NSD1610 · 2016年12月21日

目录

[Network 1](#_Toc470080041)

[1 请分别描述T568A、 T568B的线序 6](#_Toc470080042)

[2、请简要描述交换机的工作原理 6](#_Toc470080043)

[3、MAC地址的长度，组成及单播、组播、广播地址的表示方式 6](#_Toc470080044)

[4、什么是TTL，作用并简要描述TTL的原理 6](#_Toc470080045)

[5、请简要描述网络层有哪些常见协议 7](#_Toc470080046)

[6、什么是HSRP及作用 7](#_Toc470080047)

[7、什么是STP及作用 7](#_Toc470080048)

[8、三层交换机的作用 7](#_Toc470080049)

[9、请简要描述NAT的作用 7](#_Toc470080050)

[10、请描述NAT 的优点及缺点 8](#_Toc470080051)

[Linux 8](#_Toc470080052)

[11、请列举你所知道的Linux发行版与开源软件。 8](#_Toc470080053)

[12、什么是YUM，其作用是什么，主要支持哪几种方式提供软件源？ 9](#_Toc470080054)

[13、vim编辑器的工作模式及切换。 9](#_Toc470080055)

[14、部署LAMP环境需要安装哪些软件 9](#_Toc470080056)

[15、简要说明PXE安装系统流程 9](#_Toc470080057)

[16、请描述RHEL6.x系统的引导过程？ 10](#_Toc470080058)

[17、自定义Shell变量时，变量名有什么规则？ 10](#_Toc470080059)

[18、简述预定义变量$$、$?、$0、$#、$\*、$!的作用。 10](#_Toc470080060)

[19、简述什么是LNMP 11](#_Toc470080061)

[20、地址重写的好处 11](#_Toc470080062)

[21、部署实施CDN的优势是什么 11](#_Toc470080063)

[22、集群有哪些类别？ 11](#_Toc470080064)

[23、 LVS的负载平衡方式有哪些？ 11](#_Toc470080065)

[24.简述RAID的含义及特点 12](#_Toc470080066)

[25.请描述RHEL6.x系统的引导过程？ 12](#_Toc470080067)

[26.SSH协议简介。 12](#_Toc470080068)

[27.Linux常见的系统日志文件都有哪些，各自的用途？ 13](#_Toc470080069)

[28.常见的linux开机设置文件。 13](#_Toc470080070)

[29.请简单说出用户管理的相关命令及用途 13](#_Toc470080071)

[30.请简述基础正则表达式sed高级参数的使用（计时4分钟） 14](#_Toc470080072)

[31.请你描述下crontab的作用和语法，以及书写定时任务注意的要点。 14](#_Toc470080073)

[32.请写出下面Linu命令行快捷键命令的功能？ 15](#_Toc470080074)

[33.如果一台办公室内主机无法上网（打不开网站），请给出你的排查步骤？ 15](#_Toc470080075)

[34.描述Linux shell中单引号、双引号及不加引号的简单区别 16](#_Toc470080076)

[35.简要说明PXE安装系统流程 16](#_Toc470080077)

[36.简单描述虚拟化技术常见的虚拟网络类型 16](#_Toc470080078)

[37.简述DNS递归和迭代查询的作用 16](#_Toc470080079)

[38.为什么使用LAMP？ 17](#_Toc470080080)

[39.DNS的解析过程？ 17](#_Toc470080081)

[40.DNS的工作原理？ 17](#_Toc470080082)

[Shell 18](#_Toc470080083)

[1 自定义Shell变量时，变量名有什么规则？ 18](#_Toc470080084)

[2 简述预定义变量$$、$?、$0、$#、$\*、$!的作用。 18](#_Toc470080085)

[3 简述三种定界符在变量赋值操作中的特点。 18](#_Toc470080086)

[4 列出常见的整数值比较操作，并说明各自作用。 19](#_Toc470080087)

[5 简述Shell环境常见的中断及退出控制指令。 20](#_Toc470080088)

[6 正则表达式中的+、？、\*分别表示什么含义？ 20](#_Toc470080089)

[7 简述awk工具常用的内置变量、各自的作用。 20](#_Toc470080090)

[8, 什么是shell？如何查看当前系统支持的Shell? 20](#_Toc470080091)

[9，如何切换当前使用的shell 21](#_Toc470080092)

[10、/bin/bash特性有哪些 21](#_Toc470080093)

[11、用户配置文件是哪几个?有什么用？ 21](#_Toc470080094)

[12、系统配置文件是哪几个？有什么用？ 21](#_Toc470080095)

[13、shell变量类型有哪些？列举出常用的4个预定义变量 21](#_Toc470080096)

[14、自定义变量的命名规则？ 21](#_Toc470080097)

[15、变量的生命周期，和作用范围？ 21](#_Toc470080098)

[16、脚本的执行过程？脚本的执行方式？ 22](#_Toc470080099)

[17、编写脚本的步骤？ 22](#_Toc470080100)

[18、Shell条件判断类型？ 22](#_Toc470080101)

[19、eval在shell中有什么作用？请举个例子说明？ 22](#_Toc470080102)

[20、dirname有什么作用？请举个例子说明？ 22](#_Toc470080103)

[21、ssh -o stricthostkeychecking=no -o ConnectTimeout=60 分别代表什么意思？ 23](#_Toc470080104)

[22、说一下-n -z -d -f -e -r -w -x -l !-z在shell中分别代表什么意思？-n和-z试举一个例子说明 23](#_Toc470080105)

[23、正则表达式的"|"、"\n"、"\r"、"\t"分别代表什么意思 23](#_Toc470080106)

[24、写出获取公网IP的两种方法 24](#_Toc470080107)

[25、$$表示什么意思？ 24](#_Toc470080108)

[26、函数内的local是什么意思?举一脚本例子说明 24](#_Toc470080109)

[27、$@和$\*的区别 24](#_Toc470080110)

[28、$0、dirname和basename有什么作用？具个例子说明？ 24](#_Toc470080111)

[29、取出3306端口号这个数字 26](#_Toc470080112)

[30、shell中单引号和双引号与不加与号分别代表什么意思 26](#_Toc470080113)

[31、echo -n 是什么意思？举一脚本例子显示他的功能 26](#_Toc470080114)

[32、echo -e "\n" | nohup ping www.baidu.com > filename 2>&1 &这里的-e 和"\n" 是什么意思？ 26](#_Toc470080115)

[33、有1-9的数字，echo输出1-9的数字时，屏蔽0-5的数字再输出 27](#_Toc470080116)

[34、用nohup把一个脚本放在后台运行 27](#_Toc470080117)

[35、用seq打印10以空格分隔，用seq坚着打印10到1 27](#_Toc470080118)

[36、curl -I -s www.baidu.com | head -1 | wc -l 中的-I和-s代表什么意思 27](#_Toc470080119)

[37、wget -T 10 -c -q --spider www.baidu.com 这些参数分别代表什么意思？ 27](#_Toc470080120)

[38、生产环境常用的监控web的方法是哪种 27](#_Toc470080121)

[39、生产环境写脚本报错就发邮件的命令是怎么样的 28](#_Toc470080122)

[40、给文件改名 28](#_Toc470080123)

[41、查看当前目录的所有文件夹 28](#_Toc470080124)

[42、awk中的NF代表什么意思？ 28](#_Toc470080125)

[43、shell上: 0、1>、2>、>、2>&1、&>/dev/null分别代表什么意思 28](#_Toc470080126)

[Mysql 28](#_Toc470080127)

[100、 MySQL数据库的服务进程叫什么名字？监听端口是多少？默认数据库目录是？ 28](#_Toc470080128)

[1 主流数据库服务软件有哪些？开源且跨平台的数据库软件有哪些？ 29](#_Toc470080129)

[2 MySQL数据库的服务进程叫什么名字？监听端口是多少？默认数据库目录是？ 29](#_Toc470080130)

[3 MySQL默认的3个库叫什么名字？哪个库里的数据不占用物理磁盘空间？ 29](#_Toc470080131)

[4 请列出MySQL常用的数据类型，并写出定义这些数据类型所使用的关键字。 29](#_Toc470080132)

[5 简述索引的优点与缺点，默认情况下哪个文件保存表的索引信息？ 30](#_Toc470080133)

[6 简述在表中创建外键字段要满足那些条件？ 30](#_Toc470080134)

[7 简述MySQL体系结构的组成，并描述每个组成部分的作用。 30](#_Toc470080135)

[8 简述MySQL数据库访问的执行过程。 31](#_Toc470080136)

[9 简述MySQL数据库中插入、更新、查询、删除表记录的指令格式。 31](#_Toc470080137)

[10 简述用户授权命令的语法格式。 32](#_Toc470080138)

[11 在MySQL-MMM集群中有几种角色，各自的功能是什么？ 33](#_Toc470080139)

[12 在MySQL-MMM集群中可以有多少台主数据库服务器、多少台从数据库服务器？ 33](#_Toc470080140)

[13 在MySQL-MMM集群中均衡模式和排他模式的作用是？ 33](#_Toc470080141)

[14,简述mysqldump备份数据时数据库名的表示方式。 33](#_Toc470080142)

[15 什么是MySQL集群？ 33](#_Toc470080143)

[16，MySQL集群和MySQL 有和不同？ 35](#_Toc470080144)

[17 MySQL 集群的特点？ 35](#_Toc470080145)

[18 MySQL 集群有一些创建高可用性系统的专用功能，主要包括？ 35](#_Toc470080146)

[19 MySQL中myisam与innodb的区别，至少5点 35](#_Toc470080147)

[myisam 35](#_Toc470080148)

[innodb 35](#_Toc470080149)

[memory 35](#_Toc470080150)

[archive 35](#_Toc470080151)

[20什么是读写分离？ 36](#_Toc470080152)

[21读写分离的好处 36](#_Toc470080153)

[22 读写分离提高性能之原因 36](#_Toc470080154)

[23 varchar与char的区别；varchar(50)中50的涵义；int(20)中20的涵义； 36](#_Toc470080155)

[24 计划，mysqldump以及xtranbackup的实现原理；备份恢复时间；备份恢复失败如何处理。 37](#_Toc470080156)

[25 MySQL中InnoDB引擎的行锁是通过加在什么上完成(或称实现)的？为什么是这样子的？ 37](#_Toc470080157)

[26 MySQL 数据库备份方式 37](#_Toc470080158)

[27 MySQL主从复制原理？ 37](#_Toc470080159)

[28 mysql-mmm简介 38](#_Toc470080160)

[29 mysql-mmm 组成与原理 39](#_Toc470080161)

[30 多源复制下，支持master是5.6，slave是5.7吗？ 39](#_Toc470080162)

