

CPPM & Mysql 对接

Ver 1.1

目录

1. 项目背景.....	4
1.1. 客户环境	4
1.2. Mysql	4
1.2.1. 参考链接.....	4
1.2.2. RDBMS 术语.....	4
1.2.3. 环境安装（Centos7）	5
1.2.4. Mysql 安装.....	5
1.2.5. 初始化 Mysql.....	6
1.2.6. 设置 Mysql 初始化密码.....	7
1.2.7. 设置远程登录权限.....	7
1.2.8. 插入远程管理用户	7
1.2.9. 新建数据库.....	8
1.2.10. Mysql 数据库图形化软件（强烈推荐）	9
1.3. ClearPass.....	11
1.3.1. 对接数据库字段.....	11
1.3.2. CPPM 添加 Mysql 对接	12
1.3.3. 数据库对接配置.....	13

1.3.4. 加密方式.....	16
1.3.5. 测试用户写入.....	17
1.3.6. 对接成功.....	18

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/Oracle 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)

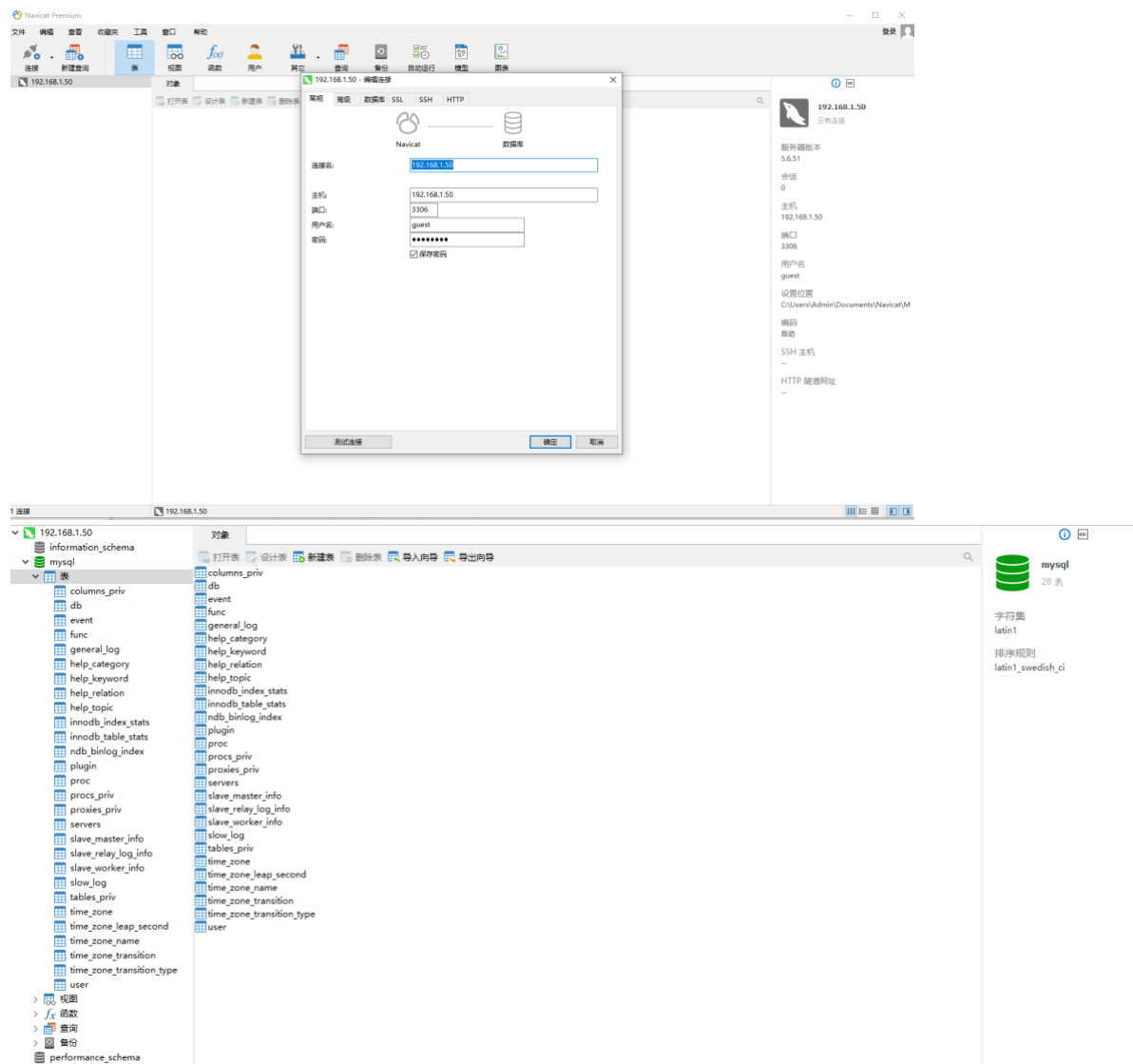
Sep 08 01:35:49 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...
