



赛磐石数权保护系统

用户操作手册

V1.0.4

北京成众志科技有限公司

2020年12月

目 录

第一章 前言.....	1
第二章 许可证管理功能介绍.....	2
2.1. 系统管理员 system.....	3
2.1.1. 许可证管理登录.....	3
2.1.2. 许可证申请.....	4
2.1.3. 许可证详情查看.....	5
第三章 数权保护系统主控台.....	6
3.1. 系统安全员 security.....	6
3.1.1. 主控台登录.....	6
3.1.2. 数权保护系统状态监测.....	8
3.1.3. 数权保护系统数据存储空间状态监测.....	9
3.1.4. 数权保护系统日志告警监测.....	10
3.1.5. 许可证状态检测.....	10
3.1.6. 更多.....	11
3.1.6.1. 数权配置.....	11
3.1.6.2. 安全资源.....	13
3.1.6.3. 数权堡垒管理.....	14
3.1.6.4. 密码修改.....	15
3.1.6.5. 修改主控人信息.....	15
3.1.6.6. 关于.....	16



第四章 块空间挂载配置.....	17
4.1. windows 系统挂载块空间.....	17
4.1.1. 资源查找.....	17
4.1.2. 本地挂载块存储.....	18
4.1.3. 格式化分区与挂载.....	19
4.2. Linux 系统挂载块空间.....	21
4.2.1. 资源配置.....	21
4.2.2. 查找目标存储.....	22
4.2.3. 将目标存储提供的资源挂载到本地.....	22
4.2.4. 查看已挂载的磁盘.....	23
4.2.5. 分区.....	24
4.2.6. 格式化.....	24
4.2.7. Mount 挂载.....	25

第一章 前言

赛磐石数权保护系统主要用于保护用户的数据控制权，隐私权和数据产权，为用户提供数据分级分类安全管控、数据确权和数据安全责任管理三大技术抓手。数权保护系统基于量子安全技术，实现数权保护。系统具备“信息隐藏不可见、数据上锁用不了”两大数据安全黑科技。即数据在存储设施上可控、可管、可存但不可见，在网络设施上可传不可见、在计算设施上可用不可见；时间超限用不了、地点超限用不了、设备不符用不了、人员不符用不了、权责缺失用不了、方式不对用不了。

赛磐石数权保护系统能够保护云租户的数据实际控制权，为云租户的安全责任人提供了直接管控云端数据的技术保障；防范了来自于单位内部关键岗位人员、接触内部敏感信息和存储设备的第三方人员（如软件研发人员、系统运维人员、数据服务人员、基础设施提供商及其工作人员等等），窃取、泄漏、扩散存储数据的安全风险；有效破解了 IT 服务外包方更换时被外包方用数据“卡脖子”的难题。

赛磐石数权保护系统为建立数据安全责任机制提供了技术抓手，确保了数据安全责任人员对数据的实际控制权，将安全责任风险点集中到安全责任人员，便于安全责任管控和追溯，有效破解了信息安全主管领导缺乏直接管控数据的技术手段而导致数据失控的技术难题。

第二章 许可证管理功能介绍

主要功能是许可证申请和许可证详情查看。许可证管理的使用者是系统管理员（system）。

在浏览器输入登陆访问地址（地址：<https://IP:30033> 其中 IP 为申请的华为云服务器的公网 IP）后，如果出现下图错误，点击高级、继续前往即可。