[31 半同步复制设置N个slave应答，如果当前Slave小于N会怎样？ 39](#_Toc470080163)

[32 gtid 如果出现不支持的语句，怎么解决 40](#_Toc470080164)

[33 基于GTID的复制，可以指定GTID复制的起始位置么，还是只能根据现有的信息？ 40](#_Toc470080165)

[34 对一个已经开启GTID的数据库再做一个从库，先把Master备份下来还原到新slave上去，直接可以同步了还是先需要做purge\_gtid的操作再同步呢？ 40](#_Toc470080166)

[35 线上全是5.5的环境，有没有办法搭建5.5到5.7的复制？ 40](#_Toc470080167)

[36 并行复制logical\_clock，如果不开启gtid是不是就不能并行了？ 41](#_Toc470080168)

[37 在主从复制过程中，是主向从推数据还是从拉数据，如果这个传送的过程中，出现网络闪断，会不会造成数据包丢失，会执行校验重传嘛？ 41](#_Toc470080169)

[38 设置了binlog\_group\_commit\_sync\_delay参数，在宕机的时候应该不会影响binglog文件安全吧？ 41](#_Toc470080170)

[39 多源复制是只能在异步模式下使用么？因为半同步的状态是全局的，一个通道关闭会导致其它通道出错，有没有考虑将半同步状态改成每个channel的私有配置呢？ 41](#_Toc470080171)

[OPERATION 42](#_Toc470080172)

[1 简述Squid的优缺点有哪些 42](#_Toc470080173)

[2 简述常见Web服务器软件有哪些 42](#_Toc470080174)

[3 简述什么是LNMP 42](#_Toc470080175)

[4 地址重写的好处 43](#_Toc470080176)

[5 简述什么是memcached 43](#_Toc470080177)

[6 部署实施CDN的优势是什么 43](#_Toc470080178)

[6 Nginx 的优点? 43](#_Toc470080179)

[7Nginx和Apache的综合对比？Web服务器 44](#_Toc470080180)

[Nginx 44](#_Toc470080181)

[Apache 44](#_Toc470080182)

[8，什么是CDN？ 44](#_Toc470080183)

[9，CDN的类型特点？ 44](#_Toc470080184)

[10 CDN的工作原理？ 45](#_Toc470080185)

[SECURITY 46](#_Toc470080186)

[1 简述信息安全防护的目标和一般原则。 46](#_Toc470080187)

[2 根据攻击/防护的对象不同，安全工作一般区分为哪些类别？ 47](#_Toc470080188)

[3 简述实现SSH密钥对验证的基本过程。 47](#_Toc470080189)

[4 简述RHEL6系统中SELinux机制的三种运行模式。 47](#_Toc470080190)

[5 简述向证书颁发机构（CA）申请数字证书的过程。 47](#_Toc470080191)

[6 简述基于Apache HTTP Server实现HTTPS安全通信的部署过程。 48](#_Toc470080192)

[7 加密的邮件通信协议及端口分别有哪些？ 48](#_Toc470080193)

[8 在网络安全工作中，扫描技术可以达成哪些目标？ 48](#_Toc470080194)

[9 iptables默认的规则链有哪些，各自的作用是什么？ 48](#_Toc470080195)

[10 iptables处理数据包的基本目标操作有哪些，各自的作用是什么？ 49](#_Toc470080196)

[11 iptables的filter过滤表包括的默认规则链是哪几个？ 49](#_Toc470080197)

[12 简述iptables状态跟踪机制所处理的几种数据包类型。 49](#_Toc470080198)

[13 简述基于DNAT策略发布私网服务器的工作原理。 49](#_Toc470080199)

[MONITOR 50](#_Toc470080200)

[1 监控描述Nagios与Cacti的区别 50](#_Toc470080201)

[2 简单描述Zabbix具有哪些监控功能 50](#_Toc470080202)

[3 Nagios的系统特点？ 51](#_Toc470080203)

[CLUSTER 51](#_Toc470080204)

[1 服务器创建存储技术有哪些？ 51](#_Toc470080205)

[2 集群有哪些类别？ 51](#_Toc470080206)

[3 LVS的负载平衡方式有哪些？ 51](#_Toc470080207)

[4 写出至少四种LVS负载平衡的调度算法 52](#_Toc470080208)

[5 HAProxy工作模式有哪些？ 52](#_Toc470080209)

[6 HAProxy配置文件有哪些组成部分？ 52](#_Toc470080210)

[7 写出RHCS的核心组件名称？ 52](#_Toc470080211)

[8 写出RHCS高可用集群配置流程 53](#_Toc470080212)

[9 LVS 三种工作模式原理、以及优缺点比较 53](#_Toc470080213)

[常用服务的端口 55](#_Toc470080214)

# NETWORK

## 1 请分别描述T568A、 T568B的线序

**参考答案**

T568A：白绿、绿、白橙、蓝、白蓝、橙、白棕、棕

T568B：白橙、橙、白绿、蓝、白蓝、绿、白棕、棕

## 2、请简要描述交换机的工作原理

**参考答案**

初始状态

根据源MAC地址学习

除源端口外的端口广播未知数据帧

接收方回应

交换机实现单播通信

## 3、MAC地址的长度，组成及单播、组播、广播地址的表示方式

**参考答案**

MAC地址长度48位，前24位代表厂商，后24位代表网卡编号，MAC 地址的第8位为0时表示该MAC地址为单播地址，为1时表示组播地址，48位都为1表示广播地址

## 4、什么是TTL，作用并简要描述TTL的原理

**参考答案**

TTL是数据生命周期

作用：避免数据在网络中无限循环转发

原理：当网络中的数据包每经过一个路由器TTL值减1，当TTL值为0时，数据包丢弃。

## 5、请简要描述网络层有哪些常见协议

**参考答案**

ARP协议

RARP协议

代理ARP

ICMP协议

## 6、什么是HSRP及作用

**参考答案**

HSRP:热备份路由选择协议

作用：确保了当网络边缘设备或接入链路出现故障时，用户通信能迅速并透明地恢复，以此为IP网络提供冗余性。通过使用同一个虚拟IP地址和虚拟MAC地址，LAN网段上的两台或者多台路由器可以作为一台虚拟路由器对外提供服务。

## 7、什么是STP及作用

**参考答案**

STP ：生成树协议

作用：逻辑上断开环路，防止广播风暴的产生。当线路故障，阻塞接口被激活，恢复通信，起备份线路的作用。

## 8、三层交换机的作用

**参考答案**

三层交换机是具有网络层功能的交换机，三层交换=二层交换+三层转发，使用三层交换技术实现VLAN间通信。

## 9、请简要描述NAT的作用

**参考答案**

通过将内部网络的私有IP地址翻译成全球唯一的公网IP地址，使内部网络可以连接到互联网等外部网络上。

## 10、请描述NAT 的优点及缺点

**参考答案**

优点：

节省公有合法IP地址

处理地址重叠

增强灵活性

安全性

缺点：

延迟增大

配置和维护的复杂性

不支持某些应用，可以通过静态NAT映射来避免

# Linux

## 11、请列举你所知道的Linux发行版与开源软件。

**参考答案**

常见的Linux发行版：

* Red Hat Enterprise Linux 5/6
* CentOS 5/6
* Suse Linux Enterprise 11
* Debian Linux 6.0
* Ubuntu Linux 13.04/13.10
* Oracle Linux 6

常见的开源软件：

* Apache HTTP Server
* MySQL Database
* PHP
* Libre Office
* Firefox
* Nginx

## 12、什么是YUM，其作用是什么，主要支持哪几种方式提供软件源？

**参考答案**

是一种基于“C/S”结构的RPM软件更新机制，所有的软件包由集中的软件仓库提供，能够自动分析并解决软件包之间的依赖关系。

支持的软件源主要包括：

* 本地文件夹：file://.. ..
* FTP服务器：ftp://.. ..
* HTTP服务器：http://

## 13、vim编辑器的工作模式及切换。

vim编辑器包括哪几种模式，各自的作用是什么，如何切换？

**参考答案**

主要包括三种工作模式：

* 命令模式：启动vim编辑器后默认进入命令模式，该模式中主要完成如光标移动、字符串查找，以及删除、复制、粘贴文件内容等相关操作。
* 输入模式：该模式中主要的操作就是录入文件内容，可以对文本文件正文进行修改、或者添加新的内容。处于输入模式时，vim编辑器的最后一行会出现“—插入 --”的状态提示信息。
* 末行模式：该模式中可以设置vim编辑环境、保存文件、退出编辑器，以及对文件内容进行查找、替换等操作。处于末行模式时，vim编辑器的最后一行会出现冒号“:”提示符。

## 14、部署LAMP环境需要安装哪些软件

**参考答案**

httpd、mysql-server、mysql、php、php-mysql

## 15、简要说明PXE安装系统流程

**参考答案**

1. 客户端向DHCP服务器请求分配IP地址；
2. DHCP服务器为客户端分配IP地址，告知Boot server；
3. 客户端向Boot server请求下载启动文件；
4. Boot server向客户端提供启动文件；
5. 客户端向文件共享服务器请求应答文件；
6. 客户端根据应答文件信息，安装操作系统。

## 16、请描述RHEL6.x系统的引导过程？

**参考答案**

* 加载BIOS，检查硬件信息
* 读取并执行第一个开机设备内MBR
* 运行grub引导加载 kernel
* 内核启动/sbin/init程序
* init 系统初始化
* 确定默认的运行级别
* 触发runlevel事件，运行/etc/rc.d/rc
* 最后执行/etc/rc.d/rc.local
* 加载终端或X-Window接口

## 17、自定义Shell变量时，变量名有什么规则？

**参考答案**

* 可以包括数字、字母、下划线，不能以数字开头
* 变量名区分大小写
* 赋值时等号两边不要有空格
* 尽量不要使用关键字和特殊字符
* 给同一个变量多次赋值时，最后一次的赋值生效

## 18、简述预定义变量$$、$?、$0、$#、$\*、$!的作用。

**参考答案**

* $$ 保存当前运行进程的（PID）号
* $? 保存命令执行结果的（返回状态）
* $0 保存当前运行的（进程名）或（脚本名）
* $# 保存位置变量的（个数）
* $\* 保存所有位置变量的（值）
* $! 保存后台（最后一个进程）的PID号