Sep 08 01:35:52 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
Sep 08 01:35:52 localhost.localdomain firewalld[759]: WARNING: AllowZoneDrifting is enabled. This is considered 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)
```

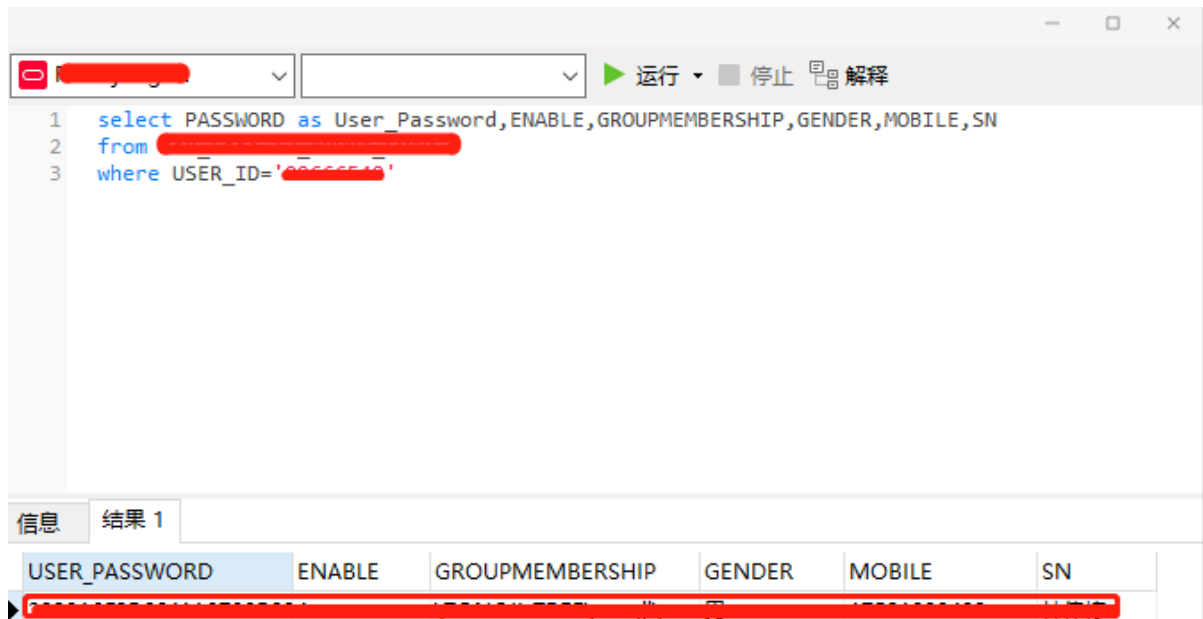

1.2.10. Mysql 数据库图形化软件 (强烈推荐)

<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>

Oracle Instant Client Downloads for Microsoft Windows (x64) 64-bit

See the [Instant Client Home Page](#) for more information about Instant Client.