图 1 系统登录

2.1. 系统管理员 system

2.1.1. 许可证管理登录

- 浏览器登录许可证管理，用户名、密码如下

用户名：system 密码：123456

- 首次登陆进入系统后，会提示修改登陆密码

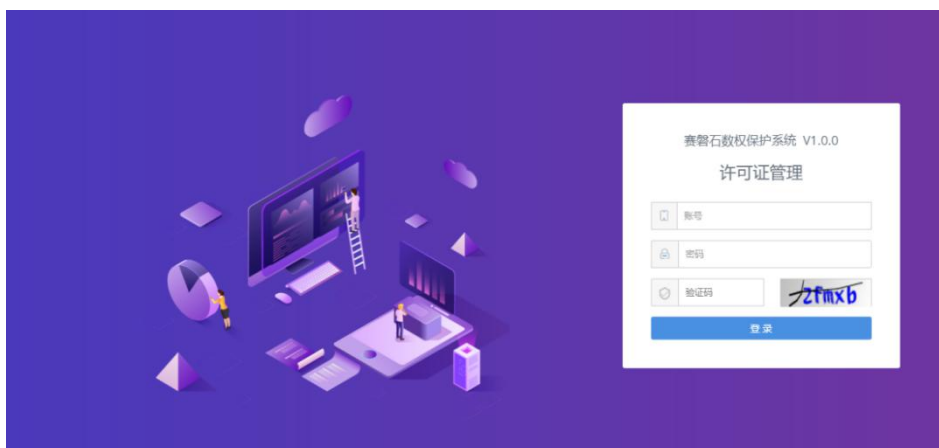


图 2 许可证管理登录页面

首次登录，请修改密码后操作

新密码：

确认密码：

保存修改


图 3 修改密码页面

2.1.2. 许可证申请

管理员可以通过申请许可证模块申请许可证，申请许可证时需填写用户名、联系电话、订单号、华为云主机公网 IP、收货人、收货人电话和收货地址。

图 4 申请许可证功能页面

具体功能操作如下：

序号	功能名称	功能图示	操作方式	功能描述
1	申请		鼠标左键点击	通过点击此按钮可进行证书申请。

2.1.3. 许可证详情查看

在我司激活许可证之后，用户可以查看许可证详情。

基本信息:	
许可证ID:	CZZ100202011300001A_0001Z
许可证版本号:	1.0.0
许可证类别:	内部测试
许可证类型:	节点锁定许可证
许可证分配类型:	单独许可证
许可证有效起始日期:	2020-11-30
许可证有效截止日期:	2021-11-30
授权产品指纹:	
CPU ID:	54 06 00 00 FF FB AB 0F
MAC地址:	00:0c:29:f2:f4:62
主板ID:	VMware-56 4d 3d b1 70 d9 ca 61-66 6f 5b ac 55 f2 f4 62
磁盘ID:	b97aed65-f9f3-4759-83f7-f0c11d024b4b
授权功能:	
支持最大用户数:	100
支持最大磁盘数:	5
支持最大磁盘容量:	20T
数权重启是否重激活:	是

图 5 许可证详情查看页面

第三章 数权保护系统主控台

数权保护系统主控台可视化的向用户提供数权保护系统整体状态查看，包括数权保护系统状态监测，数据存储空间状态监测，日志告警监测、许可证状态检测等内容。主控台的使用者是系统安全员，此角色可以分离出主控人，需由数据所有权方安全责任人担任或其书面授权人员担任，管理数据锁及数权识别码。

3.1. 系统安全员 security

3.1.1. 主控台登录

- 浏览器登录主控台，用户名、密码如下
用户名：security 密码：123456
- 首次登陆进入系统后，会提示修改登陆密码



图 6 主控台登录页面

首次登录，请修改密码后操作

新密码：

确认密码：

保存修改

图 7 修改密码页面

特别提醒：安装主控台后，进行首次登录时，需插入数据锁，登录后进行数据初始化，后续非首次登录不需要插数据锁。

登录主控台后，主页可视化页面包括数权保护系统状态监测，数权保护系统数据存储空间监测，数权堡垒日志告警监测以及许可证状态监测。



图 8 主控台首页页面

3.1.2. 数权保护系统状态监测

主控人可以查看数权保护系统累计存取数据，该数据 5 秒更新一次。可视化显示数权堡垒总数量，数权堡垒状态正常数量，数权堡垒状态异常数量以及待处置事件统计。列表展示所有数权堡垒信息，数权堡垒名称，激活日期，当前状态，逻辑磁盘数。



图 9 数权保护系统状态监测



图 10 数权保护系统状态监测-数权堡垒详情列表

具体功能操作如下：

序号	功能名称	功能图示	操作方式	功能描述
1	待处理事件		鼠标左键点击	通过点击此按钮可进行待处理事件查看，列表展示
2	数权堡垒数量		鼠标左键点击	通过点击此按钮可进行所有的数权堡垒数量列表的展示
3	数权堡垒正常状态数量		鼠标左键点击	通过点击此按钮可进行正常状态的数权堡垒数量列表的展示
4	数权堡垒异常状态数量		鼠标左键点击	通过点击此按钮可进行异常状态的数权堡垒数量列表的展示

3.1.3. 数权保护系统数据存储空间状态监测

主控人可以查看数权堡垒总存储空间，已用空间，日均空间，近一个月的吞吐量，今日吞吐量，日均吞吐量。折线图可视化显示数据流量日使用量，数据流量日均吞吐量显示。



图 11 数权保护系统数据存储空间状态监测

3.1.4. 数权保护系统日志告警监测

主控人可以查看数权保护系统的状态包括 NAS 空间分片丢失告警，NAS 空间数据无写入告警，数权保护系统连接异常告警，以及数权堡垒通告信息。



图 12 数权保护系统日志告警监测

3.1.5. 许可证状态检测

此模块可视化的为主控人显示许可证总数量，已使用数量，未使用数量，许可证过期数量。

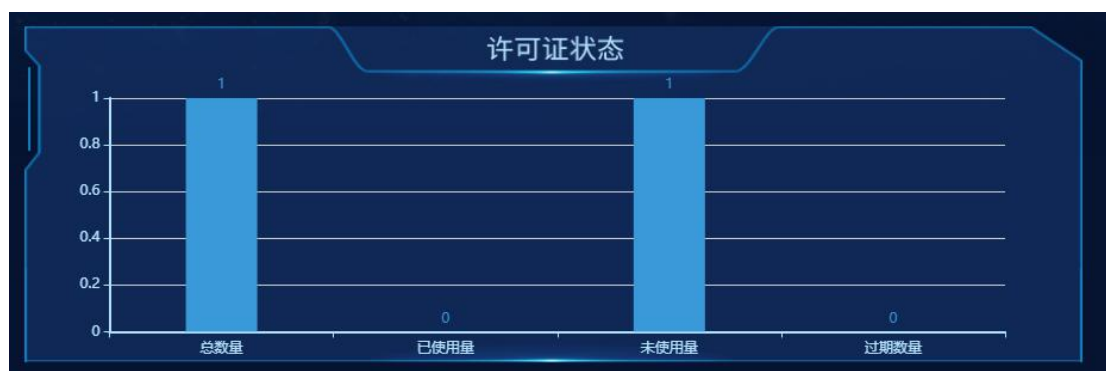


图 13 数权保护系统许可证状态监测

点击柱状图可看许可合格的具体信息，包括许可证 ID，许可证类型，许可证授权到期日，重激活时间，使用状态，是否过期，最大用户数，最大磁盘数，最大磁盘容量等参数，如下图。