## 19、简述什么是LNMP

**参考答案**

LNMP是网站运行平台。

* L：操作系统（Linux）
* N：网站服务软件（Nginx）
* M：数据库服务软件（MySQL）
* P：网站开发语言（PHP、perl、python）

## 20、地址重写的好处

**参考答案**

* 缩短URL，隐藏实际路径提高安全性；
* 易于用户记忆和键入；
* 易于被搜索引擎收录。

## 21、部署实施CDN的优势是什么

**参考答案**

* 本地Cache加速，提升访问速度和稳定性
* 网站镜像，消除不同地区、运营商网络互连的问题
* 智能DNS解析，自动选择最快的Cache服务器
* 负载优化，减轻后端源Web服务器的压力负载
* 集群抗攻击，有效降低DDOS攻击的影响

## 22、集群有哪些类别？

**参考答案**

* 高性能计算集群HPC：通过以集群开发的并行应用程序，解决复杂的科学问题。
* 负载均衡（LB）集群：客户端访问负载可以在计算机集群中尽可能平均地分摊处理。
* 高可用（HA）集群：当集群中的一个系统发生故障时，集群软件迅速做出反应，将该系统的任务分配到集群中其它正在工作的系统上执行。

## 23、 LVS的负载平衡方式有哪些？

**参考答案**

* VS/NAT：通过网络地址转换实现的虚拟服务器。Director将用户请求报文的目的地址改成选定的Real Server地址后，转发给Real Server。大并发访问时，调度器的性能成为瓶颈。
* VS/DR：直接使用路由技术实现虚拟服务器。通过改写请求报文的MAC地址，将请求发至Real Server，Real Server直接响应客户端。
* VS/TUN：通过隧道方式实现虚拟服务器。Director采用隧道技术将请求发至Real Server后，Real Server直接响应客户端。

## 24.简述RAID的含义及特点

RAID的含义及优势？RAID0、RAID1、RAID5分别指什么、各自的特点？

参考答案

1）RAID：廉价冗余磁盘阵列，指通过硬件/软件技术将多个较小/低速的磁盘整合成一个大磁盘使用的一种存储技术，其不仅可存储数据，还可以实现一定程度的冗余保障，具有“速度快、安全性高”的优势。

2）RAID0、RAID1、RAID5的含义及特点如下：

RAID0：条带模式，由两个或两个以上的磁盘组成，同一份文档分散在不同的磁盘中，并行写入，提高写效率。

RAID1：镜像模式，由至少两个磁盘组成，同一份文件被分别写入到不同的磁盘中，每份磁盘数据一样，实现容错，提高读效率。

RAID5：分布式奇偶校验的独立磁盘模式，结合RAID0和RAID1的好处，同时避免它们的缺点。由至少3块以上大小相同的磁盘组成，实现冗余。

## 25.请描述RHEL6.x系统的引导过程？

加载BIOS，检查硬件信息

读取并执行第一个开机设备内MBR

运行grub引导加载kernel

内核启动/sbin/init程序

init 系统初始化

确定默认的运行级别

触发runlevel事件，运行/etc/rc.d/rc

最后执行/etc/rc.d/rc.loc

## 26.SSH协议简介。

OpenSSH服务器使用的协议、默认端口、主配置文件分别是什么？SSH与Telnet应用的区别在哪里？

参考答案

OpenSSH使用TCP协议，默认端口是22，主配置文件/etc/ssh/sshd\_config。

SSH的英文全称是Secure SHell，即安全外壳。SSH会把传输过程中的数据加密，且支持压缩以提高传输速度；而Telnet在网络上以明文传送口令和数据，安全级别低，容易受到攻击。

## 27.Linux常见的系统日志文件都有哪些，各自的用途？

/var/log/messages 内核及公共消息日志

/var/log/cron 计划任务日志

/var/log/dmesg 系统引导日志

/var/log/maillog 邮件系统日志

/var/log/secure 记录与访问限制相关日志

## 28.常见的linux开机设置文件。

/etc/fstab与/etc/initab、/etc/rc.local三个配置文件的作用？

参考答案

/etc/fstab：实现开机自动挂载设备的配置文件

/etc/initab：定义开机进入默认级别的配置文件

/etc/rc.local：定义开机自定义任务的配置文件

## 29.请简单说出用户管理的相关命令及用途

#组管理命令

groupadd #添加组

groupdel #删除用户组

groupmod #修改用户组

groups #显示当前用户所属的用户组

grpck #检查用户组及密码文件的完整性（etc/group以及/etc/gshadow文件）

grpconv #通过/etc/group和/etc/gshadow 的文件内容来同步或创建/etc/gshadow ，如果/etc/gshadow 不存在则创建；

grpunconv #通过/etc/group 和/etc/gshadow 文件内容来同步或创建/etc/group ，然后删除gshadow文件。

#用户管理命令

useradd #添加用户

adduser #添加用户

passwd #为用户设置密码

usermod #修改用户命令，可以通过usermod 来修改登录名、用户的家目录等等

pwcov #同步用户从/etc/passwd 到/etc/shadow

pwck #pwck是校验用户配置文件/etc/passwd 和/etc/shadow文件内容是否合法或完整

pwunconv #执行pwunconv指令可以关闭用户投影密码，它会把密码从shadow文件内，重回存到passwd文件里。

finger #查看用户信息工具（危险命令，一般不用）

id #查看用户的UID、GID及所归属的用户组

chfn #更改用户信息工具

su #用户切换工具

## 30.请简述基础正则表达式sed高级参数的使用（计时4分钟）

解答：

-n取消默认输出

-p 打印

-d删除

-e允许多项编辑

sed取行，要特别注意sed -n 's###g' filename 的使用，sed的\( \)的功能可以记住正则表达式的一部分，其中，\1为第一个记住的模式即第一个小括号中的匹配内容，\2第二记住的模式，即第二个小括号中的匹配内容，sed最多可以记住9个。

实际字符的选择最好要唯一，正则表达式是贪婪的，总是尽可能的匹配更远的符合匹配的内容，另外注意字符串中的空格。

## 31.请你描述下crontab的作用和语法，以及书写定时任务注意的要点。

设置crontab后我们可以使得Linux主动执行的在固定的间隔时间，执行指定的系统指令或shell script脚本。生产环境可以用来日志分析或生产备份等。

语法格式：

crontab [ -u user ] file ===》-u的意思就是指定用户

crontab [ -u user ] { -l 显示文件内容| -r全部删除crontab文件| -e 编辑crontab文件| -i删除crontab文件前确认提示}

举例：

\*/5 10，12 \* 3-8 \* \* /usr/sbin/ntpdate 10.0.0.155 >/dev/null 2>&1

前五段是时间间隔的设定，单位分别是分钟、小时、日、月、周（尽量避免使用日月和周同时出现，以免造成系统误判）。

第一个时间段分钟范围0-59

第二个时间段小时范围0-23

第三个世间段日范围1-31

第四个时间段月范围1-12

第五个时间段周范围0-7

\*星号代表任何时间都接受命令

，逗号，表示隔开。代表分隔的时间都适用此命令。

-减号，两个时间段之间，代表在此时间段内执行定时任务。

/n斜线和n（数字）表示每隔n段时间执行一次。

注意要点分为：书写基本要领与书写注意事项

7个基本要领：

第一、为定时任务规则加必要的注释

第二、定时任务命令或程序最好写到脚本里执行

第三、定时任务执行的脚本要规范路径，如：/server/scripts

第四、执行shell脚本任务时前加/bin/sh

执行定时任务时，如果是执行脚本，尽量在脚本前面带上/bin/sh命名

第五、定时任务结尾加>/dev/null 2>&1

第六、/dev/null为特殊的字符设备文件，表示黑洞设备或空设备。

第七、有关重定向的说明

>或1> 输出重定向：把前面输出的东西输入到后边的文件中，会删除文件原有内容。

>>或1>> 追加重定向：把前面输出的东西追加到后边的文件中，不会删除文件原有内容。

<或<0 输入重定向：输入重定向用于改变命令的输入，指定输入内容，后跟文件名。

<<或<<0 输入重定向：后跟字符串，用来表示“输入结束”，也可用ctrl+d来结束输入。

2> 错误重定向：把错误信息输入到后边的文件中，会删除文件原有内容。

2>> 错误追加重定向：把错误信息追加到后边的文件中，不会删除文件原有内容。

标准输入（stdin）：代码为0，使用<或<<。

标准输出（stdout）:代码为1，使用>或>>。正常的输出。

标准错误输出（sederr）：代码为2，使用2>或2>>。

特殊：

2>&1就是把标准错误重定向到标准输出（>&）。

>/dev/null 2>&1 等价于1>/dev/null 2>/dev/null

## 32.请写出下面Linu命令行快捷键命令的功能？

Ctrl + a 光标到开头

Ctrl + c 中断当前程序

Ctrl + d 退出当前窗口或当前用户

Ctrl + e 光标到结尾

Ctrl + l 清屏相当与clear

Ctrl + u 剪切、删除（光标以前的）内容

Ctrl + k 剪切、删除（光标以后的）内容

Ctrl + r 查找（最近用过的命令）

tab 所有路径以及补全命令

Ctrl+shift+c 命令行复制内容

Ctrl+shift+v 命令行粘贴内容

Ctrl + q 取消屏幕锁定

Ctrl + s 执行屏幕锁定

## 33.如果一台办公室内主机无法上网（打不开网站），请给出你的排查步骤？

①首先确定物理链路是否联通正常。

②查看本机IP，路由，DNS的设置情况是否达标。

③telnet检查服务器的WEB有没有开启以及防火墙是否阻拦。

④ping一下网关，进行最基础的检查，通了，表示能够到达服务器。

⑤测试到网关或路由器的通常情况，先测网关，然后再测路由器一级一级的测试。

⑥测试ping公网ip的通常情况（记住几个外部IP），

⑦测试DNS的通畅。ping出对应IP。

⑧通过以上检查后，还在网管的路由器上进行检查。

## 34.描述Linux shell中单引号、双引号及不加引号的简单区别

单引号：所见即所得，即将单引号内的内容原样输出，或者描述为单引号里面看到的是什么就输出什么。

双引号：把双引号里面的内容给输出出来，如果内容中有命令、变量等，会先把，变来那个、命令解析出结果，然后输出最终内容。

双引号内的命令或者变量写法’命令或变量’或$(命令或变量)

无引号：把内容输出出来，可能不会键含有空格的字符串，视为一个整体输出，如果内容中有命令、变量等，会先把变量、命令解析出来，然后输出最终内容，如果字符串中带有空格等特殊字符，则不能完整输出，需要改加双引号。一般连续的字符串，数字，路径等可以用，不过最好用双引号，替代之。