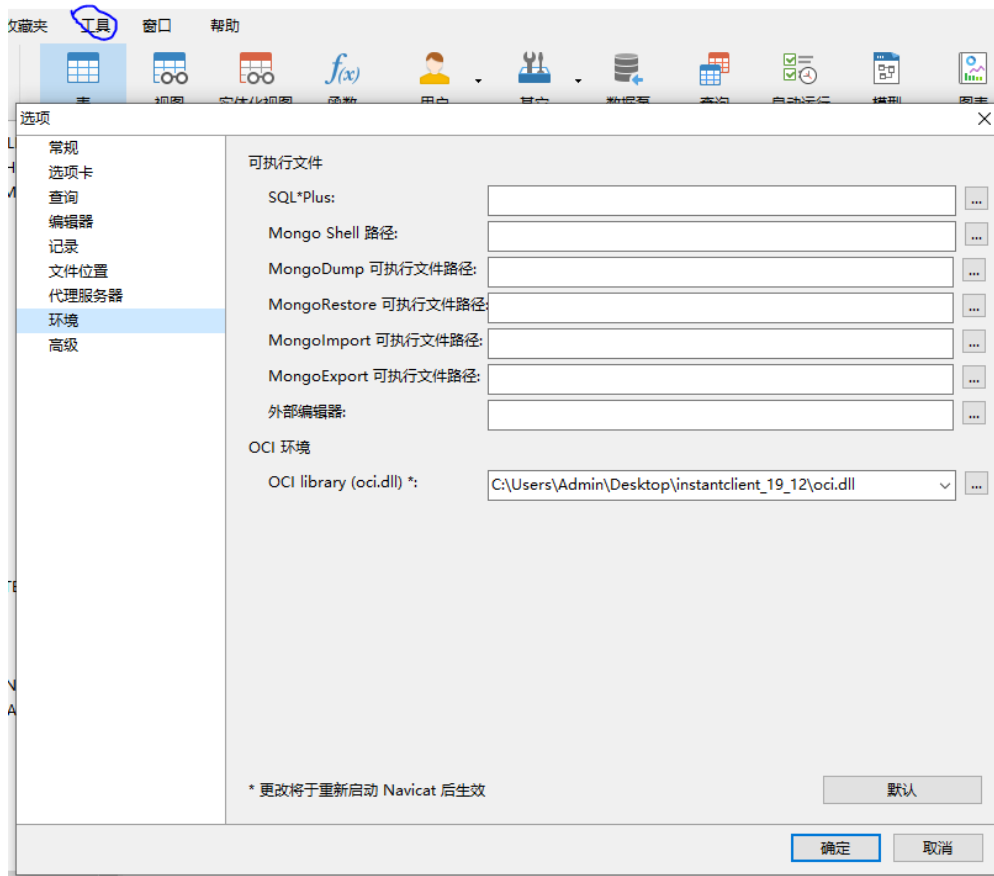
The installation instructions are at the foot of the page.

Oracle Client-to-Oracle Database version interoperability is detailed in Doc ID 2073051. For example, applications using Oracle Call Interface 19 can connect to Oracle Database 11.2 or later. Some tools may have other restrictions.

Permanent links to the latest packages are: [Basic](#), [Basic Light](#), [SQL*Plus](#), [Tools](#), [SDK](#), [JDBC Supplement](#), [ODBC](#).

Version 19.12.0.0.0
Base - one of these packages is required

Name	Download	Description
Basic Package	InstantClient-basic-windows.x64-1912.0.0.odbru.zip	All files required to run OCI, OCCI, and JDBC-OCI applications (82,590,840 bytes) (cksum - 1988610992) Review the Operating System Checklist for Oracle Database Client Installation. Note Windows 7 is not supported. The 19c Basic package requires the Microsoft Visual Studio 2017 Redistributable.



