--> Processing Dependency: mysql-community-common(x86-64) = 8.0.26-1.el7 for package:

mysql-community-server-8.0.26-1.el7.x86_64

--> Processing Dependency: mysql-community-client(x86-64) >= 8.0.11 for package:

1.2.5.初始化 Mysql

[root@localhost ~]# chown -R mysql:mysql /var/lib/mysql

[root@localhost ~]# mysqld --initialize

[root@localhost ~]# systemctl start mysqld

查看 mysql 进程状态

[root@localhost ~]# systemctl status mysqld

- mysqld.service - MySQL Community Server
  Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; vendor preset: disabled)
  Active: active (running) since Tue 2021-09-07 12:20:16 EDT; 5s ago
  Process: 56824 ExecStartPost=/usr/bin/mysql-systemd-start post (code=exited, status=0/SUCCESS)
  Process: 56763 ExecStartPre=/usr/bin/mysql-systemd-start pre (code=exited, status=0/SUCCESS)
  Main PID: 56823 (mysqld_safe)
  CGroup: /system.slice/mysqld.service
  ├─56823 /bin/sh /usr/bin/mysqld_safe --basedir=/usr
  └─57001 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql/plugin
--log-error=/var/log/mysqld.log --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/lib/mysql/mysql.sock

1.2.6.设置 Mysql 初始化密码

[root@localhost ~]# mysqladmin -u root password "Aruba123"

Warning: Using a password on the command line interface can be insecure.

1.2.7.设置远程登录权限

修改 my.cnf 文件开放插入用户权限

[root@localhost ~]# vi /etc/my.cnf

sql_mode=NO_ENGINE_SUBSTITUTION,STRICT_TRANS_TABLES

指定了严格模式，为了安全，严格模式禁止通过 insert 这种形式直接修改 mysql 库中的 user 表进行添加新用户

登录到 Mysql 数据库

[root@localhost ~]# mysql -u root -p

Enter password:

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 4

Server version: 5.6.51 MySQL Community Server (GPL)

1.2.8.插入远程管理用户

登录数据库

mysql> use mysql

Reading table information for completion of table and column names

You can turn off this feature to get a quicker startup with -A

Database changed

插入用户

mysql> INSERT INTO user

-> (host,user,password,select_priv,insert_priv,update_priv,Delete_priv,Create_priv,Drop_priv,Reload_priv,Grant_priv,Alter_priv,Shutdown_priv)

-> VALUES ('%','guest',PASSWORD('Aruba!23'),'Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y');

Query OK, 1 row affected, 3 warnings (0.00 sec)

权限刷新

mysql> FLUSH PRIVILEGES;

Query OK, 0 rows affected (0.00 sec)

关闭防火墙

[root@localhost ~]# systemctl stop firewalld.service

[root@localhost ~]# systemctl status firewalld.service

● firewalld.service - firewalld - dynamic firewall daemon

Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)

Active: inactive (dead) since Wed 2021-09-08 01:53:30 EDT; 5s ago

Docs: man:firewalld(1)

Process: 759 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (code=exited, status=0/SUCCESS)

Main PID: 759 (code=exited, status=0/SUCCESS)

Sep 08 01:35:49 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...

Sep 08 01:35:52 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.

Sep 08 01:35:52 localhost.localdomain firewalld[759]: WARNING: AllowZoneDrifting is enabled. This is considered an insecure configuration...it now.

Sep 08 01:53:30 localhost.localdomain systemd[1]: Stopping firewalld - dynamic firewall daemon...

Sep 08 01:53:30 localhost.localdomain systemd[1]: Stopped firewalld - dynamic firewall daemon.

Hint: Some lines were ellipsized, use -l to show in full.

