**全密态数据库加密网关实施方案**

版本：V1.0

**渔翁信息技术股份有限公司**

|  |
| --- |
| 地 址：威海市高区初河北路12号渔翁信息安全产业园 |
| 邮 编：264200 |
| 网 站：<https://www.fisec.cn> |
| 电 话：400-6686-188 |

1. 目的

全密态数据库加密网关（后简称为网关）实施方案编写的目的是让客户快速了解网关的使用方式，以及呈现的效果。包括四个方面，设备部署的网络拓扑，测试业务的部署，集群模式的实施方案，内存镜像模式实施方案。

1. 设备网络拓扑

网关采用旁路方式部署，与演示业务服务器部署在同一个网络中。

1. 测试业务服务部署
   1. 安装业务环境

准备X86\_64 Centos 7设备，按照《业务系统部署说明》的步骤进行部署

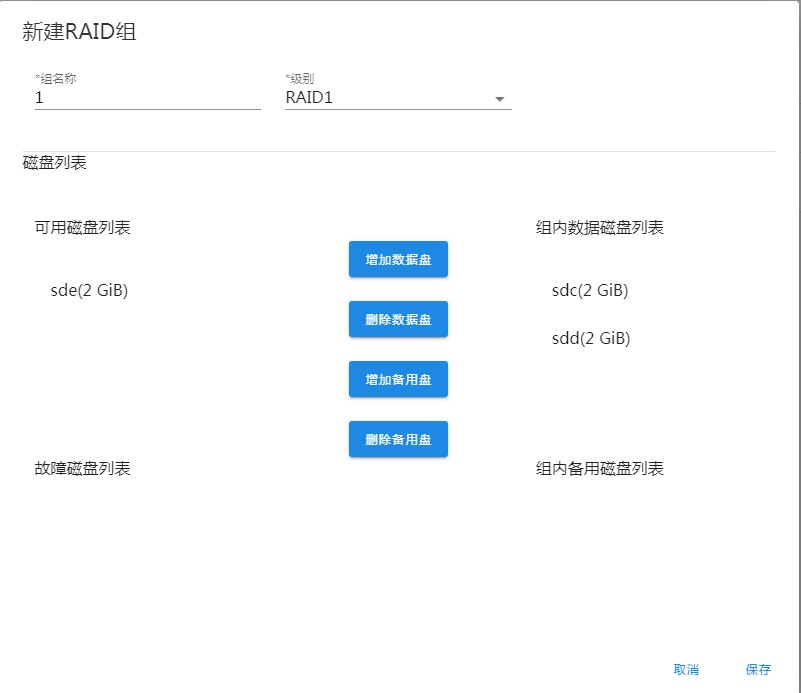
* 1. 配置演示业务系统

业务效果：



1. 集群模式方案
   1. 配置数据库加密步骤
      1. RAID组管理

进入RAID组管理模块，点击右上角【新建RAID】

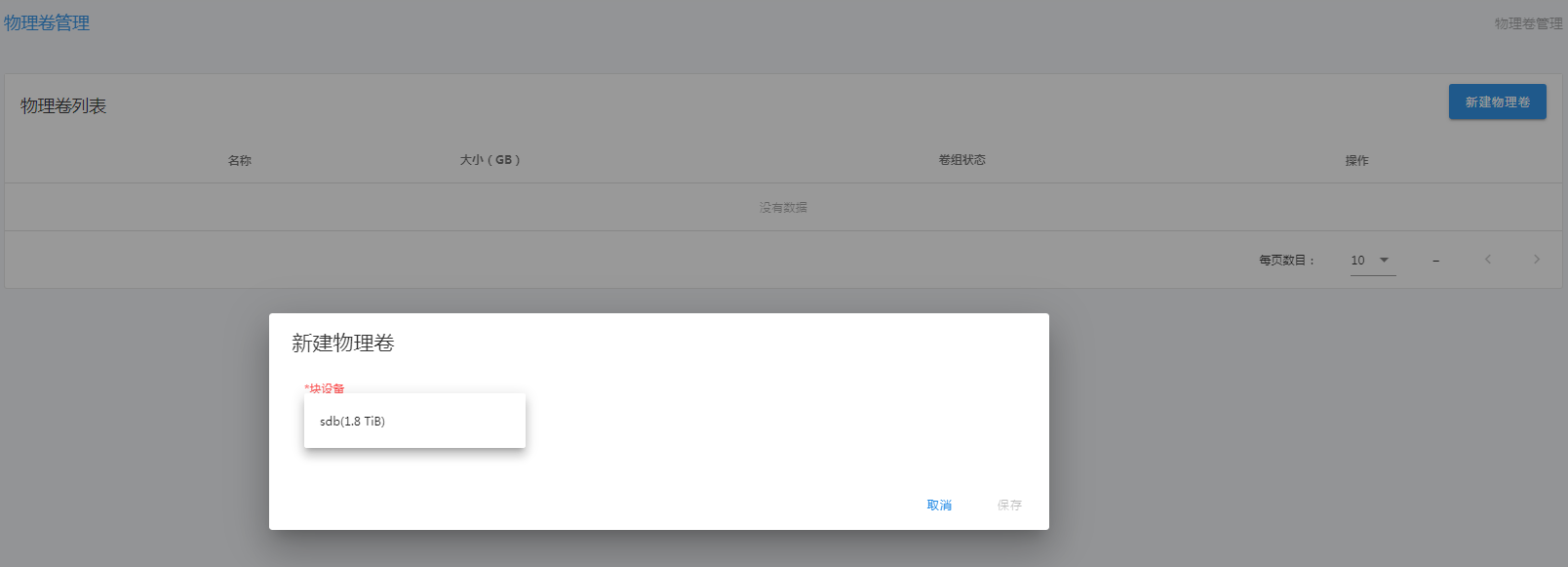


按需填写组名称，注意只能填写数字，级别选择RAID1，可用磁盘列表中选中两个硬盘，点击“增加数据盘”，组内数据磁盘列表中就会出现选中的两个硬盘，点击【保存】，raid组配置完成。配置完成后显示如下：