序号	许可证ID	许可证类型	授权到期日	重激活时间	使用状态	是否过期	最大用户数	最大磁盘数	最大磁盘容量
1	CZZ100202011300...	内部测试	2021-11-30	2021-11-30	已使用	未过期	100	5	20T

当前显示 1 到 1 条数据, 共 1 条数据

图 14 数权保护系统许可证状详细信息

3.1.6. 更多

更多模块包括安全资源、数权堡垒管理，密码修改，数权配置，关于，退出。

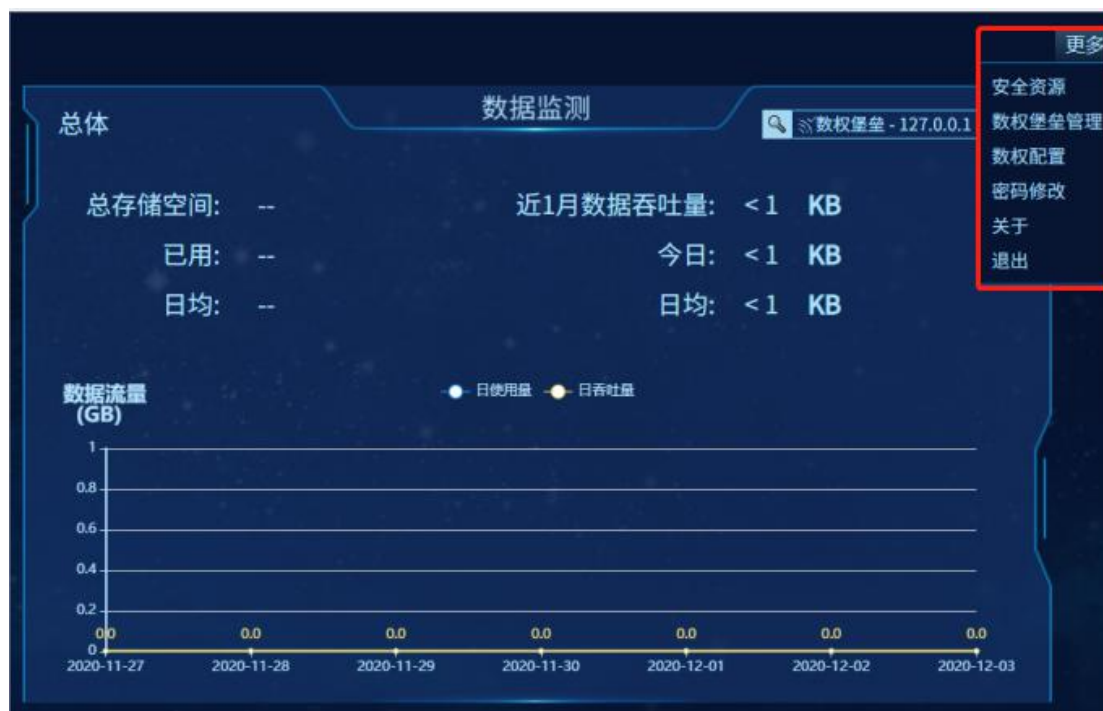


图 15 更多

3.1.6.1. 数权配置

主控人第一次安装初始化主控台时，主控人需配置数权证书，首先插入数据锁，输入数权证书因子，具体功能输入参数项包括数权识

别码，确认数权识别码，数权人单位名称，数权人姓名，具体功能页如下：

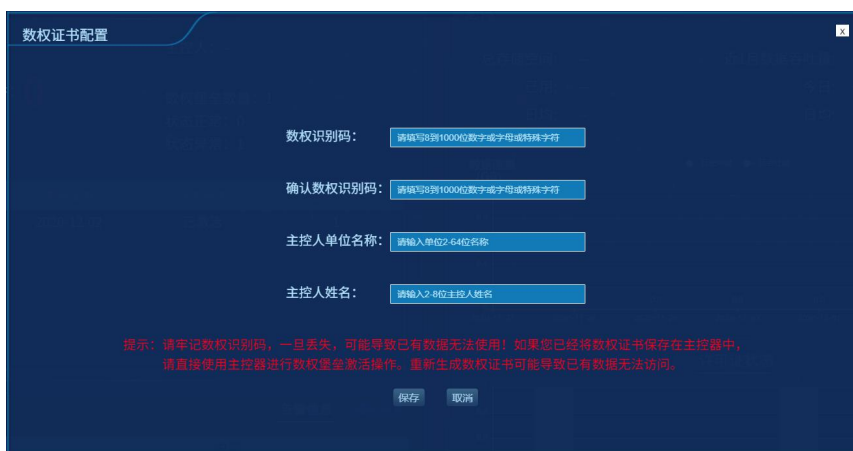




图 16 更多-数权配置

特别提示：请牢记数权识别码，一旦丢失，可能导致已有数据无法使用！如果您已经将数权证书保存在数据锁中，请直接使用数据锁进行数权堡垒激活操作。重新生成数权证书可能导致已有数据无法访问。