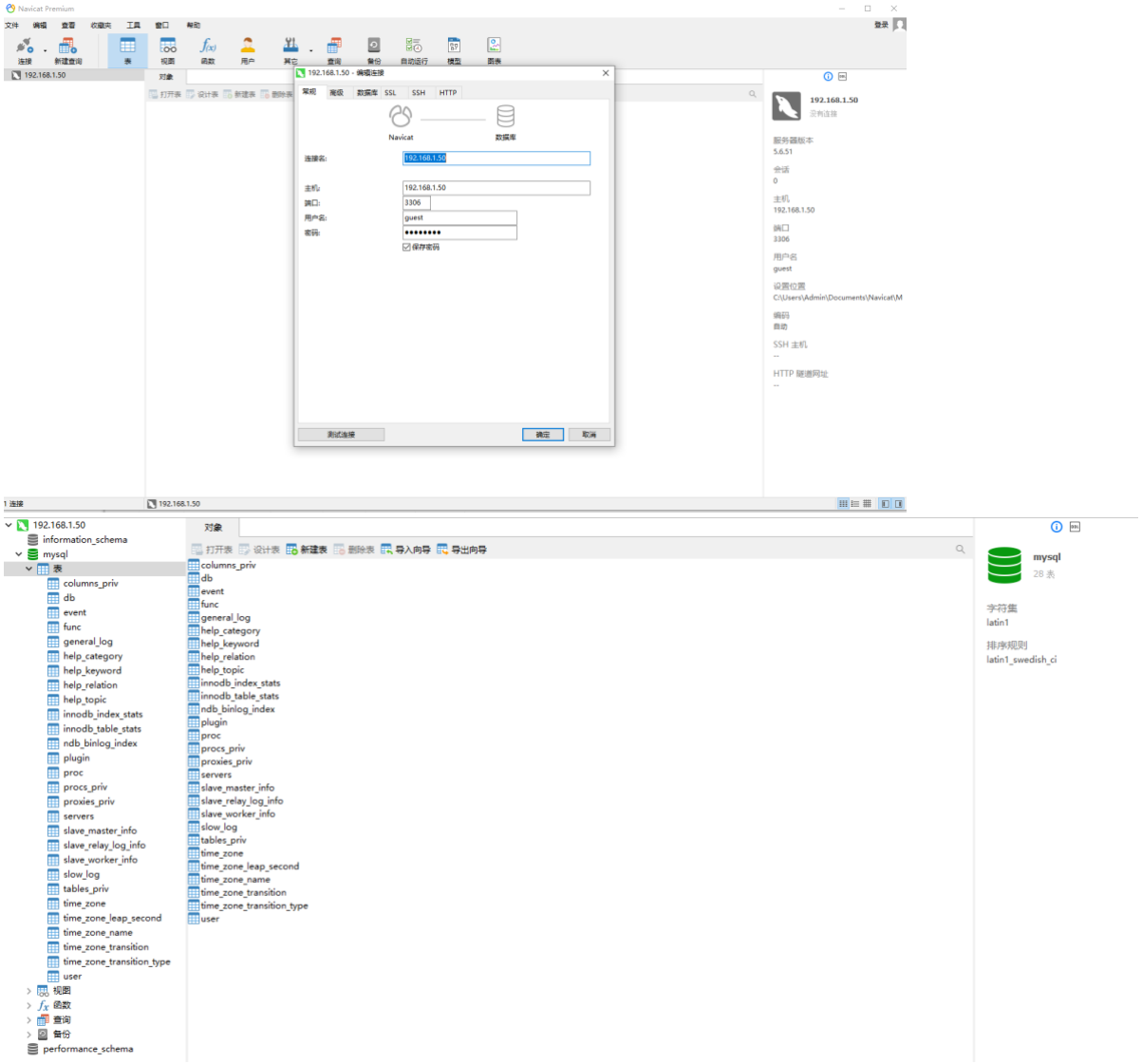
1.2.9.新建数据库

mysql> create database aruba ;

Query OK, 1 row affected (0.00 sec)