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		<input checked="" type="checkbox"/>	1	
password	varchar	255		<input type="checkbox"/>		
enable	varchar	255		<input type="checkbox"/>		
groupmembership	varchar	255		<input type="checkbox"/>		
gender	varchar	255		<input type="checkbox"/>		
mobile	varchar	255		<input type="checkbox"/>		
sn	varchar	255		<input type="checkbox"/>		

1.3.2.CPPM 添加 Mysql 对接

1.3.2.1. 添加认证源

ClearPass Policy Manager 身份验证源配置界面。显示了已配置的身份验证源列表，包括 Admin User Repository, Blacklist User Repository, eduroam, Endpoints Repository, Guest Device Repository, Insight Repository, Local User Repository, Multi-Master Cache Repository, Onboard Devices Repository, 和 Social Login Repository。

1.3.2.2. 选择 Generic SQL DB 方式

身份验证源 - Test-MySQL

摘要	常规	主要	属性
名称:	TestMySQL		
描述:			
类型:	Generic SQL DB		
用于授权:	<input checked="" type="checkbox"/> 同时启用此身份验证源来获取角色映射属性		
授权源:	<input type="text"/> <input type="button" value="删除"/> <input type="button" value="查看详细信息"/> -- Select --		
缓存超时:	36000 秒		
备份服务器优先级:	<input type="text"/> <input type="button" value="上移"/> <input type="button" value="下移"/> <input type="button" value="添加备份"/> <input type="button" value="删除"/>		

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}'

身份验证源 - Test-MySQL

摘要	常规	主要	属性
服务器名称:	192.168.134.215		
端口(可选):	3306 (仅当您希望覆盖默认值时指定)		
数据库名称:	mysql		
登录用户名:	guest1		
登录密码:		
超时:	10 秒		
ODBC 驱动程序:	MariaDB ▼		
密码类型:	明文 ▼		

Tables 填写实际表名

配置筛选器

配置

筛选器名称: Authen

筛选器查询: select password as User_Password,enable,groupmembership,gender,mobile,sn from tables where user_id=%{Authentication:Username}

名称	别名	数据类型	启用方式
1. enable	enable	String	-
2. groupmembership	groupmembership	String	-
3. gender	gender	String	-
4. mobile	mobile	String	-
5. sn	sn	String	-
6. Click to add...			

保存 关闭

配置 > 身份验证 > 源 > 添加 - Test-MySQL

身份验证源 - Test-MySQL

摘要 常规 主要 属性

指定用于获取身份验证和授权属性的筛选器查询

筛选器名称	属性名称	别名	启用方式
Authen	enable	enable	-
	groupmembership	groupmembership	-
	gender	gender	-
	mobile	mobile	-
	sn	sn	-

添加更多筛选器

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

RAC-tjdbgbk - 编辑连接

常规 高级 数据库 SSH

Navicat 数据库

连接名: test

连接类型: Basic

主机: 11.1.1.1

端口: 1521

服务名: test

服务名 SID

用户名: usr_aruba

密码: ●●●●●●

保存密码

测试连接 确定 取消

身份验证源 - Oracle

摘要 常规 主要 属性

服务器名称:	ttttt
端口(可选):	1521 (仅当您希望覆盖默认值时指定)
数据库名称:	tttt
登录用户名:	admin
登录密码:	●●●●●●
超时:	10 秒
ODBC 驱动程序:	Oracle 11g
密码类型:	NT 哈希

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

No.	Time	Source	Destination	Protocol	Length	Identification	Info
172	2021-09-09 04:01:35.464876	192.168.134.209	192.168.132.35	TCP	68	0xd429 (54313)	40586 → 1521 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=512
173	2021-09-09 04:01:35.465143	192.168.132.35	192.168.134.209	TCP	68	0x0000 (0)	1521 → 40586 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
174	2021-09-09 04:01:35.465215	192.168.134.209	192.168.132.35	TCP	56	0xd42a (54314)	40586 → 1521 [ACK] Seq=1 Ack=1 Win=29696 Len=0
175	2021-09-09 04:01:35.465322	192.168.134.209	192.168.132.35	TCP	286	0xd42b (54315)	Request, Connect (1)
176	2021-09-09 04:01:35.465422	192.168.132.35	192.168.134.209	TCP	62	0x095e (2398)	1521 → 40586 [ACK] Seq=1 Ack=231 Win=30336 Len=0
177	2021-09-09 04:01:35.465643	192.168.132.35	192.168.134.209	TCP	66	0x095f (2399)	Response, Redirect (5)[Malformed Packet]