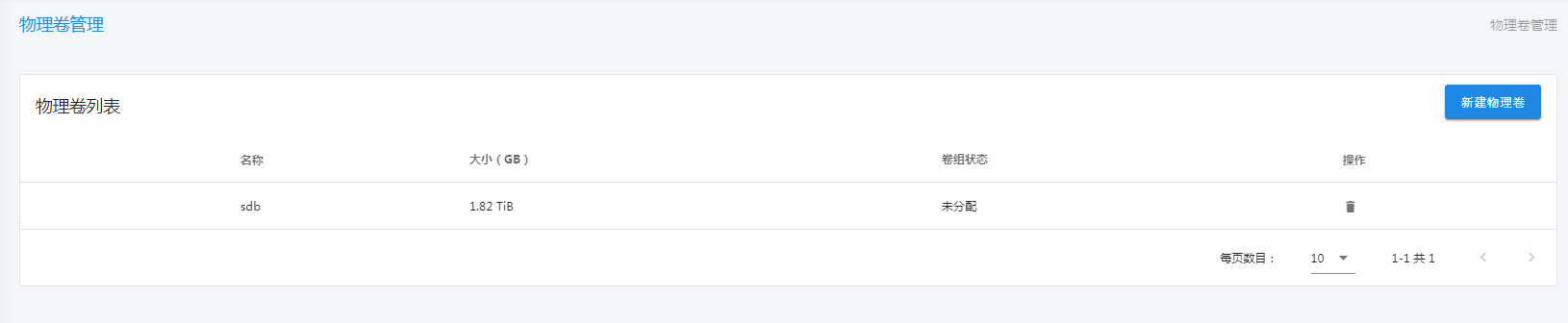


* + 1. 物理卷管理

配置RAID之后，进入物理卷管理模块，点击右上角【新建物理卷】

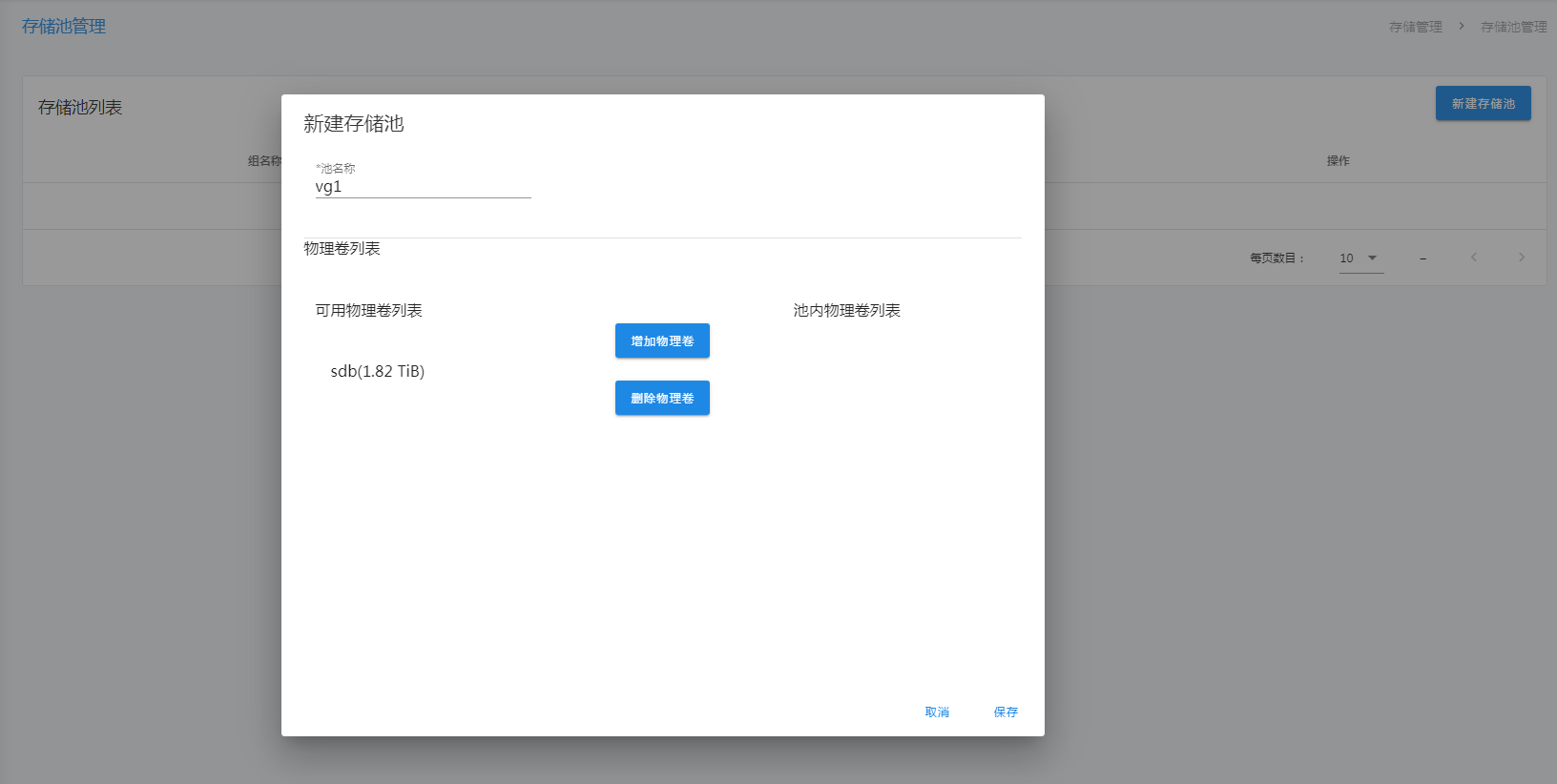


在弹窗中的下拉框选择要添加的物理卷，建议将下拉框中所有出现的块设备都添加为物理卷。配置完成后显示如下：