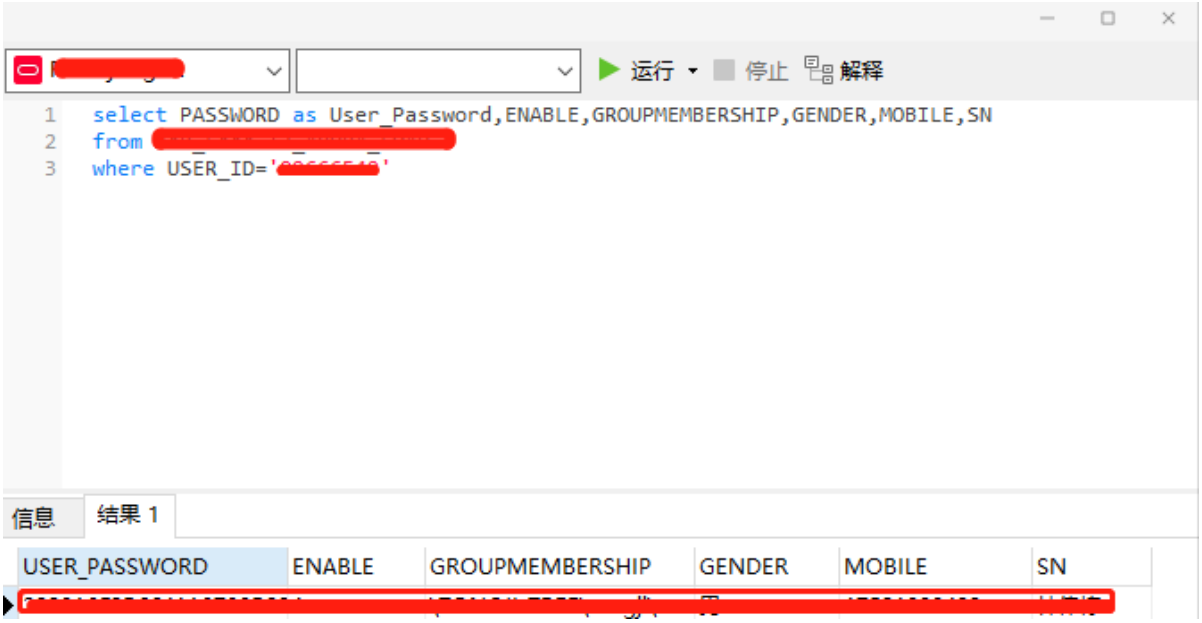
1.2.10. Mysql 数据库图形化软件（强烈推荐）

http://www.navicat.com.cn/products/



1.2.10.1. 查询测试

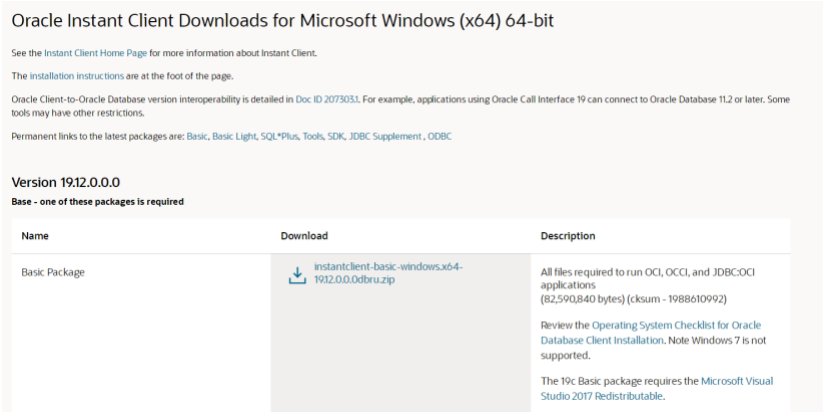
右键数据库-新建查询

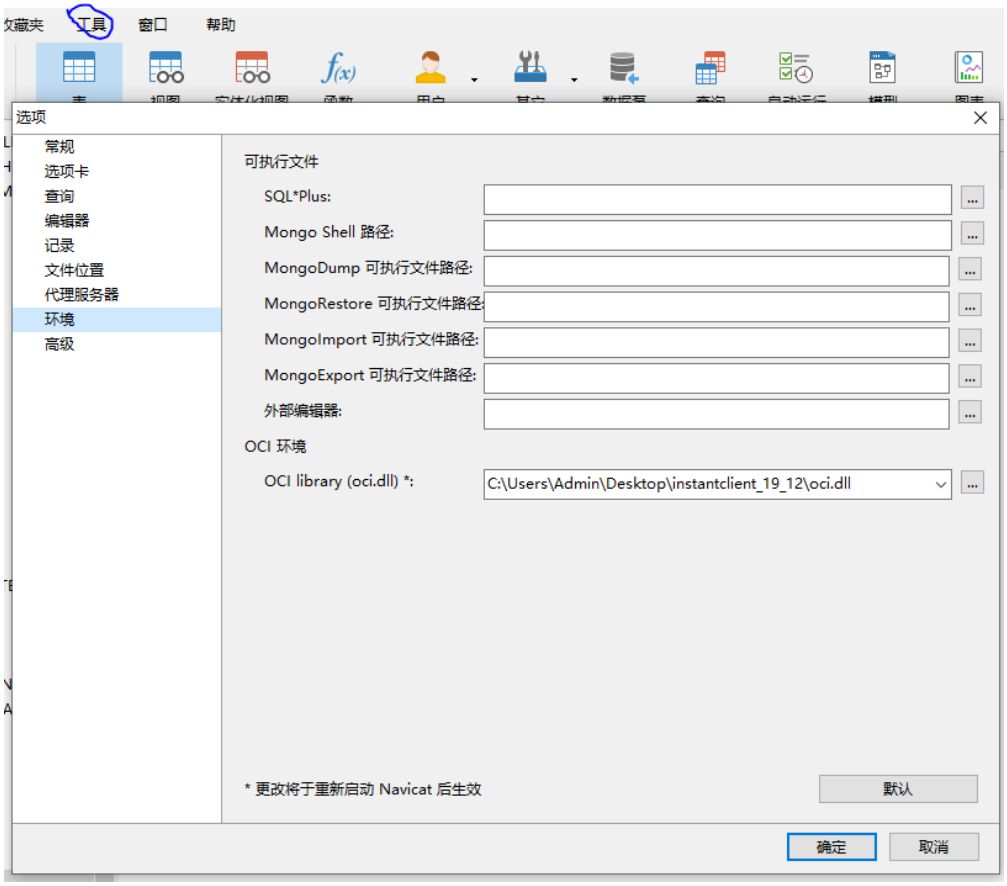


1.2.10.2. ORACL 驱动补丁

需要打补丁后可以登录 Oracle 服务器

https://www.oracle.com/database/technologies/instant-client/downloads.html