具体功能操作如下：

序号	功能名称	功能图示	操作方式	功能描述
1	确定		鼠标左键点击	点击此按钮前插入数据锁，生成数权证书存储于数据锁
2	取消		鼠标左键点击	点击此按钮可取消数权证书的配置

数权配置成功后，更多模块显示中的数权配置变成了修改主控信息，如下图：



图 17 更多

特别说明：在主控台已配置数权证书的前提下，主控台系统进行了重装初始化，再激活数权堡垒、启用数据锁时，不需要再次配置生成数权证书，直接启用数据锁激活数权堡垒。

3.1.6.2. 安全资源

主控人通过点击更多，点击安全资源，显示块存储空间名称、Initiator name 和块存储空间大小。



图 18 更多-安全资源

3.1.6.3. 数权堡垒管理

主控人通过点击更多，点击数权堡垒管理进入数权堡垒信息列表页面，可查看数权堡垒的具体信息，主控人可通过插入数据锁对数权堡垒进行启用数据锁。主控人对数权堡垒可关机，重启操作。



图 19 更多-数权堡垒管理（启用数据锁）



图 20 更多-数权堡垒管理（已启用数据锁）

具体功能操作如下：

序号	功能名称	功能图示	操作方式	功能描述
1	详情		鼠标左键点击	通过点击此按钮可查看数权堡垒详情
2	启用数据锁		鼠标左键点击	先插入数据锁，通过点击此按钮可启用数权数据锁
3	关机		鼠标左键点击	通过点击此按钮可关闭数权堡垒
4	重启		鼠标左键点击	通过点击此按钮可重启数权堡垒