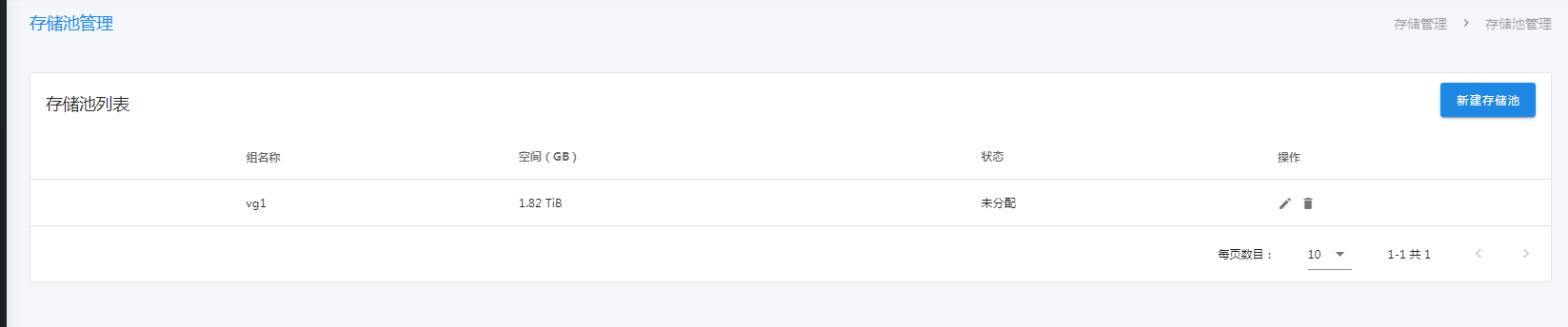


* + 1. 存储池管理

配置完物理卷后，进入存储池管理模块，点击右上角【新建存储池】

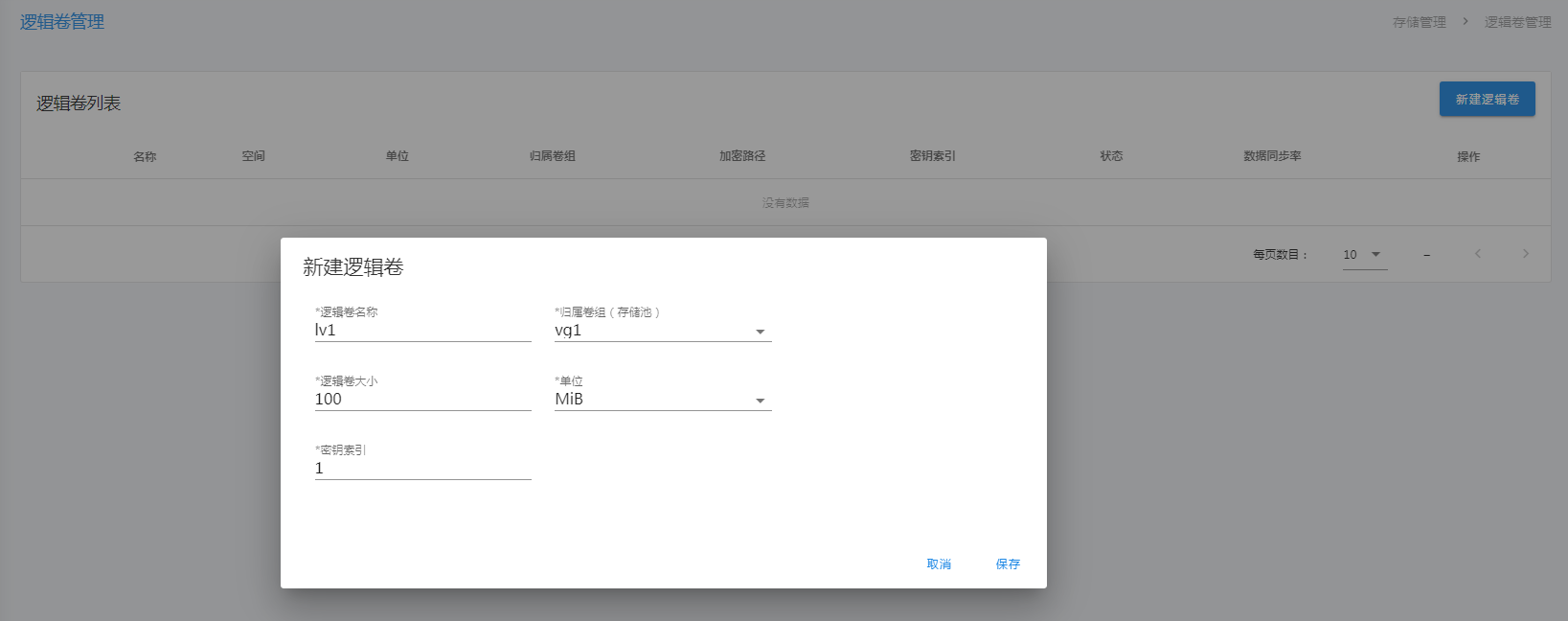


按需填写池名称，在左侧的可用物理卷列表中选中要加入池中的物理卷，可以任选n个，点击【增加物理卷】，右侧池内物理卷列表会显示选中的物理卷，点击【保存】，配置完成后显示如下：



