## 一、服务端使用Targetcli搭建存储服务器

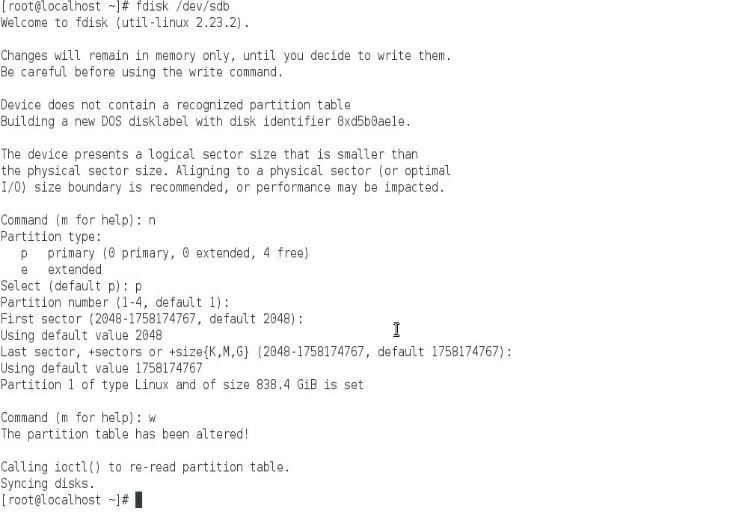
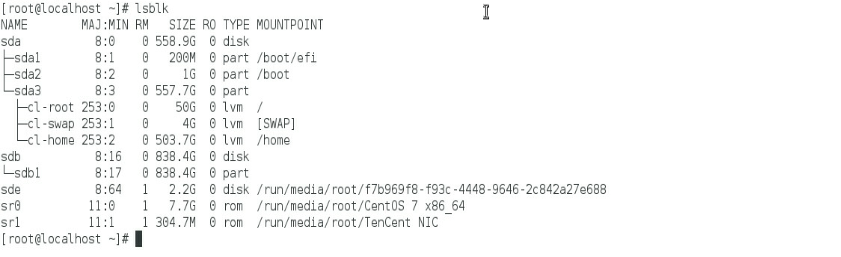
iSCSI连接到一个TCP/IP网络的直接寻址的存储库，通过块I/O SCSI指令对其进行访问。ISCSI是一种基于开放的工业标准，通过它可以用TCP/IP对SCSI(小型计算机系统接口–一种数据传输的公共协议)指令进行封装，这样就可以使这些指令能够通过基于IP(以太网或千兆位以太网)“网络”进行传输。iSCSI连接到一个TCP/IP网络的直接寻址的存储库，通过块I/O SCSI指令对其进行访问。ISCSI是一种基于开放的工业标准，通过它可以用TCP/IP对SCSI(小型计算机系统接口–一种数据传输的公共协议)指令进行封装，这样就可以使这些指令能够通过基于IP(以太网或千兆位以太网)“网络”进行传输。

