1. shell脚本:可以执行的文件,可以实现某种功能
2. 规范shell的一般组成

#!环境声明,下面所有代码由哪一个进程进行翻译

#注释文本,可以写明脚本的作用

可执行的代码

2.脚本中常用的参数

重定向输出

> 只搜集前面命令的正确信息

2> 只收集前面命令的错误信息

&> 不管错误真确的收集

>&2 将当前命令修改位错误输出信息

单引号(’’) 取消所有字符的特殊含义,原样输出

/dev/null 黑洞设备,专门用于收集不要的信息

| 管道,将前面命令的输出赋值给后面的命令

$()或反撇号``:将命令的输出,直接作为参数,参与运用

1. 变量

存在的原因:为了提高脚本适应多变的环境与需求,所以引入变量

变量类似于一个容器:以不变的名称.存储可以变化的值,方便重复运营某一个值

变量名=存储的值 变量的设定方法

定义/赋值变量时注意格式

1. 等号俩边不能有空格
2. 变量名只能有字母/数字/下划线组成,区分大小写
3. 变量名不能以数字开头,不用使用关键字和特殊字符
4. 若指定的变量已经存在,相当于位此变量重新赋值

变量的种类

环境变量:变量名一般为大写字母,有系统定义并赋值完成

USER=当前系统登录的用户名

位置变量:由系统定义提供命令行参数

表示为$n n为序号(1,2,3,4,5)

$n代表脚本后面的第几个参数

$0 代表脚本本身

$# 代表脚本后面参数的个数

#? 代表上一次命令是否执行成功(0代表成功,非0代表失败)

$\* 依次输出脚本后面的参数

预定义变量:有系统定义并赋值完成

$# 一加载位置变量的个数,专门用于用户是否输入参数

自定义变量:由用户自定义完成

查看/引用变量

基本格式

$变量名称 引用变量值

Echo $变量名 echo${变量名} 查看变量值

1. Read

存在的原因:为了降低脚本使用的难度,以及用户的体验,所以产生了交互信息以及提示信息

Read -p ‘屏幕上要显示的信息’

优点:

1. 产生交互
2. 记录用户在键盘的输入内容
3. 将记录的所有内容,最终赋值给一个变量存储
4. 条件测试

[测试表达式] 每一个部分不许有空格

比较正整数的大小参数:

-gt 大于

-ge 大于等于

-eq 等于

-ne 不等于

-lt 小于

-le 小于等于

字符串对比的参数:

== 一致为真

!= 不一致为真

1. if选择结构

if双分支结构

If [条件测试];then

命令序列xx

Else

命令序列yy

Fi

if多分枝结构

if [条件测试];then

命令序列xx

Elif [条件测试];then

命令序列yy

Elif[条件测试];then

命令序列aa

Else

命令序列zz

fi

1. for循环结构:重复性的操作

For循环处理

可以和if结合使用

根据变量的不同取值,重复执行xx处理

便利/列表式循环

列表值可以不参与循环的执行代码

造数工具:制造连续范围的数字

{起始值...结束值}

格式

For 变量名 in 值列表

Do

重复性执行的代码

Done

1. SElinux安全机制

SElinux概述

全称Security-Enhanced Linux

美国NSA国家安全局主导开发,一套增强Linux系统安全的强制访问控制体系

集成到Linux内核(2.6以上)中运行

RHEL基于selinux体系针对用户,进程,目录和文件提供了预设的保护策略,以及管理工具

SElinux运行模式的切换

Selinux的运行模式,任何模式切换到disabled都要重新启动

Enforcing 强制

Permissive 宽松

Disabled 彻底禁止

切换运行模式

临时切换 setenforce 1|0 只影响当前系统此次开机

固定配置 /etc/selinux/config文件 永久配置文件,每次开机默认状态,修改SELIBUX后面的参数

Gentenforce 查看selinux状态的命令

1. 防火墙策略管理

防火墙的作用:隔离,严格过滤入站,允许出站

类型:软件防火墙,硬件防火墙

Firewalld服务基础

Linux的防火墙体系

系统服务:firewalld

管理工具:firewall-cmd,firewall-config

预设安全区域

根据所在网络场所区分,预设保护规则集,区域类型

Pubilc:仅允许访问本机的shh,dhcp,ping,少数几个服务(默认的防火墙)