* + 1. 逻辑卷管理

配置完存储池之后进入逻辑卷管理模块，点击右上角新建逻辑卷

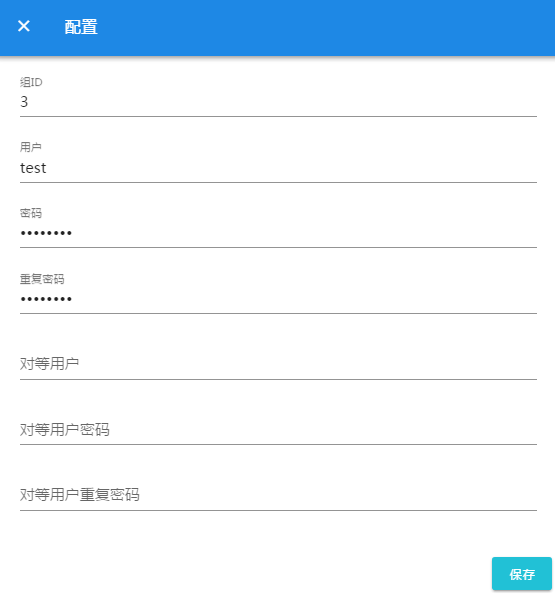


按需填写逻辑卷名称，选择归属卷组（存储池），填写逻辑卷的大小和存储单位，以及需要使用的密钥索引（可任意不可重复）。配置完成后显示如下：



* + 1. CHAP认证管理

配置完逻辑卷管理后，进入CHAP认证管理模块，点击右上角【添加】

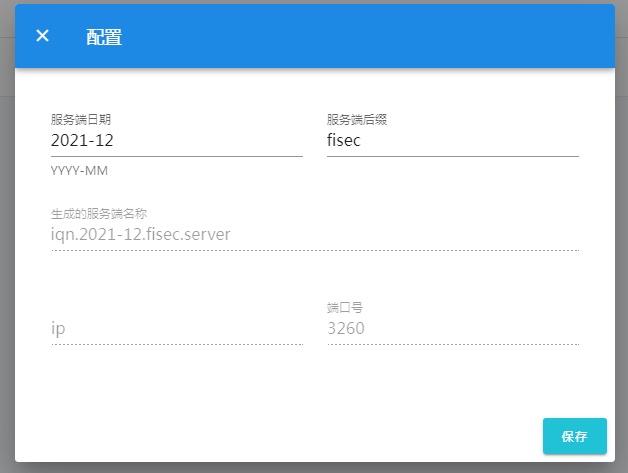


在弹框中按需填写组ID、用户、密码、重复密码（需自行记忆），后续对等用户信息可以不填写。点击【保存】。配置完成后显示如下：

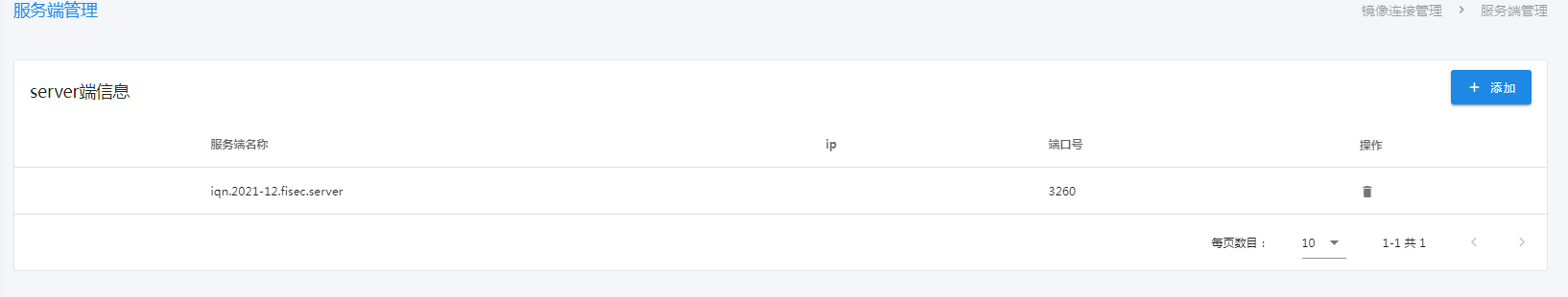


* + 1. 服务端管理

配置完CHAP认证管理后进入服务端管理模块，点击右上角【添加】

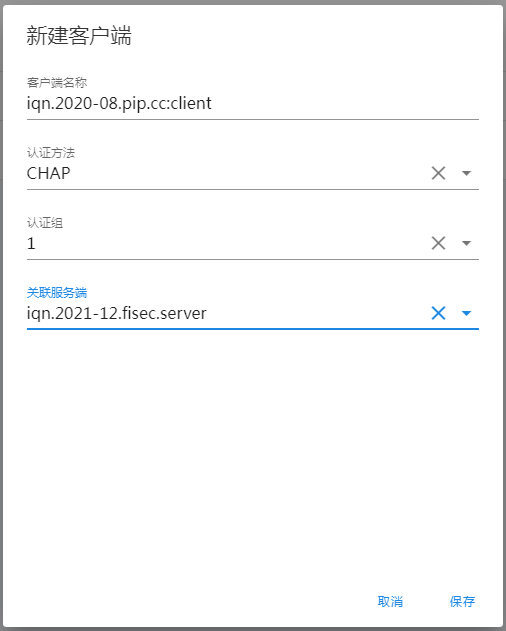


按需选择服务端日期，填写服务端后缀，其余不用填写，点击【保存】。配置完成后显示如下：



* + 1. 客户端管理

配置完服务端管理后进入客户端管理模块，点击右上角【新建客户端】

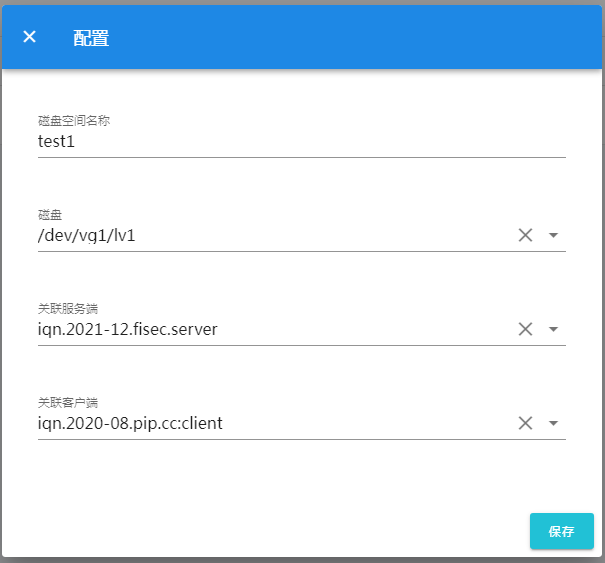


客户端名称有格式要求，建议填写iqn.2020-08.pip.cc:client，或在此格式基础上进行改动，认证方法选择“CHAP”，认证组选择在CHAP认证管理模块添加的组ID，关联服务端选择在服务端管理模块中添加的服务端名称。点击【保存】，配置完成后显示如下：



* + 1. 逻辑单元管理

配置完客户端管理后，进入逻辑单元管理模块，点击右上角【添加】

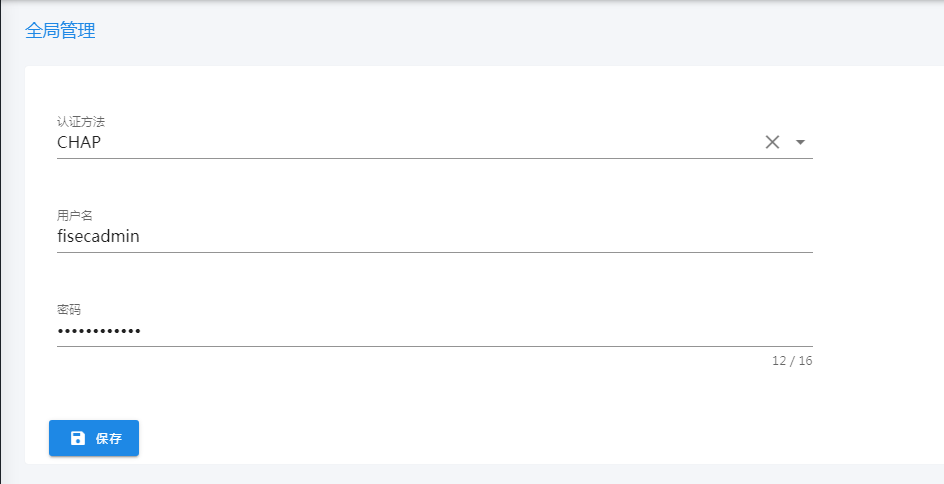


按需填写磁盘空间名称，选择磁盘，即逻辑卷管理模块中新建的逻辑卷磁盘，选择关联服务端即服务端管理模块中新建的服务端，选择关联客户端即客户端模块中新建的客户端，点击【保存】，配置完成后显示如下：