3.1.6.4. 密码修改

支持数权保护密码修改和登录密码修改，输入正确的原密码，输入新密码。



图 21 更多-密码修改

3.1.6.5. 修改主控人信息

支持修改主控人信息，包括主控人姓名和主控人单位名称。

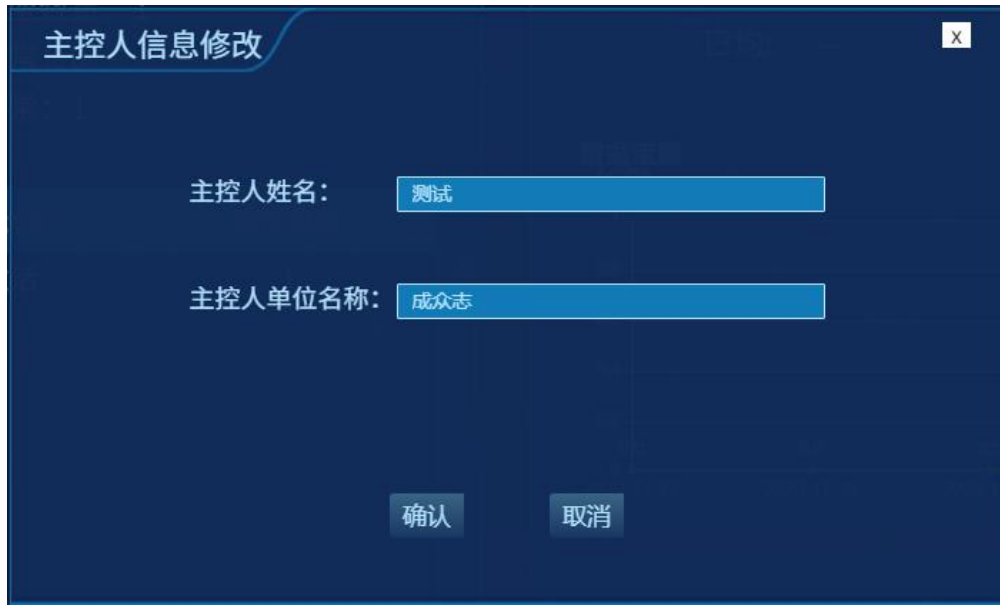


图 22 更多-修改主控人信息

3.1.6.6. 关于

主控人通过关于页面可以查看主控台版本，许可证重激活日期，主控人和主控人单位信息。

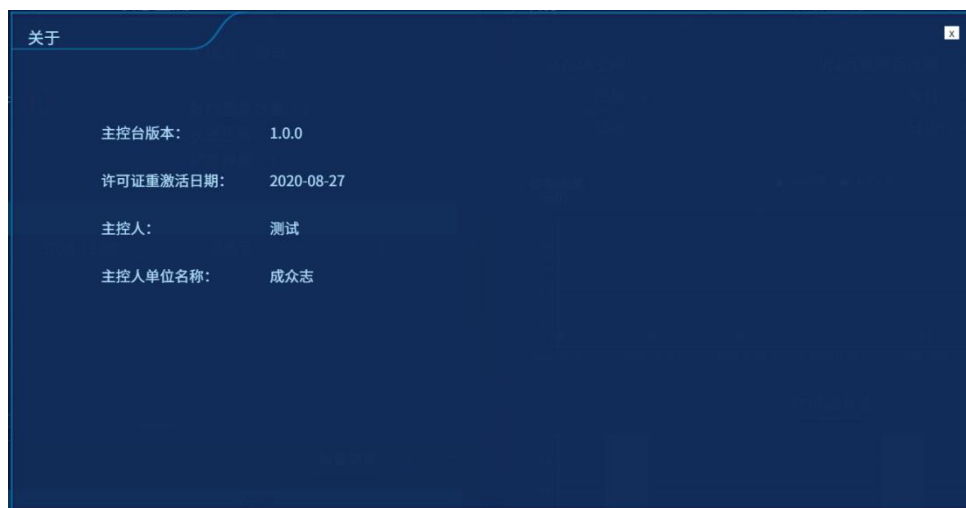


图 23 更多-关于

第四章 块空间挂载配置

【风险提示】：

以下操作需要专业运维管理人员进行操作，如操作不当，可能会导致空间挂载失败或导致将要挂载空间的系统数据丢失和系统崩溃。

4.1. windows 系统挂载块空间

4.1.1. 资源查找

运维人员登录主控台，通过点击更多-->安全资源，并复制 Initiator name。



图 24 安全资源

运维人员查看应用服务器（windows 系统）的 initiatorname，打开本机的 iSCSI 发起程序属性，查看配置，点击更改，将复制 Initiator name 复制到新发起程序名称下的对话框中，选择确定，如下图：

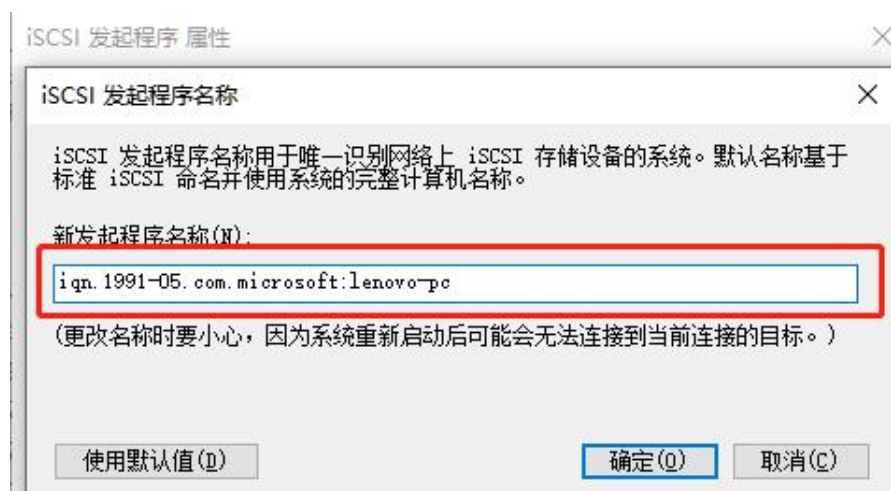


图 25 查看 initiatorname

4.1.2. 本地挂载块存储

主控人打开业务主机，执行本地存储空间挂载步骤如下：

1、左击开始，选择 windows 管理工具，打开 iSCSI 发起程序，点击目标，目标框中输入主机公网 IP （如何查找具体见使用说明书第三章）如：192.168.1.145；