**环境准备**

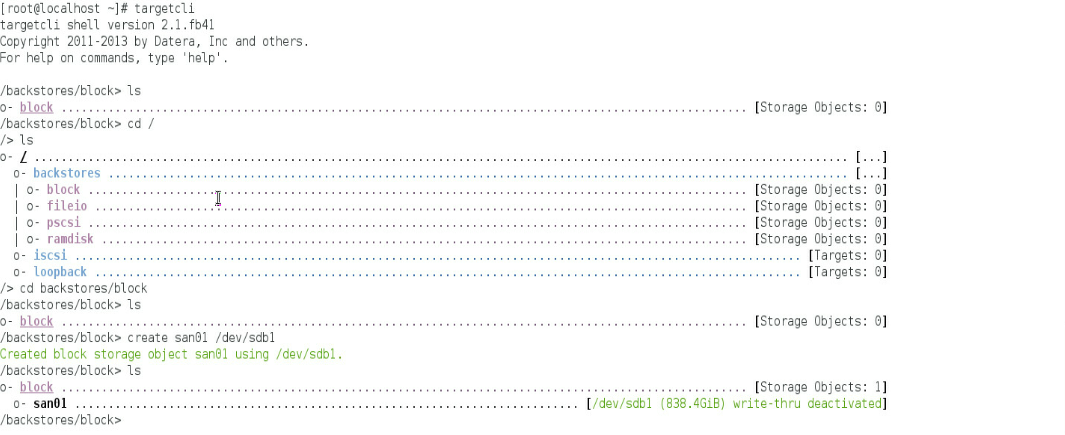
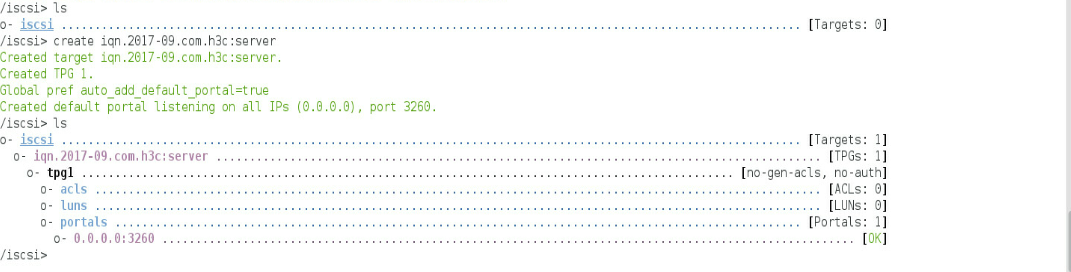
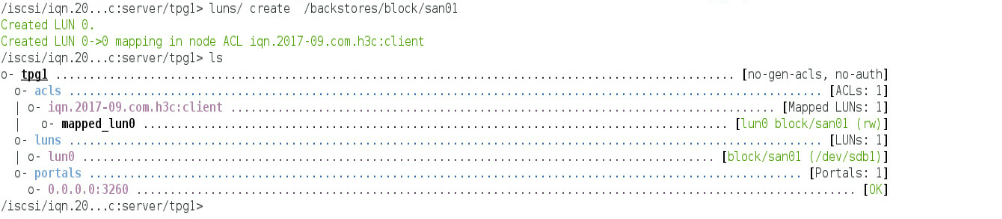
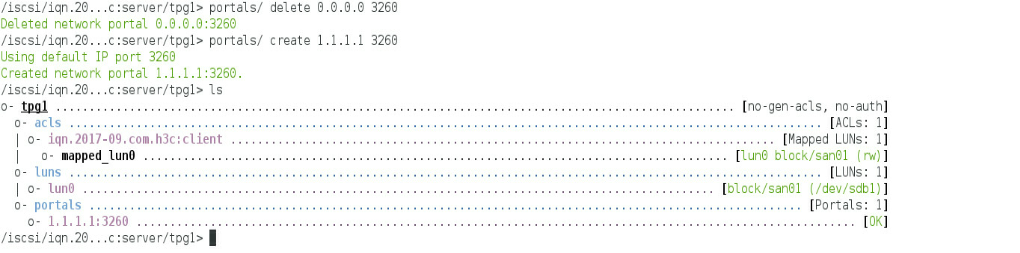
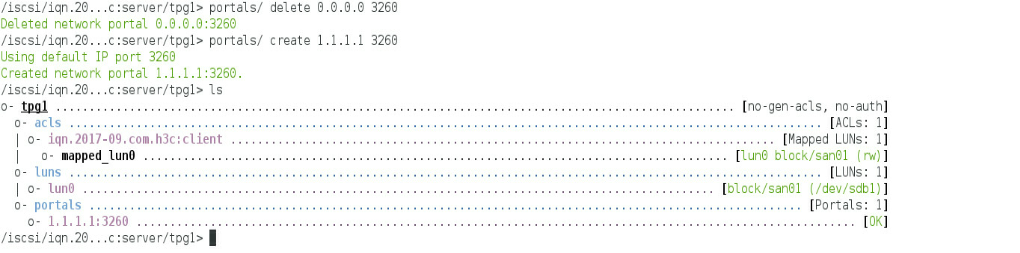
* yum install targetcli
* systemctl enable target
* systemctl start target
* 配置防火墙允许TCP3260端口通过 firewall-cmd --   
  permanent --add-port=3260/tcp或者关闭防火墙systemctl   
  stop firewalld
* 关闭SELinux setenforce 0