Trusted:允许任何访问

Block:阻塞任何来访的请求(明确拒接,给出回应)

Drop:丢弃任何来访的数据包(不给客户回应,节省服务器资源)

数据包: 源IP地址 目标IP地址 数据

防火墙进入区域的判断:

1. 首先查看客户端请求数据包中,源IP地址然后检测自己所有区域中那个区域有此源IP地址规则,则进入该区域
2. 如果没有任何一个区域符合,则进入默认区域(public)

防火墙默认区域修改

firewall-cmd --get-default-zone 查看防火墙默认的区域

firewall-cmd --set-default-zone=block(默认的防火墙区域) 修改防火墙默认区域位block

firewall-cmd --get-default-zone 再次查看,防火墙区域是否修改成功

防火墙添加规则

firewall-cmd --zone=public(位那个防火墙区域) --add-service=http(添加那个规则) 为防火墙添加协议

firewall-cmd --zone=public(要查看的区域) --list-all 查看区域规则

添加永久的规则只需要在firewall-cmd 后增加--permanent参数就可以添加永久规则

firewall-cmd --reload 重新加载防火墙的规则,使永久规则生效

firewall-cmd --zone=block(区域) --add-source=172.25.0.10(主机IP) 单独拒接某一个主机的访问

firewall-cmd --zone=block(区域) --remove-source=172.25.0.10(主机IP) 删除添加的跪着

防火墙端口映射

端口:程序服务或协议编号

数据包:源IP地址 目标IP地址 数据 端口

http:默认端口为80

ftp:默认端口位21

Ssh:默认端口位22

添加端口转发的格式:

firewall-cmd --zone=public(区域块) --add-forward-port=port=5423(其他主机要访问的端口):proto=tcp(协议类型):toport=80(转发到80端口)

firewall-cmd --zone=public(区域块) --list-all 查看区域规则

1. iscsi网络磁盘

iscsi（主）----> iscsid（子服务）

iSCSI磁盘的工作模式

Internet SCSI是一种网际SCSI接口(默认端口：3260)

一种基于C/S架构的虚拟磁盘技术,由服务器提供磁盘空间,客户机连接并当成本地磁盘使用

相当于生活中的:冰箱 -----》纸制的包装 ------》木质的包装

Iscsi 的形成的过程

后端存储---->磁盘组---->逻辑单元

backstore,后端存储（ 冰箱 /dev/vdb1）,对应到服务端提供实际存储空间的设备,需要起一个管理名称

target,磁盘组( 木质的包装 ),是客户端的访问目标,作为一个框架,由多个lun组成

Lun,逻辑单元 (动作 将 冰箱 放入 木质的箱子),每一个lun需要关联到某一个后端存储设备,在客户端会视为一块虚拟硬盘

ISCSI Qualified Name 名称规范

Iqn的名称规范的作用:用来识别 target 磁盘组,也用来识别客户机身份

iqn.yyyy-mm.倒序域名:自定义标识

示例:iqn.2016-02.com.example:server0

Iscsi服务器所需要的软件:argetcli,使用yum安装

yum -y install targetcli

安装完成后,执行targetcli命令进行iscsi配置页面

配置顺序和步骤

Ls 查看配置文件的详细信息

/> backstores/block create name=nsd(后端存储的名称) dev=/dev/vdb1(后端存储真实磁盘的路径) 生成后端存储

/> iscsi/ create iqn.2019-08.com.example:server(磁盘组iqn名) 生成磁盘组

/> iscsi/iqn.2019-08.com.example:server/tpg1/luns(磁盘组) create /backstores/block/nsd(后端存储) 将创建好的磁盘组放入后端存储中