2、点击快速连接，显示已连接，点击完成。

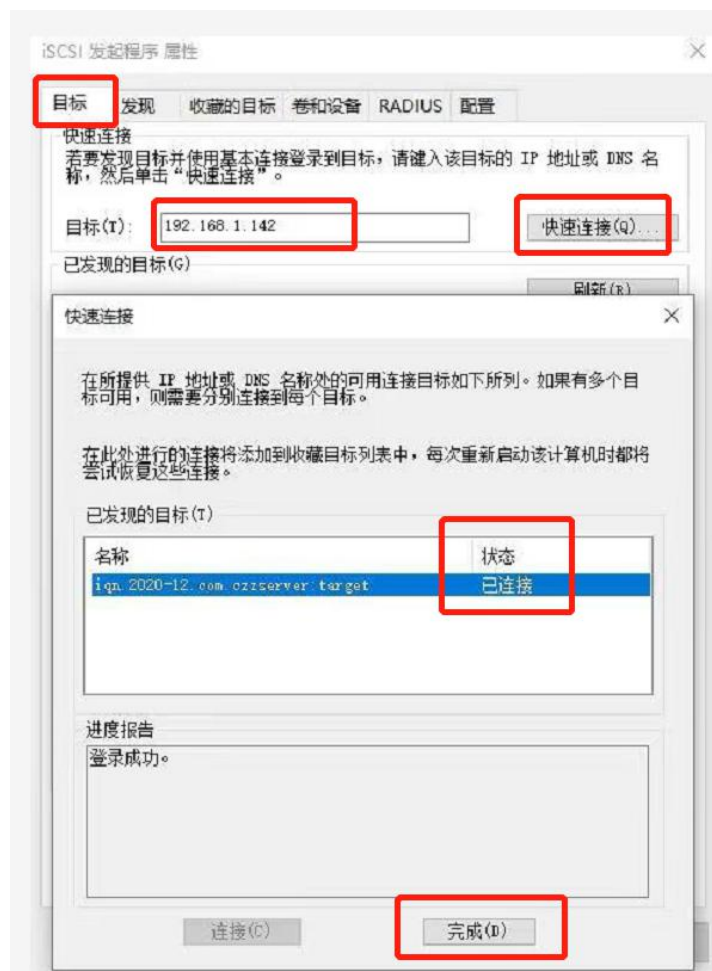


图 26 本地挂载块存储

4.1.3. 格式化分区与挂载

运维人员打开业务主机，执行格式化分区与挂载步骤如下：

- 1、右键点击此电脑，选择管理，打开管理 。 如下页面：

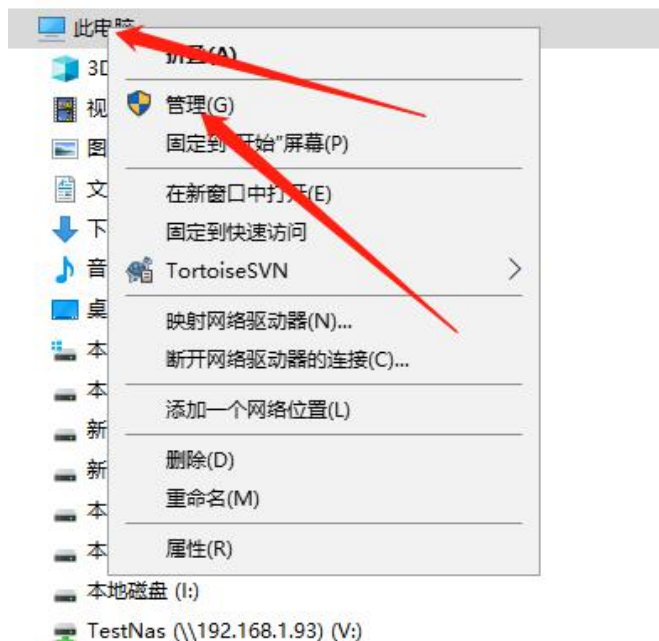


图 27 打开管理

2、格式化分区添加新卷操作，选择存储-->磁盘管理-->选中挂载的磁盘右击-->新建简单卷，点击下一步直至完成。

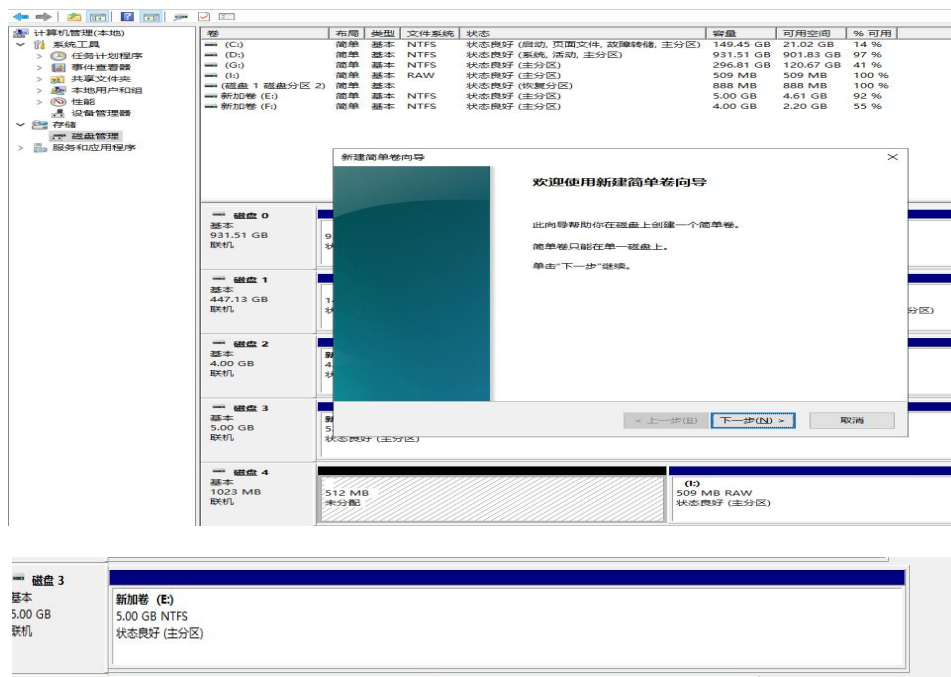


图 28 格式化分区添加新卷

至此块空间逻辑盘挂载完成。

4.2. Linux 系统挂载块空间

4.2.1. 资源配置

运维人员登录主控台，通过点击更多-->安全资源，并复制 Initiator name。



图 29 安全资源

- 1、运维人员登录业务服务主机客户端获取应用服务器的 ininitiatorname。
- 2、首先要在挂载存储空间的主机上执行以下命令 `yum -y install`

iscsi-initiator-utils, 安装 initiatorname 程序。

3、执行命令 `cat /etc/iscsi/initiatorname.iscsi` , 获取 InitiatorName。如下图:

```

/dev/sda1      1038336 132328 906008 13% /boot
tmpfs         204788  0      204788  0% /run/user/0
/dev/sr0      4364400 4364400  0      100% /media/cdrom
binfmt_misc  0        0        0      - /proc/sys/fs/binfmt_misc
//127.0.0.1/Test/ 0        0        0      - /cstorage/share/Test
/dev/sdc      5029504 4750976  0      100% /cstorage/resource/FileDocName
//127.0.0.1/TestNas/ 3029304 4750976  0      100% /cstorage/share/TestNas
[root@localhost ~]# cat /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.1994-05.com.redhat:853486f4ab5f
[root@localhost ~]# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda          8:0    0   20G  0 disk
├─sda1       8:1    0    1G  0 part /boot
├─sda2       8:2    0   19G  0 part
│   └─centos-root 253:0  0   17G  0 lvm  /
│       └─centos-swap 253:1  0    2G  0 lvm  [SWAP]
sdb          8:16   0    1G  0 disk
sdc          8:32   0    5G  0 disk /cstorage/resource/FileDocName
sr0         11:0    1  4.2G  0 rom  /media/cdrom
[root@localhost ~]# fdisk -l

磁盘 /dev/sda: 21.5 GB, 21474836480 字节, 41943040 个扇区
Units = 扇区 of 1 * 512 = 512 bytes
扇区大小(逻辑/物理): 512 字节 / 512 字节
I/O 大小(最小/最佳): 512 字节 / 512 字节
磁盘标签类型: dos
磁盘标识符: 0x0007d466

   设备 Boot      Start         End      Blocks    Id System
/dev/sda1  *           2048        2099199    1048576    83  Linux
/dev/sda2                2099200    41943039    19921920    8e  Linux LVM

磁盘 /dev/mapper/centos-root: 18.2 GB, 18249416704 字节, 35643392 个扇区
Units = 扇区 of 1 * 512 = 512 bytes
扇区大小(逻辑/物理): 512 字节 / 512 字节
I/O 大小(最小/最佳): 512 字节 / 512 字节