*targetcli需要连同依赖包一起卸载才能再次安装，否则单独卸载targetcli再次安装执行会报错*

**准备用于共享的分区或者LVM**

使用fdisk /dev/sdb进行分区操作,创建一个主分区。   
   
使用lsblk命令查看block设备信息   


**Targetcli配置**

1. 选择磁盘，在block设备列表创建san01的block设备   
   
2. 创建target启动器，命名iqn号   
   
3. 设置luns   
   
4. 修改portals   
   
5. 设置ACL，ACL可以通过识别iqn号控制允许连接的启动器   
   
6. 保存配置   
   **二、客户端使用iscsiadm连接iscsi存储**

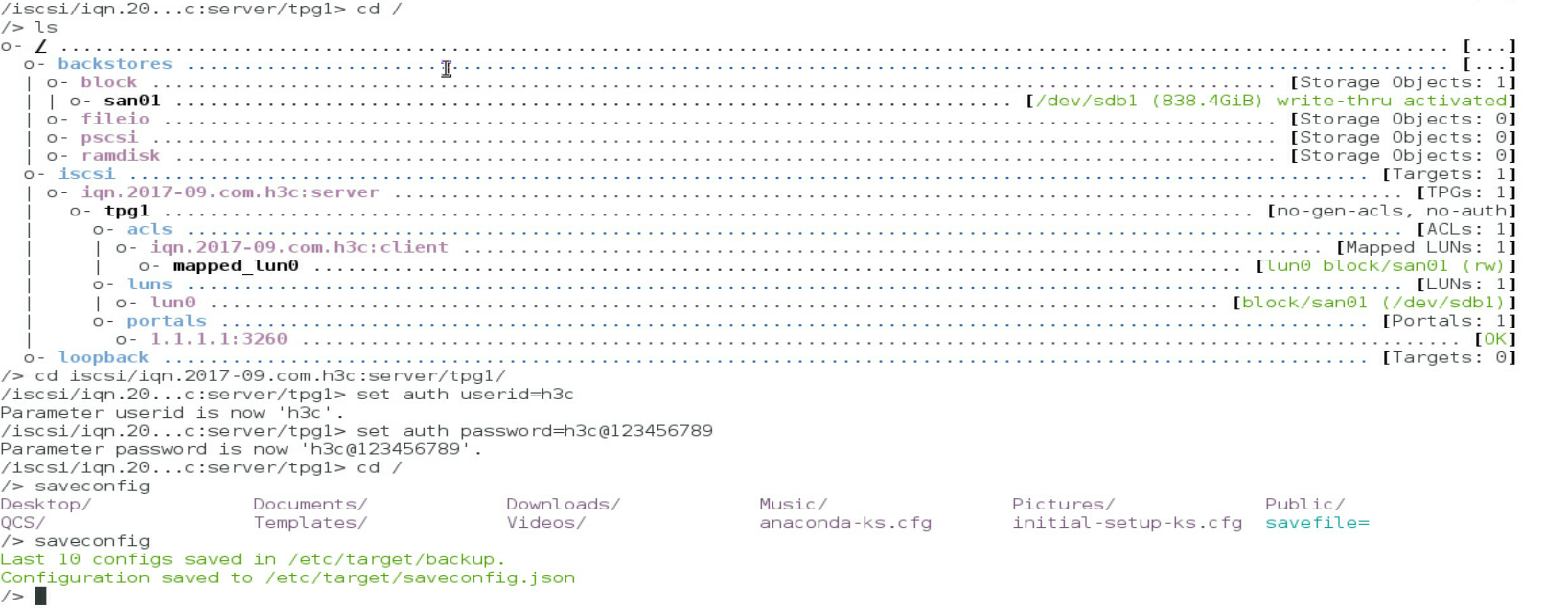
**环境准备**

Redhat系统中iscsi的客户端服务程序initiator已经被默认安装完成。   
如未安装可以使用yum install iscsi-initator-utils