* + 1. 全局管理

配置完逻辑单元管理后进入全局管理模块



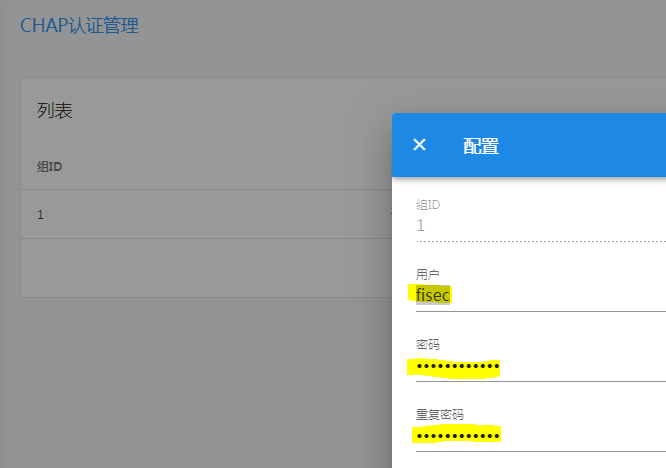
认证方法选择“CHAP”，用户名和密码按需填写（需自行记忆），点击【保存】。

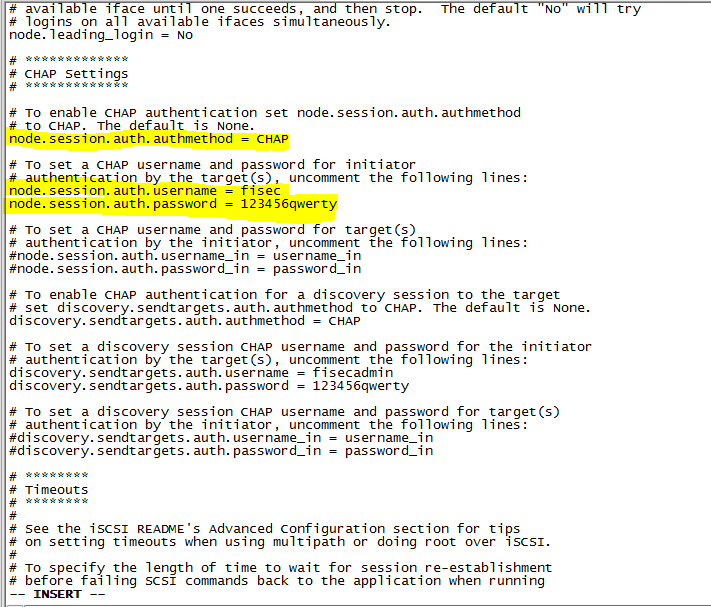
* + 1. 业务系统配置说明

（1）在客户端修改配置文件/etc/iscsi/iscsid.conf开启并配置CHAP

需要配置单向普通session认证，discover认证。

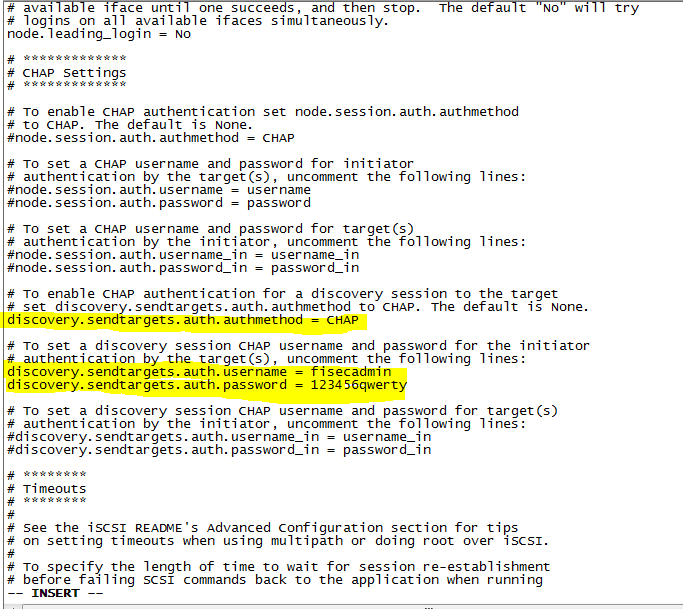
将下方部分解除注释（去掉#）并将CHAP认证管理中添加的组用户密码信息填写到此处





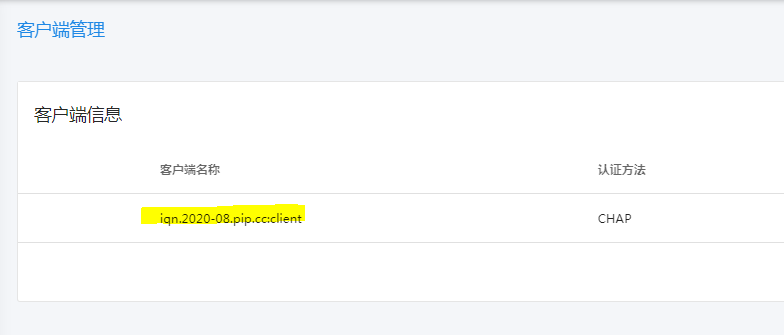
继续将下方标注处解除注释（去掉#）并将全局管理处所配置的用户名和密码填写到下方：