/> iscsi/iqn.2019-08.com.example:server/tpg1/acls create iqn.2019-08.com.example:desktop(客户端声称的名字) 设置客户端声称的名字

/> iscsi/iqn.2019-08.com.example:server/tpg1/portals create ip\_address=172.25.0.11(服务端的IP地址) 设置服务端的IP地址,以及开放的端口

重启服务,设置开机自启,服务端配置成功

客户端配置步骤

Yum安装scsi-initiator-utils软件包

Yum仓库可以补全包名前提:

1. 当前系统没有安装此软件

2.必须有yum缓存

修改/etc/iscsi/initiatorname.iscsi文件,设置客户端声称的名字

文件内容修改为:InitiatorName=iqn.2019-08.com.example:desktop

修改完成后,客户端重新启动服务,查看是否配置成功.

发现服务端共享存储:iscsiadm --mode discoverydb --type sendtargets --portal 172.25.0.11(服务端IP地址 ) --discover 可以使用man iscsiadm 命令查看帮助方法

发现完成后,从新启动服务,lsblk验证配置司法正确

总结：

iSCSI服务端：

1.防火墙默认区域设置为trusted

2.划分一个分区

3.安装软件包targetcli

4.运行targetcli进行配置

A：建立后端存储

B：建立target磁盘组

C：lun进行关联

D：设置客户端声称的名字

E：设置本机那个IP地址提供服务

5.重起target服务

客户端：

1.防火墙默认区域设置为trusted

2.安装软件包iscsi-initiator-utils

3.设置客户端声称的名字/etc/iscsi/initiatorname.iscsi

4.重起iscsid刷新客户端声称的名字

5.发现共享存储

五.数据库服务基础

数据库概念:存放数据的仓库,管理数据的一个软件

数据库结构:数据库里有很多的库,每一个库中有很多的表格

常见的关系型 数据库管理系统

微软的 SQL Server

IBM的 DB2

甲骨文的 Oracle、MySQL

社区开源版 MariaDB

现在大多数企业都是从MySQL向MariaDB转型

部署mariadb数据库服务器

mariadb-server:提供服务端有关的系统程序

mariadb:提供客户端及管理工具

使用yum安装

yum -y install mariadb-server 安装软件

ystemctl restart mariadb 启动服务

在linux中设置数据库的密码

数据库管理员和系统管理员在名字上一样以外,其他任何地方没有相同点

数据库管理员：root对数据最高权限，用户信息存放mysql库user表

系统管理员：root对系统最高权限，用户信息存放/etc/passwd

为数据库账号修改密码格式

mysqladmin [-u用户名] [-p[旧密码]] password '新密码'

非交互式改密码示例:mysqladmin -u root -p123456 password '123'(当旧密码不存在时,可以不用填写)

数据库中导入数据

mysql -u root(用户) -p123(用户使用的密码) nsd1907(将文件导入到那个库中) < /root/users.sql(本地的文件路径)

数据库的基本操作

每个命令结束时必须加分号,表示命令的结束

Mysql 进入数据库

Show(查看) databases; 查看所有的库

Create(创建) database nsd; 创建nsd库

Drop(丢弃) database nsd; 删除nsd库

Use(用) mysql; 切换到 mysql库

show tables; 查看当前库中的所有表格

数据库中表格的操作

增 insert

删 delete

改 update

查 select

use nsd1907; 切换到nsd1907库中

select \* from base(表名称); 查询base表中所有表字段、所有表记录

select \* from nsd1907.base; 在其他表中查看nsd1907表中的数据内容

select \*(查看表中的所有字段) from base where(后面为增加的条件) password='123'(条件); 条件查询

desc base; 查看dese表结构

select user,host,password from user; 查看user表中的user,host,password所包含的内容

insert base values('6','Barbara','456789'); 给base表中插入数据,书写顺序为表头顺序

数据库的授权

格式:(不区分大小写)