```

图 30 执行命令操作显示图

4.2.2. 查找目标存储

运维人员登录业务服务主机客户端，执行命令

`iscsiadm -m discovery -t sendtargets -p 192.168.1.182` (ip 为可挂载存储空间主机的 ip)

查看目标存储，如下图:

```

[root@localhost ~]# iscsiadm -m discovery -t sendtargets -p 192.168.1.147
192.168.1.147:3260,1 iqn.2020-09.com.jdxaserver:iscsiceshi1
192.168.1.147:3260,1 iqn.2020-09.com.jdxaserver:iscsiceshi2
192.168.1.147:3260,1 iqn.2020-09.com.jdxaserver:iscsiceshi3
192.168.1.147:3260,1 iqn.2020-09.com.jdxaserver:iscsiceshi4
192.168.1.147:3260,1 iqn.2020-09.com.jdxaserver:iscsiceshi5
[root@localhost ~]#

```

图 31 查看目标存储操作图

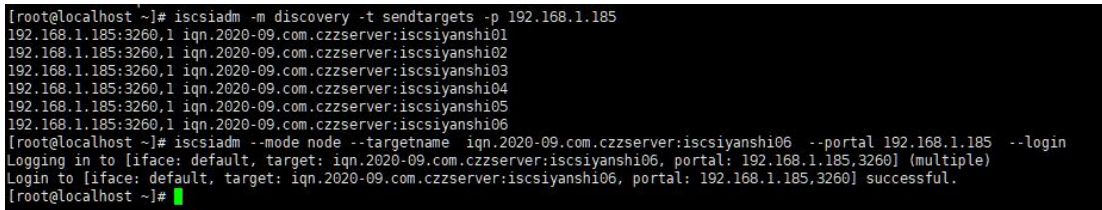
4.2.3. 将目标存储提供的资源挂载到本地

运维人员登录业务服务主机客户端，执行如下命令，可将目标存

储提供的资源挂载到本地。

1) 挂载指定名称的 iscsi 空间:

```
iscsiadm --mode node --targetname
iqn.2020-09.com.jdxaserver:iscsiceshil --portal
192.168.1.182 --login # (ip 为可挂载存储空间主机的 ip)
```



```
[root@localhost ~]# iscsiadm -m discovery -t sendtargets -p 192.168.1.185
192.168.1.185:3260,1 iqn.2020-09.com.czzserver:iscsiyanshi01
192.168.1.185:3260,1 iqn.2020-09.com.czzserver:iscsiyanshi02
192.168.1.185:3260,1 iqn.2020-09.com.czzserver:iscsiyanshi03
192.168.1.185:3260,1 iqn.2020-09.com.czzserver:iscsiyanshi04
192.168.1.185:3260,1 iqn.2020-09.com.czzserver:iscsiyanshi05
192.168.1.185:3260,1 iqn.2020-09.com.czzserver:iscsiyanshi06
[root@localhost ~]# iscsiadm --mode node --targetname iqn.2020-09.com.czzserver:iscsiyanshi06 --portal 192.168.1.185 --login
Logging in to [iface: default, target: iqn.2020-09.com.czzserver:iscsiyanshi06, portal: 192.168.1.185,3260] (multiple)
Login to [iface: default, target: iqn.2020-09.com.czzserver:iscsiyanshi06, portal: 192.168.1.185,3260] successful.
[root@localhost ~]#
```

图 32 挂载 iscsi 空间操作图

2) 检查 initiatorname 是否正确: 业务服务器和存储服务器的 initiatorname 要保持一致

```
cat /etc/iscsi/initiatorname.iscsi
```

如果不一致则需要进行修改, 以及重启服务

```
systemctl restart iscsid
```

```
systemctl restart iscsi
```