## 35.简要说明PXE安装系统流程

参考答案

客户端向DHCP服务器请求分配IP地址；

DHCP服务器为客户端分配IP地址，告知Boot server；

客户端向Boot server请求下载启动文件；

Boot server向客户端提供启动文件；

客户端向文件共享服务器请求应答文件；

客户端根据应答文件信息，安装操作系统

## 36.简单描述虚拟化技术常见的虚拟网络类型

参考答案

桥接模式：Guest与Host连接到同一个交换机上，通过桥接物理网卡，相当于直连到Host所在网络。

隔离模式：Guest可访问同一虚拟交换机上的其他Guest，但无法访问Host所在外部网络。

NAT模式：Guest的网关指向Host的virtbr0的IP地址，允许虚拟机共享真机的网络连接。

路由模式：由Host充当路由器，开启转发，需要额外设置外网与Guest之间互访的路由

## 37.简述DNS递归和迭代查询的作用

参考答案

对于一台DNS服务器来说：

若允许递归，则当客户端请求解析的域名非本DNS管辖时，本DNS会向其他DNS服务器代询；

若不允许递归，则当客户端请求解析的域名非本DNS管辖时，本DNS会放弃代询——但是，如果目标地址位于已知的某个授权子域，本DNS会告知客户端对应的子DNS服务器的地址信息（即迭代）。

## 38.为什么使用LAMP？

答案：因为LAMP 具有Web 资源丰富、轻量、快速开发等特点，与微软的.NET 架构相比，LAMP 具有通用、跨平台、高性能、低价格优势、因此LAMP 无论是性能、质量还是价格都是企业搭建网站的首选平台。

## 39.DNS的解析过程？

答案：第一步：客户机提出域名解析请求,并将该请求发送给本地的域名服务器。

第二步：当本地的域名服务器收到请求后,就先查询本地的缓存,如果有该纪

录项,则本地的域名服务器就直接把查询的结果返回。

第三步：如果本地的缓存中没有该纪录,则本地域名服务器就直接把请求发

给根域名服务器,然后根域名服务器再返回给本地域名服务器一个

所查询域(根的子域)的主域名服务器的地址。

第四步：本地服务器再向上一步返回的域名服务器发送请求,然后接受请求

的服务器查询自己的缓存,如果没有该纪录,则返回相关的下级的

域名服务器的地址。

第五步：重复第四步,直到找到正确的纪录。

第六步：本地域名服务器把返回的结果保存到缓存,以备下一次使用,同时还

将结果返回给客户机。

## 40.DNS的工作原理？

答案：域名解析有正向解析和反向解析之说，正向解析就是将域名转换成对应的IP

地址的过程，它应用于在浏览器地址栏中输入网站域名时的情形；而反向解析是

将IP 地址转换成对应域名的过程，但在访问网站时无须进行反向解析，即使在

浏览器地址栏中输入的是网站服务器IP 地址，因为互联网主机的定位本身就是

通过IP 地址进行的，只是在同一IP 地址下映射多个域名时需要。另外反向解析

经常被一些后台程序使用，用户看不到。

除了正向、反向解析之外，还有一种称为“递归查询”的解析。“递归查询”

的基本含义就是在某个DNS服务器上查找不到相应的域名与IP地址对应关系时，

自动转到另外一台DNS 服务器上进行查询。通常递归到的另一台DNS 服务器对

应域的根DNS 服务器。因为对于提供互联网域名解析的互联网服务商，无论从

性能上，还是从安全上来说，都不可能只有一台DNS 服务器，而是由一台或者

两台根DNS 服务器（两台根DNS 服务器通常是镜像关系），然后再在下面配置

了多台子DNS 服务器来均衡负载的（各子DNS 服务器都是从根DNS 服务器中

复制查询信息的），根DNS 服务器一般不接受用户的直接查询，只接受子DNS

服务器的递归查询，以确保整个域名服务器系统的可用性。

当用户访问某网站时，在输入了网站网址（其实就包括了域名）后，首先就

有一台首选子DNS 服务器进行解析，如果在它的域名和IP 地址映射表中查询到

相应的网站的IP 地址，则立即可以访问，如果在当前子DNS 服务器上没有查找

到相应域名所对应的IP 地址，它就会自动把查询请求转到根DNS 服务器上进行

查询。如果是相应域名服务商的域名，在根DNS 服务器中是肯定可以查询到相

应域名IP 地址的，如果访问的不是相应域名服务商域名下的网站，则会把相应

查询转到对应域名服务商的域名服务器上。

**41. NTP**的工作模式？

答案：

设备可以采用多种NTP 工作模式进行时间同步：

客户端/服务端模式

对等体模式

广播模式

组播模式

# Shell

## 1 自定义Shell变量时，变量名有什么规则？

参考答案

可以包括数字、字母、下划线，不能以数字开头

变量名区分大小写

赋值时等号两边不要有空格

尽量不要使用关键字和特殊字符

给同一个变量多次赋值时，最后一次的赋值生效

## 2 简述预定义变量$$、$?、$0、$#、$\*、$!的作用。

参考答案

$$ 保存当前运行进程的（PID）号

$? 保存命令执行结果的（返回状态）

$0 保存当前运行的（进程名）或（脚本名）

$# 保存位置变量的（个数）

$\* 保存所有位置变量的（值）

$! 保存后台（最后一个进程）的PID号

## 3 简述三种定界符在变量赋值操作中的特点。

参考答案

双引号" "：允许扩展，以$ 引用其他变量

单引号' '：禁用扩展，即便$ 也视为普通字符

反撇号` `：将命令的执行输出作为变量值

## 4 列出常见的整数值比较操作，并说明各自作用。

参考答案

-eq 等于（Equal）

-ne 不等于（Not Equal）

-ge 大于或等于（Greater or Equal）

-le 小于或等于（Lesser or Equal）

-gt 大于（Greater Than）

-lt 小于（Lesser Than）

## 5 简述Shell环境常见的中断及退出控制指令。

参考答案

break：跳出当前所在的循环体，执行循环体后的语句。

continue:跳过循环体内余下的语句，重新判断条件以便执行下一次循环。

exit:退出脚本，默认返回值是0。

return:用在函数里指定返回值。

shift:用于迁移位置变量，将$1~$9 依次向左顺序移动。

## 6 正则表达式中的+、？、\*分别表示什么含义？

参考答案

这三个字符用来限制关键词的匹配次数，含义分别如下：

+：最少匹配一次，比如a+可匹配a、aa、aaa等

？：最多匹配一次，比如a?可匹配零个或一个a

\*：匹配任意多次，比如a\*可匹配零个或任意多个连续的a

## 7 简述awk工具常用的内置变量、各自的作用。

参考答案

FS：保存或设置字段分隔符

$n：即$1、$2、$3……，表示指定分隔的第几个字段

$0：保存当前读入的整行文本内容

NF：记录当前处理行的字段个数（列数）

NR：记录当前已读入行的数量（行数）

FNR：保存当前处理行在原文本内的序号（行号）

FILENAME：保存awk 当前处理的（文件名）

ENVIRON：调用Shell环境变量，格式：ENVIRON["变量名"]

## 8, 什么是shell？如何查看当前系统支持的Shell?

答案：

1） 实现某种功能的，有执行权限的文件2）cat /etc/shells

## 9，如何切换当前使用的shell

答案：bash

## 10、/bin/bash特性有哪些

答案：特性：提供命令补全，命令编辑和命令历史表等功能

## 11、用户配置文件是哪几个?有什么用？

答案：

1）~/.bashrc ~/.bash\_profile

可以在里面定义变量，用户每打开一个终端时加载的文件，只针对用户有效

## 12、系统配置文件是哪几个？有什么用？

/etc/profile /etc/bashrc

可以在里面定义变量，用户每打开一个终端时加载的文件，针对所有用户生效

## 13、shell变量类型有哪些？列举出常用的4个预定义变量

1）1、自定义变量2、系统环境变量3、预定义变量4、位置变量

2）$? $# $\* $$

## 14、自定义变量的命名规则？

1、可以用数字字每下载线，但不能用数字开头和纯数字

2、同一个变量赋两个值，最后一个值生效

3、给变量赋值时，两边不能有空格

4、区分大小写

## 15、变量的生命周期，和作用范围？

1）在脚本里定义的变量，只在脚本执行过程中有效

2) 默认情况下只在当前Shell里可以使用，要想定义的Shell在所有的Shell里被使用，要把变量定义为全局变量

## 16、脚本的执行过程？脚本的执行方式？

1）从左到右从上到下

2) sh xx.sh bash xx.sh /xx/xx/sh ./xx.sh

## 17、编写脚本的步骤？

1、明确脚本要实现的功能

2、需要使用哪些命令

3、需要使用哪些流程控制

4、数据是变化的，就要用变量来表示

## 18、Shell条件判断类型？

1、文件状态

2、数值比较

3、字符比较

4、逻辑比较

## 19、eval在shell中有什么作用？请举个例子说明？

作用：

#!/bin/bash

aa=h1

bb=h2

var=(aa bb)

for vas in ${var[@]}

do

echo $vas

eval var\_temp=\$${vas}

echo $var\_temp

done

## 20、dirname有什么作用？请举个例子说明？

作用：获取当前脚本路径

例子：

#!/bin/bash

cd `dirname $0`

pwd;ls

## 21、ssh -o stricthostkeychecking=no -o ConnectTimeout=60 分别代表什么意思？

ssh加接时不需要输入key检查，然后六十秒为超时时间

## 22、说一下-n -z -d -f -e -r -w -x -l !-z在shell中分别代表什么意思？-n和-z试举一个例子说明

-n 非空为真

-z 字符串为空为真

-d 是目录且存在为真

-f 是普通文件且存在为真

-e 存在为真

-r 可读为真

-w 可写为真

-x 可执行为真

-l 是链接为真

!-z不为空

1）-n例子：

JavaApp=($(ps aux | grep "java" | grep "/app/guaji"))

if [ -n "${JavaApp[0]}" ];then

echo -e "\033[1;31m 脚本退出\033[0m"

exit 1

fi

2）-z例子：

ssh=$(ssh -o StrictHostKeyChecking=no $2 "ls /")

if [[ -z "$ssh" ]];then

echo -e "\033[1;31m \033[5m 远程主机($2)无法连接,脚本退出. \033[0m"

exit 1

fi

## 23、正则表达式的"|"、"\n"、"\r"、"\t"分别代表什么意思

|表示或的意思

\n表示换行，将当前位移置下行开头

\r回车，将当前位置移至本行开头

## 24、写出获取公网IP的两种方法

ifconfig | grep -Po "(?<=addr:).\*(?=Bcast)" | egrep -v '^192.168|^172.1[6-9].|^172.2[0-9].|^172.3[0-1].|^10.|^127.'

/sbin/ifconfig | awk -F'[ :]+' '/inet addr:/ {print $4}' | egrep -v '^192.168|^172.1[6-9].|^172.2[0-9].|^172.3[0-1].|^10.|^127.'