GRANT 权限列表 ON 数据库名.表名 TO 用户名@客户机地址 IDENTIFIED BY '密码';

示例: grant select on nsd1907.\* to lisi@localhost identified by '123';

结果:当lisi通过localhost本地登陆，输入密码123。将会获得nsd1907库中所有表格的查询权限

使用数据库进行复杂化查询

select \* from base,location where (筛选表内的某一个数据)base.name='Barbara' and(连接符号,同时满足多个条件) location.city='Sunnyvale' and base.id=location.id; 查询base和location表中相同名字,地址,id号一样的数据

select (计数,并且显示出来)count(\*) from base,location where base.name='Barbara' and location.city='Sunnyvale' and base.id=location.id; 查询base和location表中相同名字,地址,id号一样的数据有多少个

禁止空密码root访问mariadb数据库

方法:删除密码为空的记录:delete(删除) from user(表名称) where (密码为空的条件)password=''; 删除密码为空的记录

flush privileges; 刷新user表中的所有记录,时删除空行的密码命令生效

测试: mysql -u root -hserver0.example.com -h 指定登录的用户 此用户登录失败,则说明刚才的配置为成功.

1. 配置NFS共享

NFS共享概述:Network File System,网络文件系统

用途:为客户机提供共享使用的文件夹

使用的协议:NFS(TCP/UDP 2049)、RPC(TCP/UDP 111)

所需软件包:nfs-utils

系统服务:nfs-server

一般虚拟机自带安装NFS所以需要查看: rpm -q nfs-utils

服务端配置过程

创建共享目录

mkdir /public

touch /public/{1..10}.txt

ls /public/

修改配置文件指定共享目录

vim /etc/exports

配置文件修改格式

文件夹路径 客户机地址(权限) 客户机地址(权限)

示例:/public \*(ro) \*号代表允许所有客户端以只读方式访问

重起nfs-server服务: systemctl restart nfs-server

客户端配置:

创建挂载点:mkdir /mnt/nsd

挂载设备:mount 172.25.0.11:/public /mnt/nsd

显示所有正在挂在使用的设备:df -ah

查看挂载点中的测试文件ls /mnt/nsd

修改配置文件,实现开机自动挂载:

netdev:声明网络设备

开机自动挂载条件:首先确保网络服务的启动，然后在挂载本设备

vim /etc/fstab

配置文件格式:172.25.0.11:/student(网络设配) /mnt/test(本机挂载点) nfs(文件系统类型) defaults,\_netdev(说明是网络挂载点) 0(备份标记) 0(检测顺序)

umount /mnt/test/ 卸载刚才命令行挂载的设备

mount -a 使配置文件生效

df -ah 查看所有挂载点

1. HTTP服务（Web服务）：提供网页内容的服务

DNS服务器的作用将虚拟机classroom 将域名解析为IP地址

验证DNS服务器的命令: nslookup server0.example.com(需要解析的域名)

实现Web服务的软件：httpd Nginx Tomcat

Apache（软件基金会） httpd软件

Web通信基本概念

基于 B/S (Browser/Server)架构的网页服务

服务端提供网页

浏览器下载并显示网页

http和html区别

Hyper Text Markup Language（html）,超文本标记语言

Hyper Text Transfer Protocol（http）,超文本传输协议

html（书写网页内容） http（传输页面内容）

/etc/httpd/conf/httpd.conf 主配置文件

/etc/httpd/conf.d/\*.conf 调用配置文件

软件包:httpd

系统服务:httpd

http提供的默认配置

Listen:监听地址:端口(80)

ServerName:本站点注册的DNS名称(空缺)

DocumentRoot:网页文件的根目录(/var/www/html)

DirectoryIndex:起始页/首页文件名(index.html)