4.2.4. 查看已挂载的磁盘

运维人员登录业务服务主机客户端, 执行命令, `fdisk -l` 和 `lsblk` 和 `df -h`, 查看已挂载的磁盘, 操作如下图示:



```
[root@localhost ~]# fdisk -l

磁盘 /dev/sda: 21.5 GB, 21474836480 字节, 41943040 个扇区
Units = 扇区 of 1 * 512 = 512 bytes
扇区大小(逻辑/物理): 512 字节 / 512 字节
I/O 大小(最小/最佳): 512 字节 / 512 字节
磁盘标签类型: dos
磁盘标识符: 0x0007d466

   设备  Boot      Start         End      Blocks   Id  System
/dev/sda1  *          2048       2099199       1048576   83  Linux
/dev/sda2          2099200     41943039       19921920   8e  Linux LVM

磁盘 /dev/mapper/centos-root: 18.2 GB, 18249416704 字节, 35643392 个扇区
Units = 扇区 of 1 * 512 = 512 bytes
扇区大小(逻辑/物理): 512 字节 / 512 字节
I/O 大小(最小/最佳): 512 字节 / 512 字节

磁盘 /dev/mapper/centos-swap: 2147 MB, 2147483648 字节, 4194304 个扇区
Units = 扇区 of 1 * 512 = 512 bytes
扇区大小(逻辑/物理): 512 字节 / 512 字节
I/O 大小(最小/最佳): 512 字节 / 512 字节

WARNING: fdisk GPT support is currently new, and therefore in an experimental phase. Use at your own discretion.

磁盘 /dev/sdb: 1073 MB, 1073741824 字节, 2097152 个扇区
Units = 扇区 of 1 * 512 = 512 bytes
```

图 33 查看挂载磁盘操作图

4.2.5. 分区

运维人员登录业务服务主机客户端，执行命令 `fdisk /dev/sdb1`，进行分区。

```
g---n---回车---回车---w
```

如不需要可不分区直接格式化

```
[root@localhost ~]# fdisk /dev/sdb1
欢迎使用 fdisk (util-linux 2.23.2)。

更改将停留在内存中，直到您决定将更改写入磁盘。
使用写入命令前请三思。

Device does not contain a recognized partition table
使用磁盘标识符 0x7a9dcd89 创建新的 DOS 磁盘标签。

命令(输入 m 获取帮助): █
```

图 34 分区操作图

4.2.6. 格式化

运维人员登录业务服务主机客户端，执行命令：以下有两种格式
可选，一般选第一种

`mkfs.ext4 -T largefile /dev/sdb1` (`df -h` 可查看要格式化的
分区是哪一个)

```
mkfs.xfs -T largefile /dev/sdb1
```



```
[root@localhost ~]# mkfs.xfs /dev/sdb1
meta-data=/dev/sdb1          isize=512    agcount=4, agsize=6400 blks
       =                   sectsz=512    attr=2, projid32bit=1
       =                   crc=1          finobt=0, sparse=0
data     =                   bsize=4096   blocks=25600, imaxpct=25
       =                   sunit=0       swidth=0 blks
naming   =version 2         bsize=4096   ascii-ci=0 ftype=1
log      =internal log     bsize=4096   blocks=855, version=2
       =                   sectsz=512   sunit=0 blks, lazy-count=1
realtime =none             extsz=4096   blocks=0, rtextents=0
[root@localhost ~]# partprobe
```

图 35 格式化操作图

4.2.7. Mount 挂载

1、查看要挂载的资源名称

```
ll /dev/disk/by-path
```

```
[root@localhost ~]# ll /dev/disk/by-path
总用量 0
lrwxrwxrwx. 1 root root 9 10月 16 17:47 ip-192.168.1.182:3260-iscsi-iqn.1991-05.com.targetservice-input-lun-0 -> ../../sdb
lrwxrwxrwx. 1 root root 9 10月 29 16:08 ip-192.168.1.182:3260-iscsi-iqn.2020-09.com.czzserver:iscsiyanshi06-lun-0 -> ../../sdc
lrwxrwxrwx. 1 root root 9 10月 16 17:10 pci-0000:02:03.0-ata-1.0 -> ../../sr0
lrwxrwxrwx. 1 root root 9 10月 16 17:10 pci-0000:03:00.0-scsi-0:0:0:0 -> ../../sda
lrwxrwxrwx. 1 root root 10 10月 16 17:10 pci-0000:03:00.0-scsi-0:0:0:0-part1 -> ../../sda1
lrwxrwxrwx. 1 root root 10 10月 16 17:10 pci-0000:03:00.0-scsi-0:0:0:0-part2 -> ../../sda2
[root@localhost ~]#
```

图 36 查看挂在资源操作图

2、执行挂载

```
cd /dev/disk/by-path
```

```
mount
```

```
ip-192.168.1.182:3260-iscsi-iqn.2018-08.com.czzserver:target1-lun-0-part1 /cstorage/ceshi/
```

【说明】

ip-192.168.1.182:3260-iscsi-iqn.2018-08.com.czzserver:target1-lun-0-part1 为 ll /dev/disk/by-path 查看到的要挂载的资源名称/cstorage/ceshi/为要挂载的目录

3、查看是否挂载成功

```
df -h
```



```
[root@localhost by-path]# mount ip-192.168.1.182:3260-iscsi-iqn.1991-05.com.targetservice-input-lun-0 /root/kang/
[root@localhost by-path]# df -h
文件系统      容量  已用  可用  已用% 挂载点
/dev/mapper/centos-root 17G  6.2G  11G   37% /
devtmpfs        2.0G   0    2.0G   0% /dev
tmpfs           2.0G   0    2.0G   0% /dev/shm
tmpfs           2.0G  9.5M  2.0G   1% /run
tmpfs           2.0G   0    2.0G   0% /sys/fs/cgroup
/dev/sda1       1014M  157M  858M  16% /boot
tmpfs           396M  12K  396M   1% /run/user/42
tmpfs           396M   0    396M   0% /run/user/0
/dev/sdb        4.9G  20M  4.6G   1% /root/kang
[root@localhost by-path]#
```

图 37 查看挂载成功操作图