## 25、$$表示什么意思？

获取当前执行脚本的进程名

## 26、函数内的local是什么意思?举一脚本例子说明

脚本中局部变量，存在于脚本函数(function)中的变量称为局部变量，要以local方式进行声明，使之只在本函数作用域内有效，

防止变量在函中的命名与变量外部程序中变量重名造成程序异常，下面是一脚本例子：

#!/bin/sh

a() {

local s=1

echo $s

}

b() {

s=2

echo $s

}

s=0

a

echo $s

b

echo $s

## 27、$@和$\*的区别

$@将命令行每个参数视为单独的字符串，等同于"$1"、"$2"、"$3"

$\*将所有的命令行所有参数视为单个字符串，等同于"$1$2$3"

## 28、$0、dirname和basename有什么作用？具个例子说明？

作用：

dirname获取脚本路径名

basename获取脚本名

$0获取脚本路径和脚本名

例子：

#!/bin/basha

echo "####################"

echo "# this is '$ 0' test#"

echo "####################"

echo $0

echo

echo "#########################"

echo "# this is 'dirname' test#"

echo "#####################@@@#"

cd `dirname $0` && pwd

echo

echo "##########################"

echo "# this is 'basename' test#"

echo "##########################"

echo `basename $0`

## 29、取出3306端口号这个数字

netstat -tlnp| grep 3306 | awk '[ :]+' '{print $5}' #[ :]+ 以空格和点为分隔符，这种分隔符有一个或多个

## 30、shell中单引号和双引号与不加与号分别代表什么意思

单引号：可以说是所见即所得，即将单号引号的内容原样输出

双引号：把双引号的内容输出出来，如果内容中有命令、变量等，会先把变量、命令解析出结果，然后再输出最终内容来

无引号：把内容输出出来，会将含有空格的字符串视为一个整体输出，如果内容中有命令、变量等，会先把变量、命令解析出结果，

然后再输出内容来，如果字符串中带有空格等特殊字符，则不能完整的输出，需要改加双引号，一般连续的字符串，数字

路径等可以不加任何引号，不过最好用双引号替代之

## 31、echo -n 是什么意思？举一脚本例子显示他的功能

-n不换行

#!/bin/bash

. /etc/init.d/functions

echo "---------Please wait while we are checking-------------"

echo -n "6秒后执行该操作."

for ((i=0;i<6;i++))

do

echo -n ".";sleep 2

#[ $i -eq 3 ] && break

done

echo

action "test success" /bin/true

## 32、echo -e "\n" | nohup ping www.baidu.com > filename 2>&1 &这里的-e 和"\n" 是什么意思？

-e是代表后面输入的内容包含特珠字符需要加的参数

\n 是代表换行

## 33、有1-9的数字，echo输出1-9的数字时，屏蔽0-5的数字再输出

echo '1234567890' | sed 's/[0-5]//g'

## 34、用nohup把一个脚本放在后台运行

nohup sh test.sh > filename 2>&1 &

## 35、用seq打印10以空格分隔，用seq坚着打印10到1

seq -s " " 10

seq 10 -1 1

## 36、curl -I -s www.baidu.com | head -1 | wc -l 中的-I和-s代表什么意思

-s 沉默或安静模式。不显示进度表或错误消息。使卷曲静音

-I 只读取HTTP头！HTTP的服务器功能命令HEAD此用来获取

--connetct-timeout 2 2秒连接超时

## 37、wget -T 10 -c -q --spider www.baidu.com 这些参数分别代表什么意思？

-T 超时10少

-c 断点续传

-q 为执行命令时屏蔽他打印输出的意思，执行命令不会任何内容出来

--spider wget命令加spider参数不会下载任何东西，spider的主要作用是测试下载链接。

tries

## 38、生产环境常用的监控web的方法是哪种

用wget或curl的方法作监控

## 39、生产环境写脚本报错就发邮件的命令是怎么样的

mail -s "uname -n 's httpd status is on" 123456@qq.com < $logfile

## 40、给文件改名

mv $file 1linux-`echo $file | cut -d "-" -f2`

ls \*.jpg | awk -F '\_finished' '{print "mv " " $0" "$1".jpg"}' | bash

## 41、查看当前目录的所有文件夹

ls -F |grep /

## 42、awk中的NF代表什么意思？

NF代表结尾的意思

## 43、shell上: 0、1>、2>、>、2>&1、&>/dev/null分别代表什么意思

0表示标准输入

1>表示标准输出

2>表示标准错误输出

> 默认为标准输出重定向，与1> 相同

2>&1 意思是把标准错误输出重定向到标准输出.

&>/dev/null 意思是把标准输出和标准错误输出都重定向到空

# Mysql

## 100、 MySQL数据库的服务进程叫什么名字？监听端口是多少？默认数据库目录是？

**参考答案**

服务进程名是mysqld；监听端口是3306；默认数据库目录为 /var/lib/mysql。

## 1 主流数据库服务软件有哪些？开源且跨平台的数据库软件有哪些？

参考答案

主流数据库服务软件有：

甲骨文公司Oracle

IBM DB2

微软SQL Server

美国Sybase公司Sybase

加州大学伯克利分校计算机系开发的PostgreSQL

开源且跨平台的数据库软件有：

MySQL、PostgreSQL：开源且跨平台

Oracle、DB2：跨平台不开源

SQL Server：不跨平台不开源

Sybase：跨平台不开源

## 2 MySQL数据库的服务进程叫什么名字？监听端口是多少？默认数据库目录是？

参考答案

服务进程名是mysqld；监听端口是3306；默认数据库目录为/var/lib/mysql。

## 3 MySQL默认的3个库叫什么名字？哪个库里的数据不占用物理磁盘空间？

参考答案

3个默认库：mysql、test 和information\_schema。

其中，information\_schema库的数据不占用磁盘空间，仅保存在内存里。

## 4 请列出MySQL常用的数据类型，并写出定义这些数据类型所使用的关键字。

参考答案

MySQL常用的数据类型：

数值类型：所用关键字为int、float

字符类型：所用关键字为char、varchar

日期时间类型：所用关键字为year、time、datetime

枚举类型：所用关键字为set、enum

## 5 简述索引的优点与缺点，默认情况下哪个文件保存表的索引信息？

参考答案

索引的优点与缺点如下：

索引就像一本书的目录

加快查询记录的速度

会降低插入、更新记录的速度

默认情况下“表名.MYI”文件保存表的索引信息

## 6 简述在表中创建外键字段要满足那些条件？

参考答案

在表中创建外键字段要满足以下条件：

表必须都使用innodb存储引擎

表中外键字段的类型要匹配

被参照字段要有明确的索引

## 7 简述MySQL体系结构的组成，并描述每个组成部分的作用。

参考答案

主要包括8个部分：

连接池：进程数限制、内存检查、缓存检查等。

SQL接口：用户通过sql客户端发过来的命令，由sql接口接收，sql操作(DML数据操作语言：查询、修改、升级数据等；DDL数据定义语言：创建一个新的数据库、新的索引、删除一个用户等；存储过程、视图触发器。

分析器：分析查询语句事务处理对象访问权限。

优化器：优化访问路径、生成执行树。

缓存和缓冲：保存sql查询结果。

存储引擎：用于管理存储的文件系统，将逻辑结构转换为物理结构的程序；不同的存储引擎有不同的功能和存储方式。

管理工具：备份，恢复，安全，移植，集群等，这些工具一般和文件系统打交道，不需要和mysql-server打交道，它们对应的都是命令。

物理存储设备(文件系统)。

## 8 简述MySQL数据库访问的执行过程。

参考答案

1）客户端发出请求。

2）服务器端开辟线程响应客户端请求。

3）客户端发起sql语句查询数据库。

4）查询缓存：记录用户的sql查询语句，如果查询内容相同，直接从查询缓存回复。

5）如果缓存没有进入分析器。

6）分析器：分析用户命令语法是否正确，将用户的命令进行切片，一个词一个词用空格隔开，获得用户要查询的表、内容、用户的权限等。

7）优化器：执行路径的选择，生成执行树。（每个SQL语句都有很多执行路径，优化的目的就是在这些执行路径里选择最优的执行路径）。

8）存储引擎：用于管理存储的文件系统，不同的存储引擎有不同的功能和存储方式。

## 9 简述MySQL数据库中插入、更新、查询、删除表记录的指令格式。

连接到MySQL数据库服务器，练习以下表记录操作：

向表中插入记录的语法格式

更新表记录的语法格式

查询表记录的语法格式

删除表记录的语法格式

参考答案

1）向表中插入记录的语法格式

insert （into）表名（字段名列表）values(字段名=值，字段名=值，…);

2）更新表记录的语法格式

update 表名（set）（字段名=值，字段名=值，…）where（条件表达式列表）；

3）查询表记录的语法格式

select （字段名列表）（from）表名（where）条件表达式列表；

4）删除表记录的语法格式

delete （from）表名（where）（条件表达式列表）；

## 10 简述用户授权命令的语法格式。

参考答案

grant 权限列表on 数据库to 用户名@“客户端地址”

identified by “密码”with grant option;

## 11 在MySQL-MMM集群中有几种角色，各自的功能是什么？

参考答案

共3种角色：客户端、monitor节点（管理节点）、agent节点（数据库节点）

客户端：访问集群

管理节点：负责所有的监控工作的监控守护进程，决定故障节点的移除或恢复

数据库节点：运行在MySQL服务器上的代理守护进程，提供简单远程服务集、提供给监控节点（可用来更改只读模式、复制的主服务器等）

## 12 在MySQL-MMM集群中可以有多少台主数据库服务器、多少台从数据库服务器？

参考答案

在MySQL-MMM环境中主数据库有且只能有2台，从数据库理论上可以任意多台。

## 13 在MySQL-MMM集群中均衡模式和排他模式的作用是？

参考答案

均衡模式一般用于从数据库，可实现多个虚拟IP地址。

排他模式一般用于主数据库，只可设置一个虚拟IP地址。

## 14,简述mysqldump备份数据时数据库名的表示方式。

参考答案

--all-databases 所有库

数据库名指定单个库

数据库名.表名指定库里的指定表

-B 数据1 数据库2 备份多个库

## 15 什么是MySQL集群？

答案：MySQL 集群是一个无共享的（shared-nothing），分布式节点架构的存储方案，其目的是提供容错性和高性能。数据在单个数据节点（有时也称存储节点）上存储和复制，每个数据节点运行在独立的服务器上并维护数据的一份拷贝。每个集群还有管理节点。数据更新使用读已提交隔离级别（read-committed isolation）来保证所有节点数据的一致性，使用两阶段提交机制（two-phased commit）保证所有节点都有相同的数据（如果任何一个写操作失败，则更新失败）。