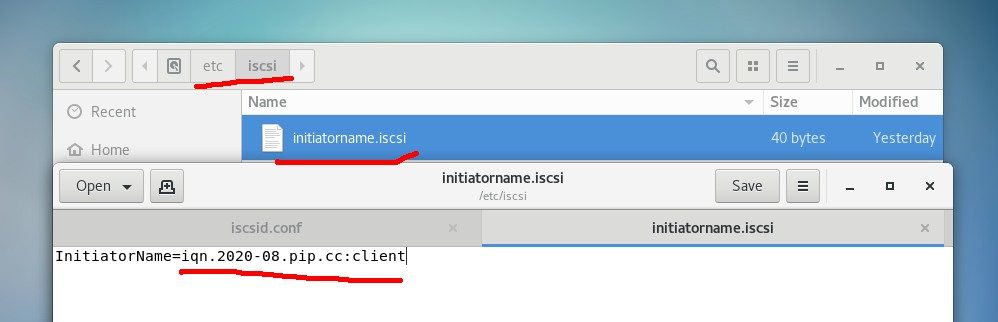




保存并退出。

（2）按实际情况修改客户端文件/etc/iscsi/initiatorname.iscsi，将客户端名称填写到文件中。





（3）重启iscsi服务

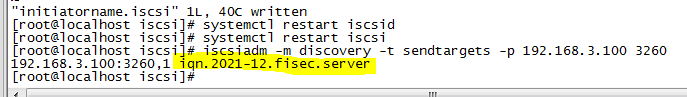
systemctl restart iscsid

systemctl restart iscsi

（4）查看目标存储（这里需要已知目标存储的IP及端口信息）

iscsiadm -m discovery -t sendtargets -p 192.168.3.100 3260

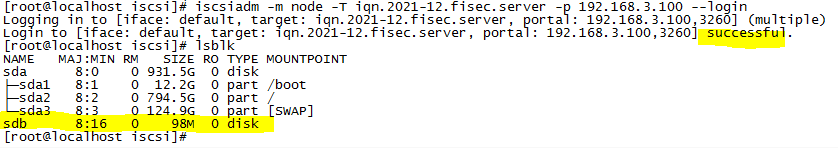
可以看到在服务端管理处添加的服务：



（5）登录（这里需要已知目标存储的服务名称及IP）

iscsiadm -m node -T iqn.2021-12.fisec.server -p 192.168.3.100 --login

当提示successful并且通过lsblk命令可以看到磁盘设备多了一个，说明连接共享磁盘成功。



（6）将密文卷挂载到业务系统中

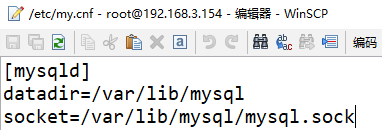
先进行分区fdisk /dev/sdb

mkfs.ext4 /dev/sdb

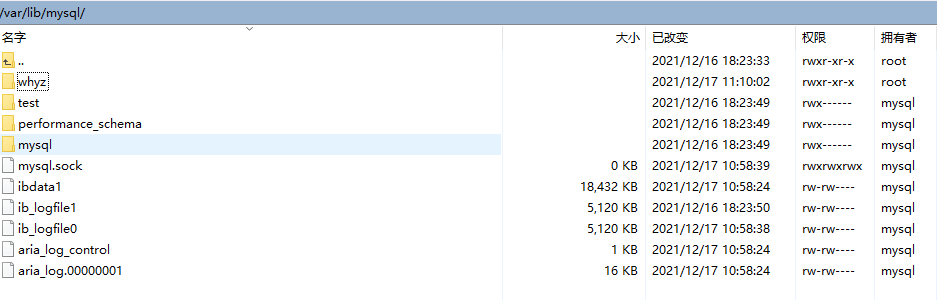
mount /dev/sdb /mnt/data

* + 1. 数据库迁移（以mysql (mariadb)为例）

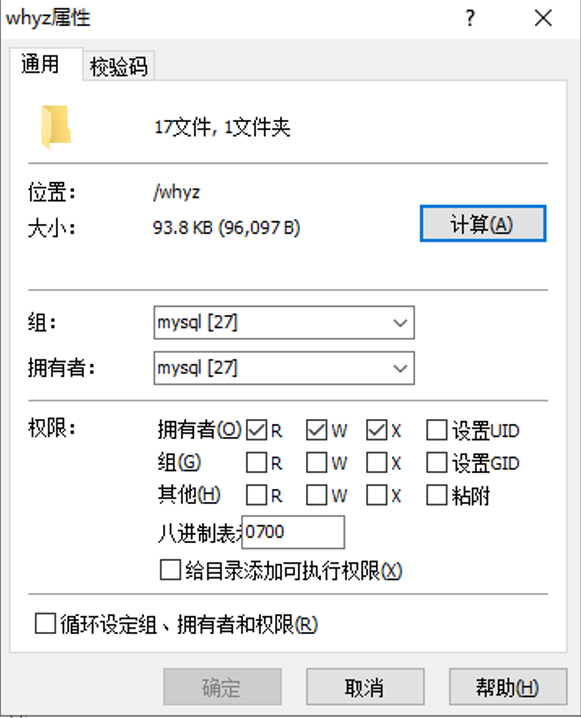
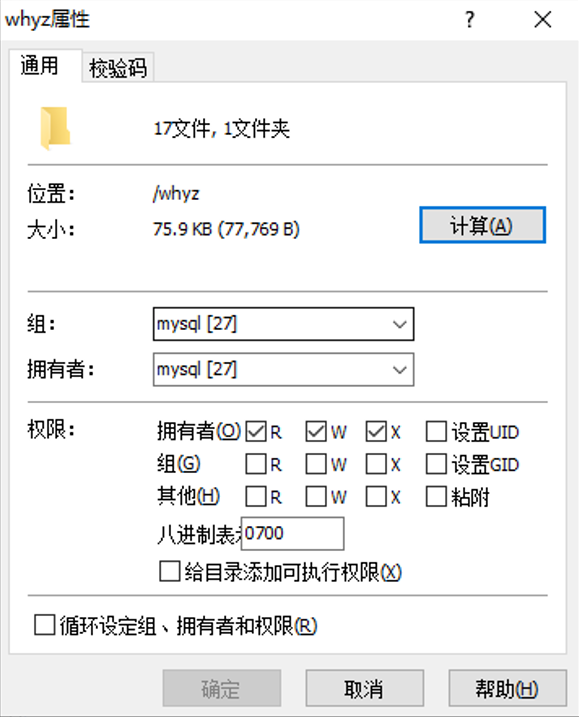
1. 关闭数据库systemctl stop mariadb。查看/etc/my.cnf文件，查看数据库的安装路径。



1. 进入路径，找到需要迁移的表空间，以whyz表空间为例，将此文件夹移动到其他文件夹中，一般为共享磁盘挂载的文件夹，例：迁移到/whyzdir文件夹下 ,同时需要修改文件权限，chmod 777 –R /whyzdir
2. 给复制到新文件夹的库MySQL权限 chown -R mysql /whyzir/whyz



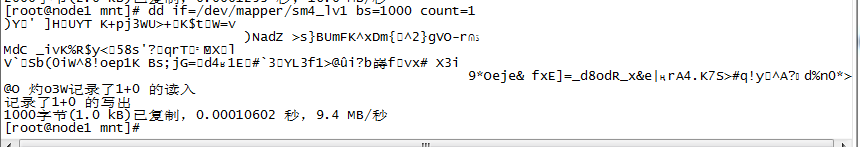
1. 在原目录中，创建软连接指向新目录。例： ln –s /whyzdir/whyz /var/lib/mysql/whyz，重启数据库，systemctl restart mariadb
2. 验证数据库是否迁移成功。备份几个表的数据，可以使用navicate工具。查看whyz文件夹大小，删除几个表的数据库，再次查看文件夹大小，如果文件夹大小改变，则证明迁移成功。