**iscsiadm连接存储**

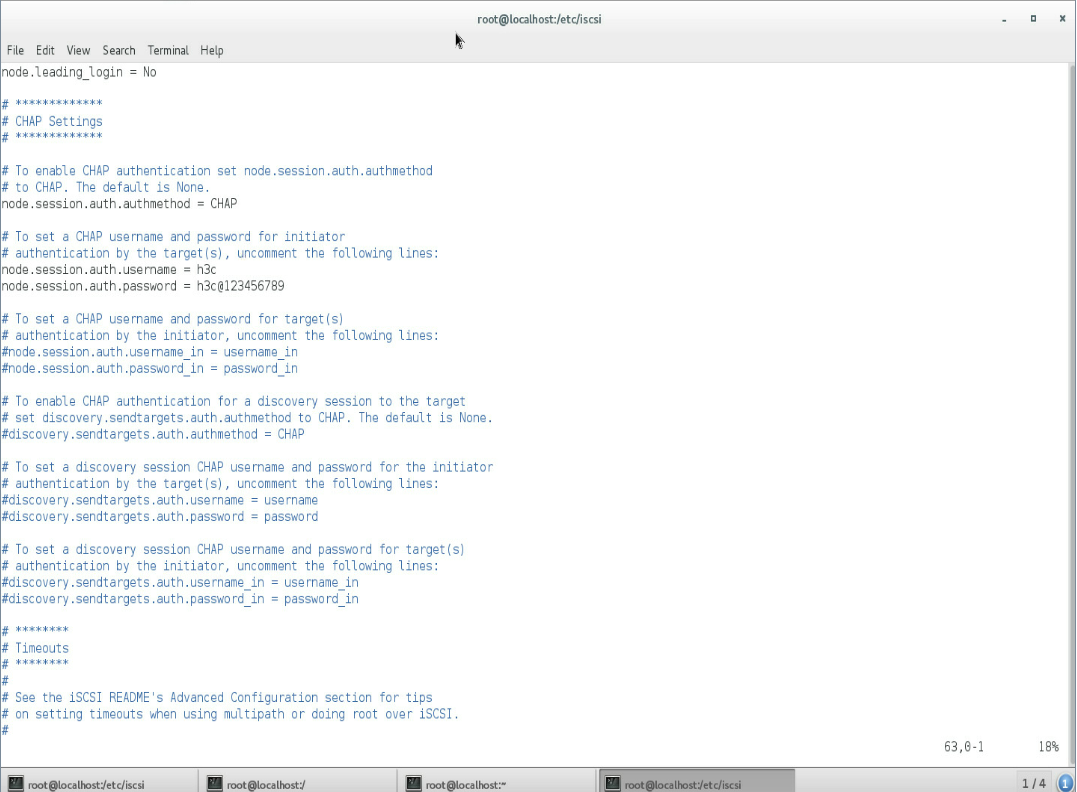
1. 修改initiator IQN号   
   iscsiadm的配置文件存在于/etc/iscsi/目录   
   目录下initiatorname.iscsi文件保存有iscsi启动器的iqn配置   
   修改**iqn号**使其与**Target中配置的ACL允许iqn号相同**   
   修改完成后重新启动iscsi服务systemctl restart iscsid   
   
2. 使用discovery模式发现目标ip所有target   
   iscsiadm -m discovery -t sendtargets -p 1.1.1.1:3260   
   C:\Users\Administrator\Documents\My Knowledge\temp\edc7c1d5-b537-4505-adfe-223563f27b30\128\index_files\discovery.PNG   
   \*\* 记录下查询到的target iqn号 \*\*
3. 使用node模式，登录到节点   
   iscsiadm -m node -T iqn.2017-09.com.h3c:server -p 1.1.1.1:3260 -l
4. **三、CHAP认证开启**

**在iscsi target端，开启CHAP认证**

在targetcli命令行下，进入 /iscsi/iqn.2017-09.com.h3c:server/tgp1/   
使用set auth userid=h3c配置用户名   
使用set auth password=h3c@123456789配置密码   


**在发起端开启并配置CHAP**

**1. 方法一：修改iscsi发起端配置文件**

iscsiadm的配置文件存在于/etc/iscsi/目录   
目录下**iscsid.conf**文件保存有iscsi启动器的连接配置   
修改\*\* CHAP Settings \*\* 选项   
  
使用systemctl restart iscsid重新启动iscsi服务使配置生效。   
然后按照正常操作登录节点即可。

**1. 方法二：使用命令行配置**

使用如下命令添加认证方式与认证信息

* 开启认证   
  iscsiadm -m node -T [装置] -o update --name node.session.auth.authmethod --value=CHAP
* 添加用户   
  iscsiadm -m node -T [装置] --op update --name node.session.auth.username --value=[用户名]
* 添加密码   
  iscsiadm -m node -T [装置] --op update --name node.session.auth.password --value=[密码]

然后按照正常操作登录节点即可。

1. **四、iscsiadm其他操作**

* 删除iscsi发现记录   
  iscsiadm -m node -o delete -T LUN\_NAME -p ISCSI\_IP
* 登出iscsi存储   
  iscsiadm -m node -T LUN\_NAME -p ISCSI\_IP -u
* 登出所有iscsi节点   
  iscsiadm -m node -U all
* 查看那些target记录在Open-iSCSI数据库中   
  iscsiadm -m node
* 查询当前session   
  iscsiadm -m session