MySQL 集群的最初实现将所有信息都保存在主存内，没有任何永久性存储。后来MySQL 集群允许数据存储在磁

盘上。通过存储引擎层MySQL 服务器作为查询引擎，可以使MySQL 集群的性能达到最佳。这样就可以将MySQL 应用透明地迁移到MySQL 集群中去。

无共享的对等节点使得某台服务器上的更新操作在其他服务器上立即可见。传播更新使用一种复杂的通信机制，这一机制专用来提供跨网络的高吞吐量。该架构通过多个MySQL服务器分配负载，从而最大程度地达到高性能，通过在不同位置存储数据保证高可用性和冗余。

## 16，MySQL集群和MySQL 有和不同？

答案：你可能会问：“集群和复制之间有什么区别那？” 集群的定义很多，通常认为集群包含成员、消息、冗余和自动故障转移等功能，而复制仅仅是一个服务器向别一个服务器发送消息（数据）的方式。我们先讨论集群内部的复制（又称本地复制）。

## 17 MySQL 集群的特点？

答案：为了实现最高性能。高可用性和冗余等目标。数据在集群内部的对等数据节点之间互相复制。数据复制采用同步机制，每个数据节点到所有其他数据节点上，数据在多个数据节点上存储。

## 18 MySQL 集群有一些创建高可用性系统的专用功能，主要包括？

答案：节点回复、日志、检查点、系统恢复、热备份恢复、无单点故障、故障转移、分区、联机操作

## 19 MySQL中myisam与innodb的区别，至少5点

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 【评析】将Mysql常见的存储引擎的特点归纳表格如下 点 | myisam | innodb | memory | archive |
| 存储限制 | 256TB | 64TB | 有 | 无 |
| 事物安全 | 不 | 支持 | 不 | 不 |
| 支持索引 | 支持 | 支持 | 支持 | 不支持 |
| 锁颗粒（锁力度） | 表锁 | 行锁（没有索引的情况是表锁） | 表锁 | 行锁 |
| 数据压缩 | 支持 | 不支持 | 支持 | 不支持 |
|  |  |  |  |  |
|  |  |  |  |  |

## 20什么是读写分离？

MySQL Proxy最强大的一项功能是实现“读写分离(Read/Write Splitting)”。基本的原理是让主数据库处理事务性查询，而从数据库处理SELECT查询。数据库复制被用来把事务性查询导致的变更同步到集群中的从数据库。当然，主服务器也可以提供查询服务。使用读写分离最大的作用无非是环境服务器压力。

## 21读写分离的好处

1.增加冗余

2.增加了机器的处理能力

3.对于读操作为主的应用，使用读写分离是最好的场景，因为可以确保写的服务器压力更小，而读又可以接受点时间上的延迟。

## 22 读写分离提高性能之原因

1.物理服务器增加，负荷增加

2.主从只负责各自的写和读，极大程度的缓解X锁和S锁争用

3.从库可配置myisam引擎，提升查询性能以及节约系统开销

4.从库同步主库的数据和主库直接写还是有区别的，通过主库发送来的binlog恢复数据，但是，最重要区别在于主库向从库发送binlog是异步的，从库恢复数据也是异步的

5.读写分离适用与读远大于写的场景，如果只有一台服务器，当select很多时，update和delete会被这些select访问中的数据堵塞，等待select结束，并发性能不高。对于写和读比例相近的应用，应该部署双主相互复制

6.可以在从库启动是增加一些参数来提高其读的性能，例如--skip-innodb、--skip-bdb、--low-priority-updates以及--delay-key-write=ALL。当然这些设置也是需要根据具体业务需求来定得，不一定能用上

7.分摊读取。假如我们有1主3从，不考虑上述1中提到的从库单方面设置，假设现在1分钟内有10条写入，150条读取。那么，1主3从相当于共计40条写入，而读取总数没变，因此平均下来每台服务器承担了10条写入和50条读取（主库不承担读取操作）。因此，虽然写入没变，但是读取大大分摊了，提高了系统性能。另外，当读取被分摊后，又间接提高了写入的性能。所以，总体性能提高了，说白了就是拿机器和带宽换性能。MySQL官方文档中有相关演算公式：官方文档见6.9FAQ之“MySQL复制能够何时和多大程度提高系统性能”

8.MySQL复制另外一大功能是增加冗余，提高可用性，当一台数据库服务器宕机后能通过调整另外一台从库来以最快的速度恢复服务，因此不能光看性能，也就是说1主1从也是可以的。

## 23 varchar与char的区别；varchar(50)中50的涵义；int(20)中20的涵义；

char是定长变量，varchar是变长变量。varchar(50)表示这一行的变量最大的存储字节是50个字节，int(20)同理。

【评析】假设有一行是name char(8),如果有一个数据是叫AAA，那么它仅仅只有三个字节被存储进去，但是依旧存储了8个字节，多余的5个字节空着也就空着了。而是name varchar(8),同样是AAA，由于是变长，所以只保存了3个字节，剩下5个字节是弹性的，有就用，没有就不用。

在读取方面，char的读取速度要比varchar快，也就是常说的“用读取换容量”，但是还是多用varchar，当数据库内容成万上亿的时候，节省的容量是非常非常可观的。

## 24 计划，mysqldump以及xtranbackup的实现原理；备份恢复时间；备份恢复失败如何处理。

mysqldump是采用sql级别的备份机制，将数据表导成sql脚本文件，在不用的mysql版本之间升级时相对比较合适。

xtranbackup是innodb的hotbackup工具，xtrbackup在启动的时候会复制所有的数据文件，同时会启动一个后台进程，用于监视事务日志，并且从事务日志复制最新的修改。所以xtrbackup在启动的开始，就不懂的将事务日志的每个数据文件的修改都记录下来。

mysqldump的备份和恢复时间都很慢，任何数据的更新和变化都会被挂起。

xtrabackup的恢复时间比mysqldump快一点，但是会锁表。

备份恢复失败的话，其实原因很多，主要可能就是参数设置的不对，检查一下参数。

【评析】使用mysqldump备份数据表的命令，在shell下执行：

mysqldump -u用户名-p密码（可以直接-p）-h主机名--databases 数据库名> 要备份的文件路径

mysqldump -u用户名-p密码-h主机名--all-databases >要备份的文件路径

mysqldump -u用户名-p密码-h主机名--no-data 数据库名>要备份的文件路径

这里并不全，另写文章专门补充。

## 25 MySQL中InnoDB引擎的行锁是通过加在什么上完成(或称实现)的？为什么是这样子的？

InnoDB的行锁是通过加在索引上实现的，为什么这么设计，我也不知道，去问mysql的设计公司。

## 26 MySQL 数据库备份方式

增量备份、差异备份、完整备份

## 27 MySQL主从复制原理？

答案：

分为同步复制和异步复制，实际复制架构中大部分为异步复制。

复制的基本过程如下：

1)、Slave上面的IO进程连接上Master，并请求从指定日志文件的指定位置（或者从最开始的日志）之后的日志内容；

2)、Master接收到来自Slave的IO进程的请求后，通过负责复制的IO进程根据请求信息读取制定日志指定位置之后的日志信息，返回给Slave 的IO进程。返回信息中除了日志所包含的信息之外，还包括本次返回的信息已经到Master端的bin-log文件的名称以及bin-log的位置；

3)、Slave的IO进程接收到信息后，将接收到的日志内容依次添加到Slave端的relay-log文件的最末端，并将读取到的Master端的bin-log的文件名和位置记录到master-info文件中，以便在下一次读取的时候能够清楚的告诉Master“我需要从某个bin-log的哪个位置开始往后的日志内容，请发给我”；

4)、Slave的Sql进程检测到relay-log中新增加了内容后，会马上解析relay-log的内容成为在Master端真实执行时候的那些可执行的内容，并在自身执行。

Mysql为了解决这个风险并提高复制的性能，将Slave端的复制改为两个进程来完成。提出这个改进方案的人是Yahoo!的一位工程师“Jeremy Zawodny”。这样既解决了性能问题，又缩短了异步的延时时间，同时也减少了可能存在的数据丢失量。当然，即使是换成了现在这样两个线程处理以后，同样也还是存在slave数据延时以及数据丢失的可能性的，毕竟这个复制是异步的。只要数据的更改不是在一个事物中，这些问题都是会存在的。如果要完全避免这些问题，就只能用mysql的cluster来解决了。不过mysql的cluster是内存数据库的解决方案，需要将所有数据都load到内存中，这样就对内存的要求就非常大了，对于一般的应用来说可实施性不是太大。

复制常用架构

Mysql复制环境90%以上都是一个Master带一个或者多个Slave的架构模式，主要用于读压力比较大的应用的数据库端廉价扩展解决方案。因为只要master和slave的压力不是太大（尤其是slave端压力）的话，异步复制的延时一般都很少很少。尤其是自slave端的复制方式改成两个进程处理之后，更是减小了slave端的延时。而带来的效益是，对于数据实时性要求不是特别的敏感度的应用，只需要通过廉价的pc server来扩展slave的数量，将读压力分散到多台slave的机器上面，即可解决数据库端的读压力瓶颈。这在很大程度上解决了目前很多中小型网站的数据库压力瓶颈问题，甚至有些大型网站也在使用类似方案解决数据库瓶颈。