* 1. 验证方式

数据库内容无变化

从服务端可以查看到密文

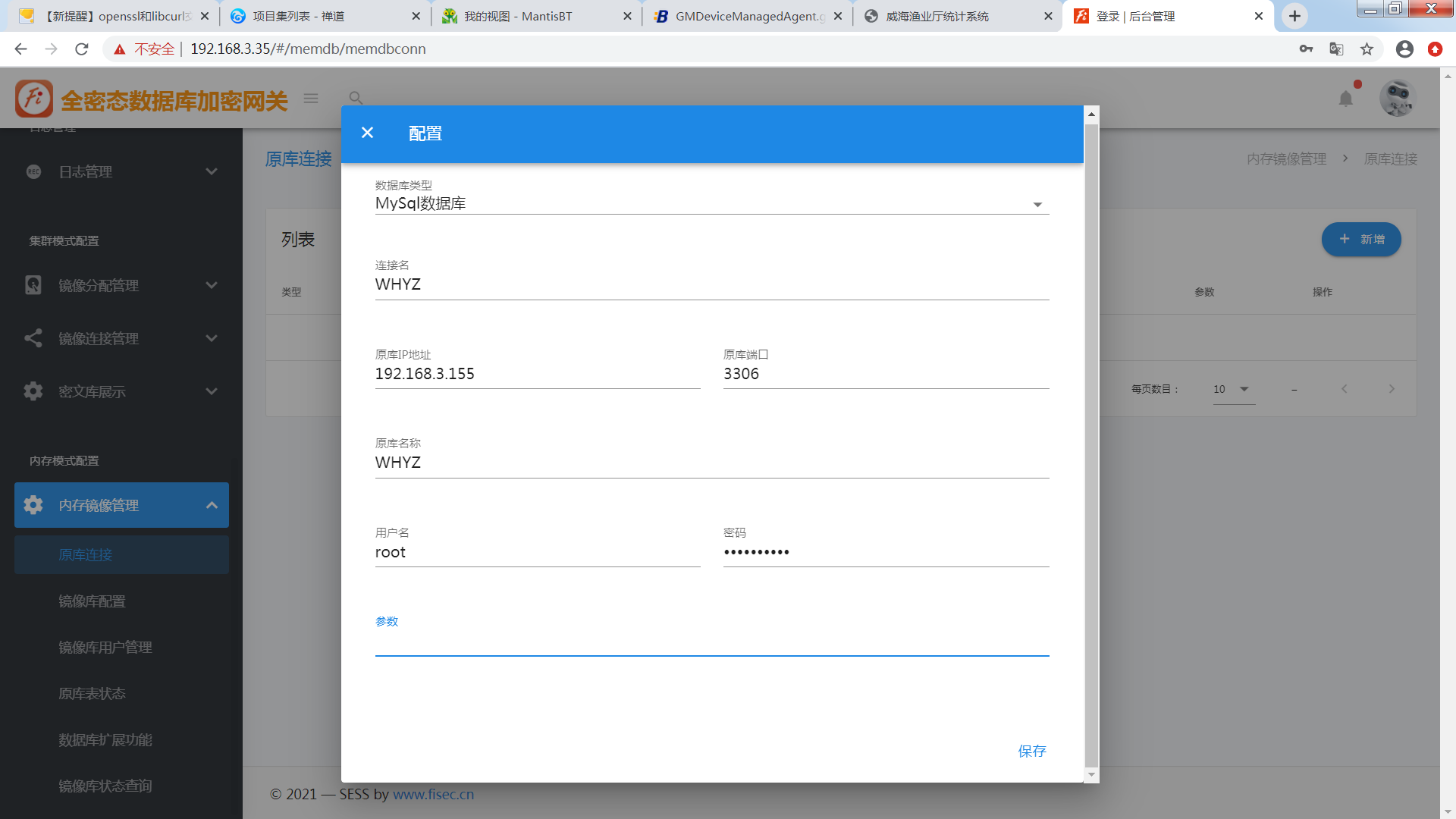


应用数据正常

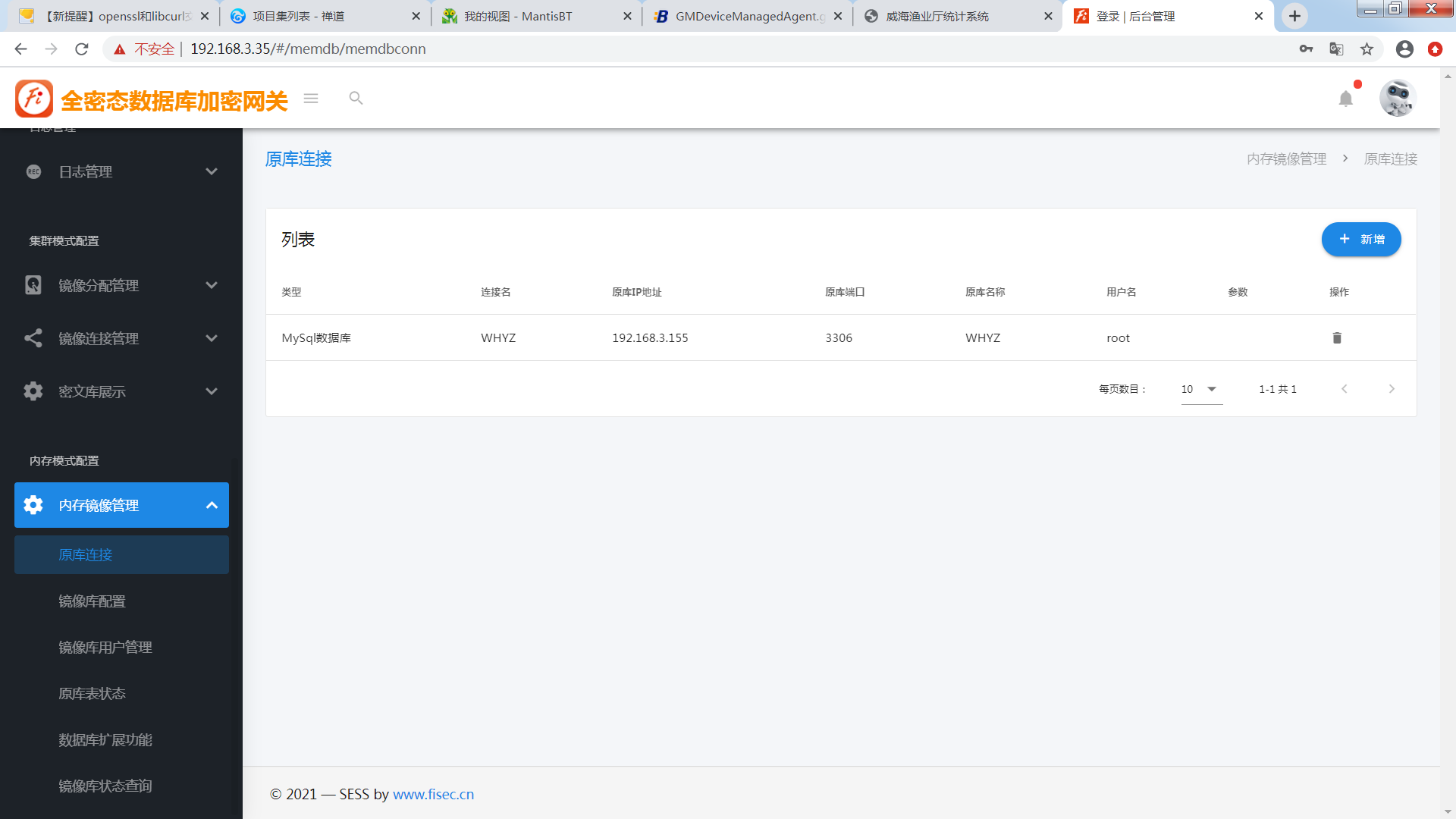


1. 内存镜像模式方案
   1. 配置数据库加密步骤
      1. 创建数据库连接

点击“内存镜像管理”-“原库连接”-“新增”，添加演示业务数据库的连接信息。

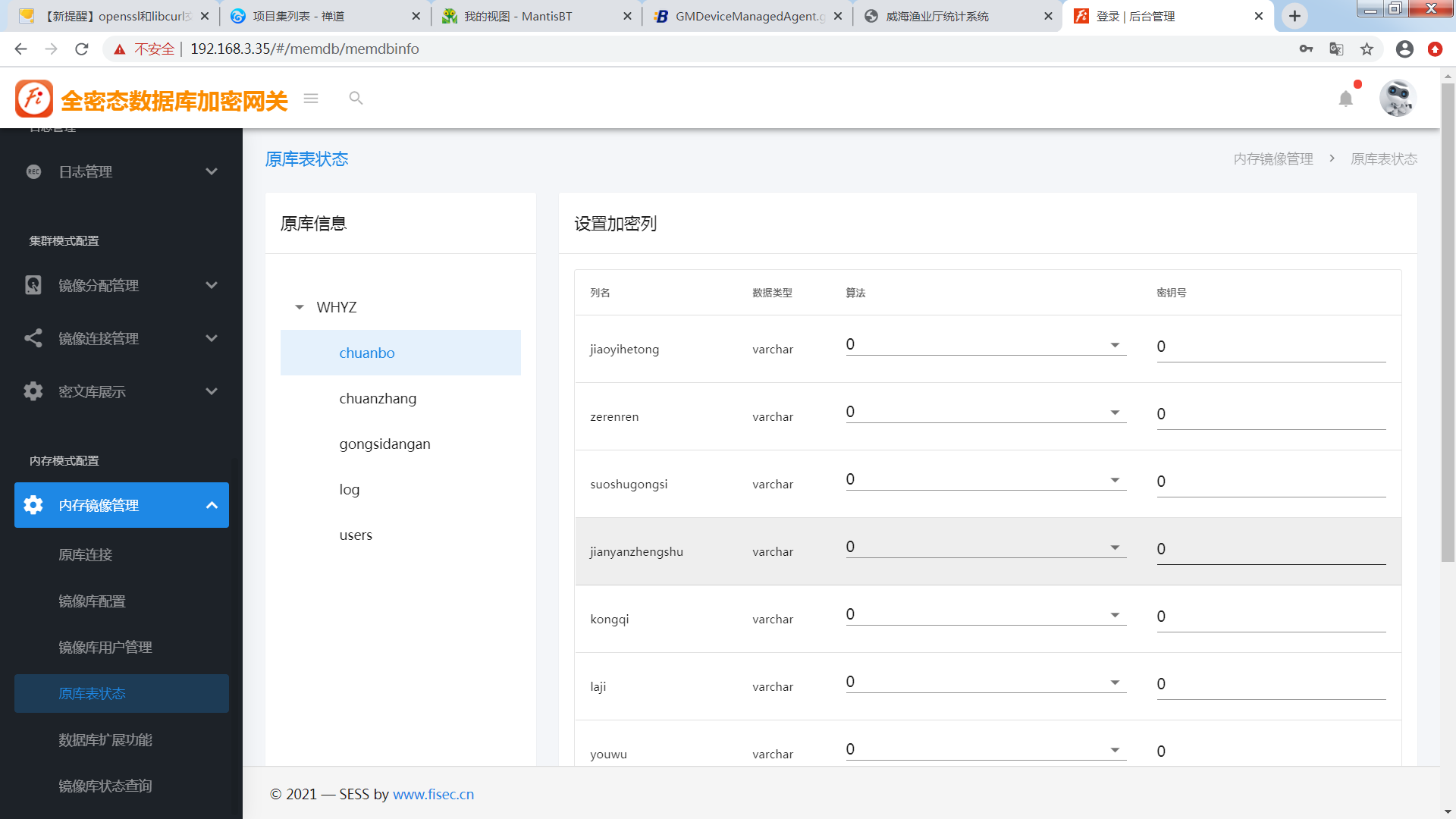


添加数据库成功后，列表中会出现对应条目。



* + 1. 配置加密列

点击“内存镜像管理”-“原库表状态”，展开“WHYZ”数据库，选择“chuanbo”表，选择“duwei”字段，加密算法配置为8（SM4加密）， 密钥号选择1，点击“保存”。



* + 1. 重新加载服务

重启全密态数据库加密网关的内存镜像模块，加载数据

cd /mnt/apache-tomcat-8.5.57/bin/

./shutdown.sh

./startup.sh

* + 1. 修改业务系统数据库配置信息

原配置信息(/mnt/etc/config.properties)

driver=com.mysql.jdbc.Driver