178	2021-09-09 04:01:35.465673	192.168.134.209	192.168.132.35	TCP	56	0xd42c (54316)	40586 → 1521 [ACK] Seq=231 Ack=11 Win=29696 Len=0
179	2021-09-09 04:01:35.465696	192.168.132.35	192.168.134.209	TCP	320	0x0960 (2400)	Response, Data (6), unknown
180	2021-09-09 04:01:35.465763	192.168.134.209	192.168.132.35	TCP	56	0xd42d (54317)	40586 → 1521 [FIN, ACK] Seq=231 Ack=276 Win=30720 Len=0
181	2021-09-09 04:01:35.465852	192.168.132.35	192.168.134.209	TCP	62	0x0961 (2401)	1521 → 40586 [ACK] Seq=276 Ack=232 Win=30336 Len=0
505	2021-09-09 04:01:40.173725	192.168.134.209	192.168.132.35	TCP	68	0xc6cf (50895)	40602 → 1521 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=512
506	2021-09-09 04:01:40.173805	192.168.132.35	192.168.134.209	TCP	68	0x0000 (0)	1521 → 40602 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
507	2021-09-09 04:01:40.173930	192.168.134.209	192.168.132.35	TCP	56	0xc6d0 (50896)	40602 → 1521 [ACK] Seq=1 Ack=1 Win=29696 Len=0

Length of Connect Data: 156
Offset to Connect Data: 74
Maximum Receivable Connect Data: 5120
> Connect Flags 0: 0xd1, NA services wanted
> Connect Flags 1: 0xd1, NA services wanted
Trace Cross Facility Item 1: 0x017d0000
Trace Cross Facility Item 2: 0x00000000
Trace Unique Connection ID: 0x0000000000000000
Connect Data: (DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=XXXXXXXXXX)(CID=(PROGRAM=radiusd)(HOST=CPPM2)(USER=appuser))))(ADDRESS=(PROTOCOL=tcp)(HOST=192.168.132.35)(PORT=1521)))

1.3.4.加密方式

1.3.4.1. 明文

身份验证源 - Test-MySQL

摘要	常规	主要	属性
服务器名称:			
		192.168.134.215	
端口(可选):			
		3306 (仅当您希望覆盖默认值时指定)	
数据库名称:			
		mysql	
登录用户名:			
		guest1	
登录密码:			
		
超时:			
		10 秒	
ODBC 驱动程序:			
		MariaDB	
密码类型:			
		明文	

1.3.4.2. NTHash

身份验证源 - Test-MySQL

摘要	常规	主要	属性
服务器名称:	<input type="text" value="192.168.134.215"/>		
端口(可选):	<input type="text" value="3306"/> (仅当您希望覆盖默认值时指定)		
数据库名称:	<input type="text" value="mysql"/>		
登录用户名:	<input type="text" value="guest1"/>		
登录密码:	<input type="password" value="....."/>		
超时:	<input type="text" value="10"/> 秒		
ODBC 驱动程序:	MariaDB ▼		
密码类型:	NT 哈希 ▼		

1.3.5.测试用户写入

1.3.5.1. 明文用户

The screenshot shows a SQL Server Enterprise Manager interface. On the left, a tree view shows the server '192.168.1.50' with a database 'aruba' containing a table 'aruba_sql'. The main pane displays the 'aruba_sql' table with the following data:

user_id	password	enable	groupmembership	gender	mobile	sn
123	123456	(Null)	(Null)	(Null)	(Null)	(Null)
321	3DBDE697D71690A769204BEB12283678	(Null)	(Null)	(Null)	(Null)	(Null)

1.3.5.2. NT Hash 用户

123 nt hash 值 = 3DBDE697D71690A769204BEB12283678

The screenshot shows a SQL Server Enterprise Manager interface. On the left, a tree view shows the server '192.168.1.50' with a database 'aruba' containing a table 'aruba_sql'. The main pane displays the 'aruba_sql' table with the following data:

user_id	password	enable	groupmembership	gender	mobile	sn
123	123456	(Null)	(Null)	(Null)	(Null)	(Null)
321	3DBDE697D71690A769204BEB12283678	(Null)	(Null)	(Null)	(Null)	(Null)

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:	[REDACTED]
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:	[REDACTED]
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