## 28 mysql-mmm简介

答案：

MMM(Master-Master replication manager for Mysql) 是一套灵活的脚本程序，用来

对mysql replication 进行监控和故障迁移，并能管理mysql Master-Master 复制的配置

( 同一时间只有一个节点是可写的) 。附带的工具套件可以实现多个slaves 的read 负载均衡，

因此你可以使用这个工具移除一组服务器中复制延迟较高的服务器的虚拟IP ，它还可以备

份数据，两节点之间再同步等等。

Mysql-mmm 是一套脚本程序，基于perl 实现，通过不同的perl 脚本实现对mysql 服

务器的管理与维护。它仅仅是一个管理程序，自己本身并不提供mysql 服务功能。

被管理的mysql server 机需要安装相关的agent 脚本，mysql-mmm 的监控端可以监

管所以安装过此脚本的mysql server 。

当出现多台可写mysql server 时，mmm 可以保证在同一时间点只使用一台mysql

server 进行写入操作，以保证数据有效性，防止写入冲突。所以它并不适用于有大并发写入

要求的生产环境。相反，当有多台可读mysql server 存在时，它可以通过一些其他软件的

配合，实现负载均衡方式的读取，大大提高mysql server 的读性能。

在运行过程中，如果某一台mysql server 处于不可用状态时，mmm 可以将原有操作

请求迁移至其他可用mysql ，从而实现服务的高可用性。包括写请求迁移，读请求迁移，主

从同步的master 迁移。

Mysql-mmm 同时也提供了一套很好用的运维管理工具，可以实现简单快捷的数据备份与

维护。简化管理员的日常维护成本。

## 29 mysql-mmm 组成与原理

答案：

Mysql-mmm 的管理功能主要通过三个脚本来实现

mmm\_mond

监控进程，负责所有的监控工作，决定和处理所有节点角色活动。此脚本需要在监管

机上运行。

mmm\_agentd

运行在每个mysql 服务器上的代理进程，完成监控的探针工作和执行简单的远端服务

设置。此脚本需要在被监管机上运行。

mmm\_control

一个简单的脚本，提供管理mmm\_mond 进程的命令

mysql-mmm 的监管端会提供多个虚拟IP （VIP ），包括一个可写VIP ，多个可读

VIP ，通过监管的管理，这些IP 会绑定在可用mysql 之上，当某一台mysql 宕机时，监管

机会将VIP 迁移至其他mysql 。

在整个监管过程中，需要在mysql 中添加相关授权用户，以便让mysql 可以支持监理

机的维护。授权的用户包括一个mmm\_monitor 用户和一个mmm\_agent 用户，如果想使

用mmm 的备份工具则还要添加一个mmm\_tools 用户。

## 30 多源复制下，支持master是5.6，slave是5.7吗？

答：可以的

【老叶补充】非常不建议跨大版本的MySQL Replication。

## 31 半同步复制设置N个slave应答，如果当前Slave小于N会怎样？

答：取决于rpl\_semi\_sync\_master\_wait\_no\_slave的设置。

-rpl\_semi\_sync\_master\_wait\_no\_slave = 0

会立刻变成异步复制。

-rpl\_semi\_sync\_master\_wait\_no\_slave = 1

仍然等待应答，直到超时。

## 32 gtid 如果出现不支持的语句，怎么解决

答：从应用中去掉不支持的语句/事务：

例如：

-CREATE TABLE ... SELECT

可以该为:

CREATE TABLE

INSERT ... SELECT

## 33 基于GTID的复制，可以指定GTID复制的起始位置么，还是只能根据现有的信息？

答：GTID复制就是为了摆脱对binlog文件名和位置的依赖。所以不能指定复制的起始位置，也完全没有必要指定。

## 34 对一个已经开启GTID的数据库再做一个从库，先把Master备份下来还原到新slave上去，直接可以同步了还是先需要做purge\_gtid的操作再同步呢？

答：需要设置gtid\_purged。整个过程可以通过mysqldump完成。

请参考手册：http://dev.mysql.com/doc/refman/5.7/en/replication-gtids-failover.html#replication-gtids-failover-copy

## 35 线上全是5.5的环境，有没有办法搭建5.5到5.7的复制？

答：可以，但不能开启gtid功能。

【老叶补充】非常不建议跨大版本的MySQL Replication，更何况是垮了2个大版本，最好是先进行升级。

## 36 并行复制logical\_clock，如果不开启gtid是不是就不能并行了？

答：不开启gtid,也能使用logical\_clock并行复制。

## 37 在主从复制过程中，是主向从推数据还是从拉数据，如果这个传送的过程中，出现网络闪断，会不会造成数据包丢失，会执行校验重传嘛？

答：Slave 的IO线程发起到Master的连接。

然后master开始发送events,slave只是被动的接收。

slave和master之间使用的是tcp 连接。tcp是可靠的连接。网络丢包等都是tcp层自动处理的。

mysql不需要处理。

如果slave长时间不能收到一个完整的Event，或者接收event时出错。slave

会进行相应的处理。

如果slave认为，重新建立连接能解决问题。slave则自动的断开原来的连接，然后重新连接到master去。

如果slave认为，这个错误无法自动解决，slave会停掉io线程，并报错。

## 38 设置了binlog\_group\_commit\_sync\_delay参数，在宕机的时候应该不会影响binglog文件安全吧？

答：不影响

## 39 多源复制是只能在异步模式下使用么？因为半同步的状态是全局的，一个通道关闭会导致其它通道出错，有没有考虑将半同步状态改成每个channel的私有配置呢？

答：只有一个通道可以开启seimsync，其他的都要使用异步通道。不光是Semisync，异步通道的状态也要改成每个channel的私有配置，都有考虑。

# OPERATION

## 1 简述Squid的优缺点有哪些

参考答案

优势：

通过缓存增加访问速度；

提高网络的安全性；

Squid历史悠久，技术积淀深厚，同时无需支付任何费用。

缺点：

性能不足，借助于windows、linux等通用操作系统才能实现上网加速等功能。

## 2 简述常见Web服务器软件有哪些

参考答案

Apache、Nginx、Lighttpd 、Tomcat、IBM WebSphere、IIS。

## 3 简述什么是LNMP

参考答案

LNMP是网站运行平台。

L：操作系统（Linux）

N：网站服务软件（Nginx）

M：数据库服务软件（MySQL）

P：网站开发语言（PHP、perl、python）

## 4 地址重写的好处

参考答案

缩短URL，隐藏实际路径提高安全性；

易于用户记忆和键入；

易于被搜索引擎收录。

## 5 简述什么是memcached

参考答案

memcached是高性能的分布式缓存服务器，是一个跨平台的、开源的实现分布式缓存服务的软件

用来集中缓存数据库查询结果，减少数据库访问次数，以提高动态Web应用的响应速度

memcached支持许多平台：Linux、FreeBSD、Solaris (memcached 1.2.5以上版本)、Mac OS X、Windows

2 简述memcached什么情况下会删除缓存数据

参考答案

当分配的存储空间存满时，有新数据需要存储时，删除最近最少使用的数据。腾出空间存储新数据；

重新启动memcached服务会删除缓存数据；

运行memcached服务的操作系统重启后会删除缓存数据。

## 6 部署实施CDN的优势是什么

参考答案

本地Cache加速，提升访问速度和稳定性

网站镜像，消除不同地区、运营商网络互连的问题

智能DNS解析，自动选择最快的Cache服务器

负载优化，减轻后端源Web服务器的压力负载

集群抗攻击，有效降低DDOS攻击的影响

## 6 Nginx 的优点?

答案：

（1） 它可以高并发连接：官方测试连接数（5万）实际生产环境中可支撑（2~4万）

（2） 内存消耗少

（3） 成本低廉

（4） 其他理由（配置文件非常简单，支持Rewrite重写规则）

（5） 内置的健康检查功能

（6） 节省宽带（支持GZIP压缩，可以添加浏览器本地缓存的Header 头）

（7） 稳定性高

（8） 支持热部署

## 7 .Nginx和Apache的综合对比？weB服务器

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 反向代理 | 非常好 | 好 |
| Rewrite规则 | 非常好 | 好 |
| FastCGI | 好 | 差 |
| 热部署 | 支持 | 不支持 |
| 系统压力比较 | 很小 | 小 |
| 稳定性 | 非常好 | 好 |
| 安全性 | 一般 | 好 |
| 技术资料 | 很少 | 非常多 |
| 静态文件处理 | 非常好 | 一般 |
| 虚拟主机 | 支持 | 支持 |
| 内存消耗 | 非常小 | 很大 |

## 8，什么是CDN？

答案：CDN的全称是内容分发网络。其目的是通过在现有的Internet中增加一层新的网络架构，将网站的内容发布到最接近用户的网络“边缘”，使用户可以就近取得所需的内容，提高用户访问网站的响应速度。CDN有别于镜像，因为它比镜像更智能，或者可以做这样一个比喻：CDN=更智能的镜像+缓存+流量导流。因而，CDN可以明显提高Internet网络中信息流动的效率。从技术上全面解决由于网络带宽小、用户访问量大、网点分布不均等问题，提高用户访问网站的响应速度。

## 9，CDN的类型特点？

答案：CDN的实现分为三类：镜像、高速缓存、专线。

（1）镜像站点（Mirror Site）:是最常见的，它让内容直接发布，适用于静态和准动态的数据同步。但是购买和维护新服务器的费用较高还必须在各个地区设置镜像服务器，配备专业技术人员进行管理与维护。对于大型网站来说，更新所用的带宽成本也大大提高了。

（2）高速缓存:成本较低，适用于静态内容。Internet的统计表明，超过80%的用户经常访问的是20%的网站的内容，在这个规律下，缓存服务器可以处理大部分客户的静态请求，而原始的服务器只需处理约20%左右的非缓存请求和动态请求，于是大大加快了客户请求的响应时间，并降低了原始服务器的负载。

（3）专线:让用户直接访问数据源，可以实现数据的动态同步。

## 10 CDN的工作原理？

答案：

若是忽略各种缓存，传统的网站访问过程为: 1. 用户在浏览器中输入要访问的域名； 2. 浏览器向域名解析服务器发出解析请求，获得此域名对应的IP地址； 3. 浏览器利用所得到的IP地址，向该IP对应的服务器发出访问请求； 4. 服务器对此响应，将数据回传至用户浏览器端显示出来。 与传统访问方式不同，CDN网络则是在用户和服务器之间增加Cache层，将用户的访问请求引导到Cache节点而不是服务器源站点，要实现这一方式，主要是通过接管DNS实现。

使用CDN缓存后的网站访问过程演变为：

1. 用户在浏览器中输入要访问的域名；

2. 浏览器向域名解析服务器发出解析请求，由于CDN对域名解析过程进行了调整，所以用户端一般得到的是该域名对应的CNAME记录，此时浏览器需要再次对获得的CNAME域名进行解析才能得到缓存服务器实际的IP地址。在此过程中，全局负载均衡DNS解析服务器会根据用户端的源IP地址，如地理位置（深圳还是上海）、接入网类型（电信还是网通）将用户的访问请求定位到离用户路由最短、位置最近、负载最轻的Cache节点（缓存服务器）上，实现就近定位。定位优先原则可按位置、可按路由、也可按负载等等； 3. 再次解析后浏览器得到该域名CDN缓存服务器的实际IP地址，向缓存服务器发出访问请求； 4. 缓存服务器根据浏览器提供的域名，通过Cache内部专用DNS解析得到此域名源服务器的真实IP地址，再由缓存服务器向此真实IP地址提交访问请求； 5. 缓存服务器从真实IP地址得到内容后，一方面在本地进行保存，以备以后使用，同时把得到的数据发送到客户端浏览器，完成访问的响应过程； 6. 用户端得到由缓存服务器传回的数据后显示出来，至此完成整个域名访问过程； 不论是否使用CDN网络，用户客户端设置不需做任何改变，直接使用被加速网站原有域名访问即可。对于要加速的网站，只需修改整个访问过程中的域名解析部分，便能实现透明的网络加速服务。