url=jdbc:mysql://127.0.0.1:3306/WHYZ

user=root

pass=12345678

par=allowMultiQueries=true&useSSL=false&zeroDateTimeBehavior=round&characterEncoding=UTF-8

修改为

driver= com.fisec.jdbc.Driver

url=jdbc:mysql://192.168.3.35:9092/WHYZ

user=root

pass=12345678

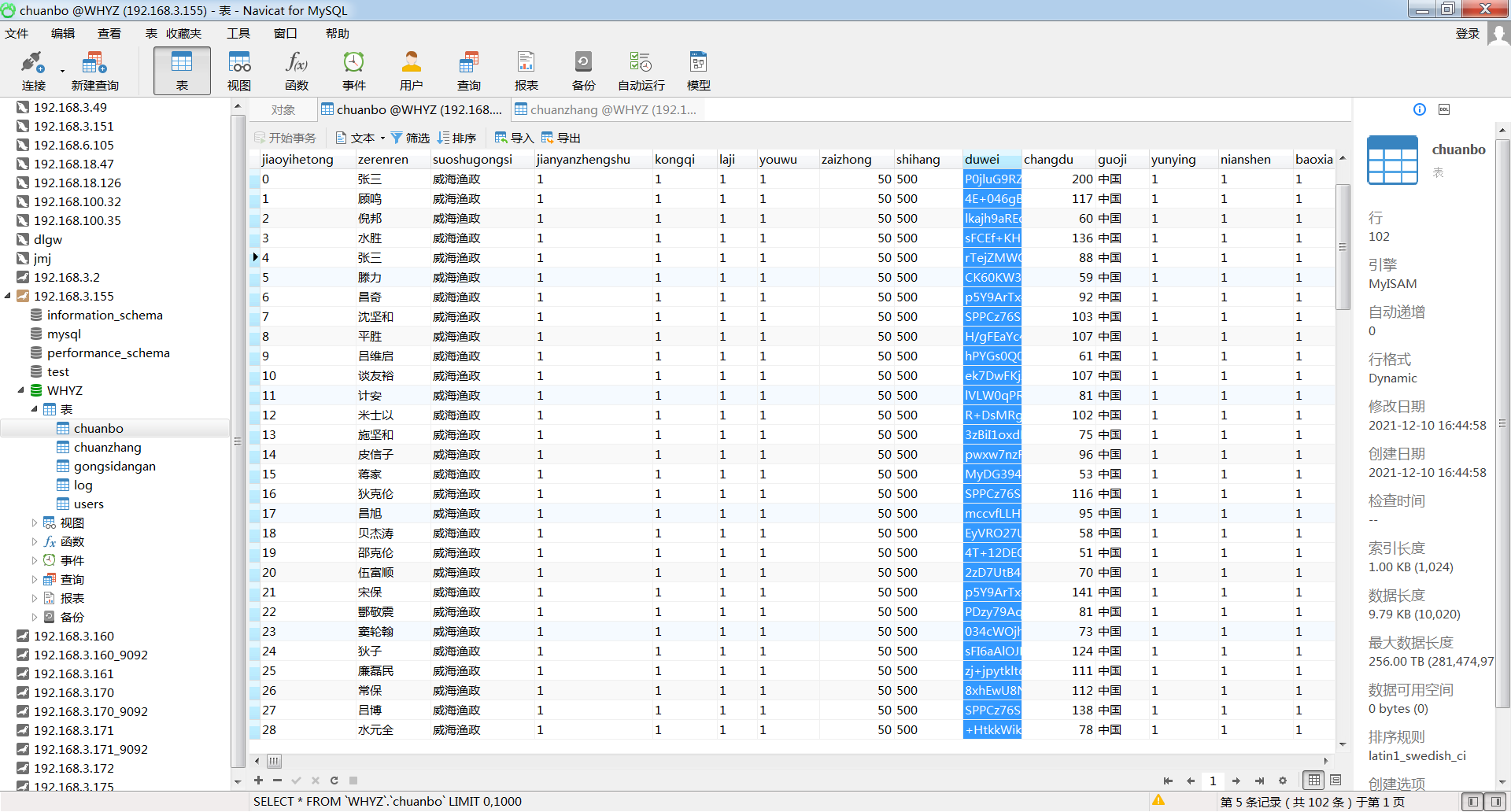
par=allowMultiQueries=true&useSSL=false&zeroDateTimeBehavior=round&characterEncoding=UTF-8

将网关的jdbc包fisec-jdbc-1.1.0.jar放出业务系统中

修改数据库连接信息将数据库driver改为com.mysql.jdbc.Driver，将url改为网关的IP和端口，类型默认为mysql，端口默认为9092，将用户名密码改为网关镜像库的用户名密码，默认为root/12345678

* 1. 验证方式

数据库数据内存发生变化，对应字段为密文



重新启动业务服务，查看业务信息，正常。