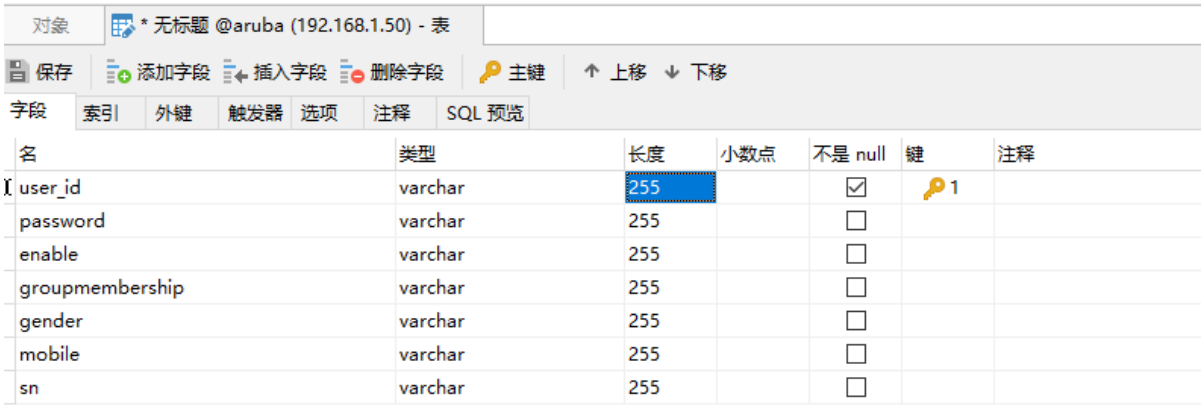


1.3. ClearPass

1.3.1.对接数据库字段

数据库字段名与 ClearPass 字段需要严格对应

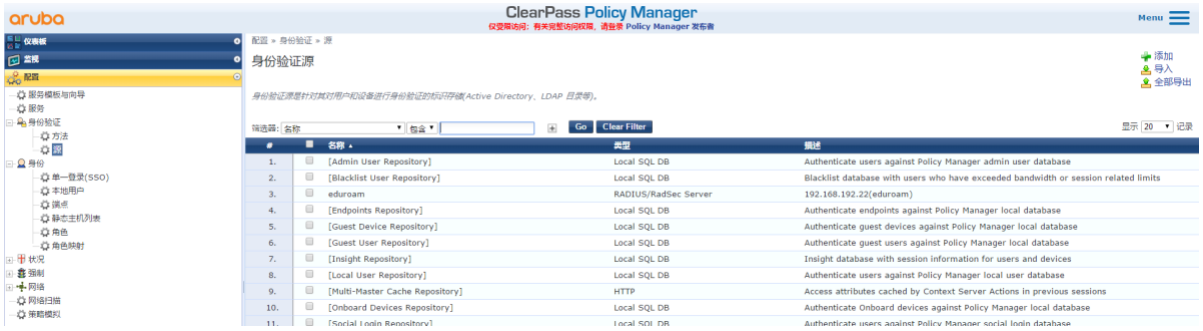
user_id varchar(255)
password varchar(255)
enable varchar(255)
groupmembership varchar(255)
gender varchar(255)
mobile varchar(255)
sn varchar(255)



名	类型	长度	小数点	不是 null	键	注释
user_id	varchar	255		☑	1	
password	varchar	255		☐		
enable	varchar	255		☐		
groupmembership	varchar	255		☐		
gender	varchar	255		☐		
mobile	varchar	255		☐		
sn	varchar	255		☐		

1.3.2.CPPM 添加 Mysql 对接

1.3.2.1. 添加认证源



1.3.2.2. 选择 Generic SQL DB 方式

1.3.3.数据库对接配置

1.3.3.1. MySQL

服务器名称设置 IP 地址+3306（mysql 默认对接端口）

MYSQL 查询字段

select password as User_Password,enable,groupmembership,gender,mobile,sn

from 表名

where user_id='%{Authentication:Username}'

Tables 填写实际表名

CPPM&MySQL 对接 Request 数据包（CPPM 界面的 Database name=数据库名）

```
199 2021-09-09 07:11:39.764116 192.168.134.209 192.168.134.215 MySQL 233 0xc490 (50320) Login Request user=guest1 db=mysql
200 2021-09-09 07:11:39.764325 192.168.134.215 192.168.134.209 TCP 62 0xe45b (58459) 3306 → 58592 [ACK] Seq=79 Ack=178 Win=30336 Len=0
201 2021-09-09 07:11:39.764438 192.168.134.215 192.168.134.209 MySQL 67 0xe45c (58460) Response OK
202 2021-09-09 07:11:39.764511 192.168.134.209 192.168.134.215 MySQL 66 0xc491 (50321) Request Use Database
203 2021-09-09 07:11:39.764697 192.168.134.215 192.168.134.209 MySQL 67 0xe45d (58461) Response OK
204 2021-09-09 07:11:39.764764 192.168.134.209 192.168.134.215 MySQL 91 0xc492 (50322) Request Query
205 2021-09-09 07:11:39.764988 192.168.134.215 192.168.134.209 MySQL 67 0xe45e (58462) Response OK
206 2021-09-09 07:11:39.765052 192.168.134.209 192.168.134.215 MySQL 77 0xc493 (50323) Request Query
```

1.3.3.2. Oracle

Oracle 支持 11g 以上版本（虽然配置界面只到 11g，测试 12C 通过）

Oracle 远程访问必须字段（地址+端口+服务名+用户名+密码）

ORACL 查询字段,需要含数据库名

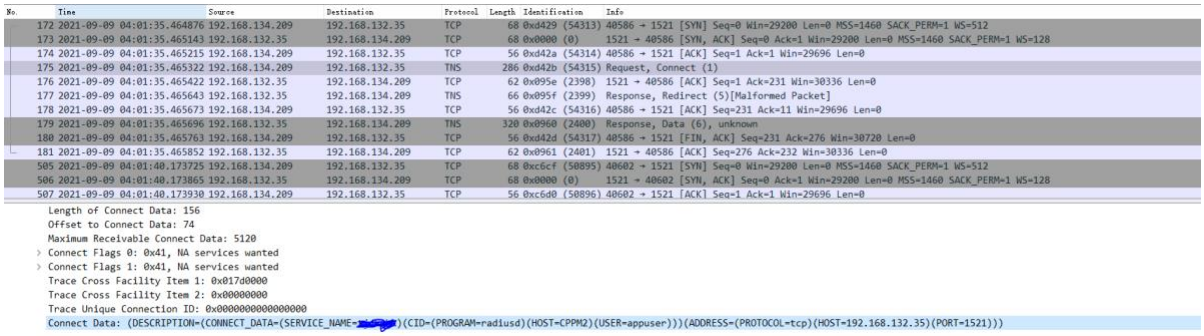
select PASSWORD as User_Password,ENABLE,GROUPMEMBERSHIP,GENDER,MOBILE,SN

from 数据库.表

where USER_ID='%{Authentication:Username}'

ClearPass 数据库名称对应服务名

CPPM&ORACLE 对接 Request 数据包（CPPM 界面的 Database name=service name）



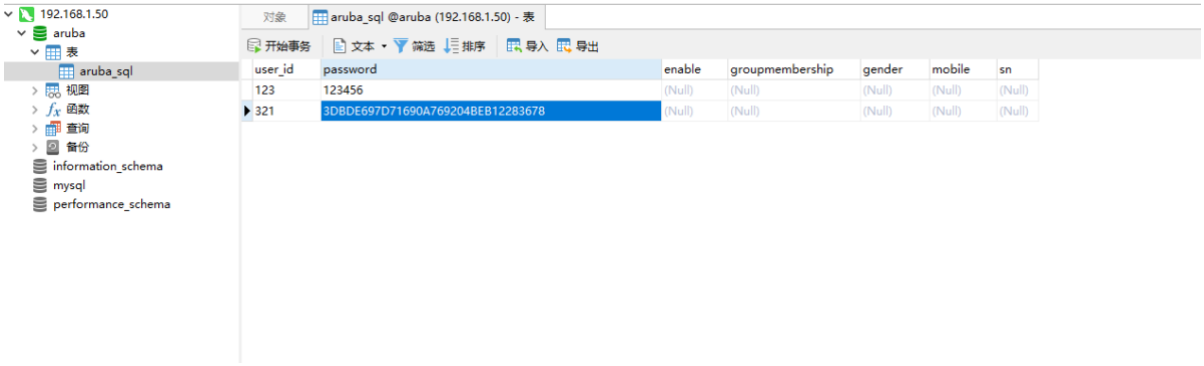
1.3.4.加密方式

1.3.4.1. 明文

1.3.4.2. NTHash

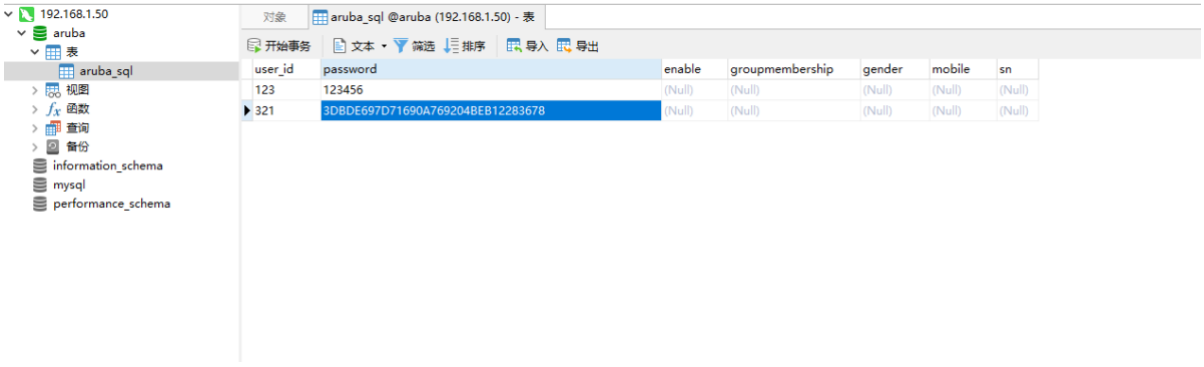
1.3.5.测试用户写入

1.3.5.1. 明文用户



1.3.5.2. NT Hash 用户

123 nt hash 值 = 3DBDE697D71690A769204BEB12283678



1.3.6.对接成功


请求详细信息
摘要
输入
输出
记帐
登录状态:
ACCEPT
会话标识符:
R00000332-02-61306753
日期和时间:
Sep 02, 2021 13:55:31 CST
终端主机标识符:
E0-CC-F8-B3-A3-C7
用户名:
123
访问设备 IP/端口:
172.21.2.40
访问设备名称:
系统状况状态:
UNKNOWN (100)
使用的策略 -
服务:
Aruba-AC-1xAuth_new
身份验证方法:
EAP-PEAP,EAP-MSCHAPv2
身份验证源:
Sql:192.168.134.215
授权源:
角色:
[User Authenticated], 学生角色
强制配置文件:
[Allow Access Profile]
显示第 8 条记录，共 1-20 条
更改状态
显示配置
导出
显示日志
关闭