# SECURITY

## 1 简述信息安全防护的目标和一般原则。

参考答案

信息安全防护的目标：

保密性，Confidentiality

完整性，Integrity

可用性，Usability

可控制性，Controlability

不可否认性，Non-repudiation

信息安全防护的一般原则：

权限最小化：受保护的敏感信息只应在一个有限的可控的小范围内被分享。

分权制衡：所有权限应该适当划分给多个授权主体，达到既相互协作又相互制约、相互监督的效果，避免出现权限垄断

安全隔离：将信息主体与客体分离，通过安全通道对双方之间的访问进行控制

## 2 根据攻击/防护的对象不同，安全工作一般区分为哪些类别？

参考答案

物理安全：各种设备/主机、机房环境

系统安全：主机或设备的操作系统

应用安全：各种网络服务、应用程序

网络安全：对网络访问的控制、防火墙规则

数据安全：信息的备份与恢复、加密解密

管理安全：各种保障性的规范、流程、方法

## 3 简述实现SSH密钥对验证的基本过程。

参考答案

1）用户在客户端生成密钥对；

2）用户将公钥上传至目标服务器；

3）在服务器上将用户上传的公钥导入到指定用户的~/.ssh/authorized\_keys中；

4）客户端连接验证。

## 4 简述RHEL6系统中SELinux机制的三种运行模式。

参考答案

三种运行模式：

ENFORCING，强制模式：发生操作违规会禁止

PERMISSIVE，警告模式：发生操作违规仍然可以继续，但是会写入日志

DISABLED，禁用模式：即关闭，不使用SELinux机制

切换规律：

强制模式切换到禁用模式需要重启系统，反之亦然

而强制和警告模式间的切换会立即生效

## 5 简述向证书颁发机构（CA）申请数字证书的过程。

参考答案

1）在应用服务器上生成私钥

2）利用私钥生成证书请求文件，CSR文件

3）将CSR文件提交至CA

4）CA核实CSR 请求

5）CA签署数字证书

6）CA将签署的数字证书颁发给请求者

7）在应用服务器上部署数字证书

## 6 简述基于Apache HTTP Server实现HTTPS安全通信的部署过程。

参考答案

1）在Web服务器上生成私钥

2）利用私钥生成证书请求文件CSR

3）将CSR文件提交给CA申请证书文件CRT

4）在WEB服务器上将私钥和CRT文件拷贝至指定目录

5）安装mod\_ssl并修改配置文件

## 7 加密的邮件通信协议及端口分别有哪些？

参考答案

SMTP（25）+ TLS/SSL

POP3（110）、POP3S（995）

IMAP（143）、IMAPS（993）

## 8 在网络安全工作中，扫描技术可以达成哪些目标？

参考答案

检测潜在的风险

查找可攻击目标

收集设备/主机/系统/软件信息

发现可利用的安全漏洞

## 9 iptables默认的规则链有哪些，各自的作用是什么？

参考答案

INPUT：处理入站数据包

OUTPUT：处理出站数据包

FORWARD：处理转发的数据包

POSTROUTING：路由选择之后处理

PREROUTING：路由选择之前处理

## 10 iptables处理数据包的基本目标操作有哪些，各自的作用是什么？

参考答案

ACCEPT：允许通过/放行

DROP：直接丢弃，不给出任何回应

REJECT：拒绝通过，必要时会给出提示

LOG：记录日志，然后传给下一条规则

## 11 iptables的filter过滤表包括的默认规则链是哪几个？

参考答案

INPUT：主要与想要进入Linux 本机的数据包有关

OUTPUT：主要与Linux 本机所要送初的数据包有关

FORWARD：与Linux 本机没有关系，它可以传递数据包到后端的计算机中，与NAT 的table 相关性较高

## 12 简述iptables状态跟踪机制所处理的几种数据包类型。

参考答案

NEW，请求建立连接的包、完全陌生的包

ESTABLISHED，将要或已经建立连接的包

RELATED，与已知某个连接相关联的包

INVALID，无对应连接，以及连接无效的包

UNTRACKED，未跟踪状态的包

## 13 简述基于DNAT策略发布私网服务器的工作原理。

参考答案

为只有私网IP地址的服务器在网关上建立DNAT端口映射；当互联网中的客户机访问网关的映射端口时，由网关修改数据包的目标IP地址和端口，改为私网服务器的真实IP地址和端口（从网关可达）；私网服务器提供的响应包根据映射关系原路返回，从而实现了私网服务器的公开化访问。

# MONITOR

## 1 监控描述Nagios与Cacti的区别

参考答案

Cacti：在监控方面绘图比较不错，在流量与图型展现比较存在优势；

Nagios：在故障分析比较不错，报警机制相对来说比较好，报警机制：邮箱、短信等，而且也比Cacti灵活；同时适用监控大量服务器以及服务器上面大批服务状态是否正常，重点不在图形化，而在状态故障的监控。

## 2 简单描述Zabbix具有哪些监控功能

参考答案

具备常见的商业监控软件所具备的功能

主机性能监控、网络设备监控、数据库监控等

支持多种报警机制

支持自动发现网络设备和服务器

可以通过配置自动发现服务器规则来实现

支持分布式，能集中展示、管理分布式的监控点

编写插件容易，可以自定义监控项

具有实时绘图功能

## 3 Nagios的系统特点？

答案：

（1） 监控主机资源和网络服务

（2） 允许用户通过设计实现简单的插件来监控自己特定的服务

（3） 当被监控对象出现问题时，会及时通知管理人员

（4） 事先定义时间处理程序，当对象出现问题时自动调用对应用的处理程序

（5） 通过Web 页面来监视对象状态，警告提示和日志文件。

# CLUSTER

## 1 服务器创建存储技术有哪些？

参考答案

DAS

NAS

SAN

## 2 集群有哪些类别？

参考答案

高性能计算集群HPC：通过以集群开发的并行应用程序，解决复杂的科学问题。

负载均衡（LB）集群：客户端访问负载可以在计算机集群中尽可能平均地分摊处理。

高可用（HA）集群：当集群中的一个系统发生故障时，集群软件迅速做出反应，将该系统的任务分配到集群中其它正在工作的系统上执行。

## 3 LVS的负载平衡方式有哪些？

参考答案

VS/NAT：通过网络地址转换实现的虚拟服务器。Director将用户请求报文的目的地址改成选定的Real Server地址后，转发给Real Server。大并发访问时，调度器的性能成为瓶颈。

VS/DR：直接使用路由技术实现虚拟服务器。通过改写请求报文的MAC地址，将请求发至Real Server，Real Server直接响应客户端。

VS/TUN：通过隧道方式实现虚拟服务器。Director采用隧道技术将请求发至Real Server后，Real Server直接响应客户端。

## 4 写出至少四种LVS负载平衡的调度算法

参考答案

轮询（Round Robin）

加权轮询（Weighted Round Robin）

最少连接（Least Connections）

加权最少连接（Weighted Least Connections ）

基于局部性的最少链接（Locality-Based Least Connections）

带复制的基于局部性最少链接（Locality-Based Least Connections with Replication）

目标地址散列（Destination Hashing）

源地址散列（Source Hashing）

最短的期望的延迟（Shortest Expected Delay Scheduling SED）

最少队列调度（Never Queue Scheduling NQ）

## 5 HAProxy工作模式有哪些？

参考答案

mode http：客户端请求被深度分析后再发往服务器。

mode tcp：在客户端与服务器这间建立全双工会话，不检查第七层信息。

mode health：仅做健康状态检查，已经不建议使用。

2 HTTP Keep-alive事务模型的特点是什么？

参考答案

一次连接可以传输多个请求；

客户端需要知道传输内容的长度，以避免无限期的等待传输结束；

降低两个HTTP事务间的延迟；

需要相对较少的服务器资源。

## 6 HAProxy配置文件有哪些组成部分？

参考答案

default：为后续的其他部分设置缺省参数，缺省参数可以被后续部分重置；

frontend：描述集群接收客户端请求的信息集合；

backend：描述转发链接的后端服务器集合；

listen：把frontend和backend结合到一起的完整声明。

## 7 写出RHCS的核心组件名称？

参考答案

cman（cluster manager）：集群管理器；

rgmanger（Cluster resource group manager）：集群资源管理器；

corosync：集群间通信软件；

rcci：集群远程管理器。

## 8 写出RHCS高可用集群配置流程

参考答案

配置yum服务器和客户端；

设置iSCSI共享存储；

节点上设置iSCSI客户端连接；

关闭node1~3节点上的NetworkManager服务；

节点上安装ricci通信工具；

安装luci Web界面集群管理工具；

通过luci安装集群；

配置fence；

配置apache高可用集群。

## 9 LVS 三种工作模式原理、以及优缺点比较

一、**NAT**模式（**VS-NAT**）

原理：就是把客户端发来的数据包的IP头的目的地址，在负载均衡器上换成其中一台RS的IP地址，并发至此RS来处理,RS处理完成后把数据交给经过负载均衡器,负载均衡器再把数据包的原IP地址改为自己的IP，将目的地址改为客户端IP地址即可｡期间,无论是进来的流量,还是出去的流量,都必须经过负载均衡器｡

优点：集群中的物理服务器可以使用任何支持TCP/IP操作系统，只有负载均衡器需要一个合法的IP地址。

缺点：扩展性有限。当服务器节点（普通PC服务器）增长过多时,负载均衡器将成为整个系统的瓶颈，因为所有的请求包和应答包的流向都经过负载均衡器。当服务器节点过多时，大量的数据包都交汇在负载均衡器那，速度就会变慢！

二、**IP**隧道模式（**VS-TUN**）

原理：首先要知道，互联网上的大多Internet服务的请求包很短小，而应答包通常很大。那么隧道模式就是，把客户端发来的数据包，封装一个新的IP头标记(仅目的IP)发给RS,RS收到后,先把数据包的头解开,还原数据包,处理后,直接返回给客户端,不需要再经过负载均衡器｡注意,由于RS需要对负载均衡器发过来的数据包进行还原,所以说必须支持IPTUNNEL协议｡所以,在RS的内核中,必须编译支持IPTUNNEL这个选项

优点：负载均衡器只负责将请求包分发给后端节点服务器，而RS将应答包直接发给用户。所以，减少了负载均衡器的大量数据流动，负载均衡器不再是系统的瓶颈，就能处理很巨大的请求量，这种方式，一台负载均衡器能够为很多RS进行分发。而且跑在公网上就能进行不同地域的分发。

缺点：隧道模式的RS节点需要合法IP，这种方式需要所有的服务器支持”IP Tunneling”(IP Encapsulation)协议，服务器可能只局限在部分Linux系统上。

三、直接路由模式（**VS-DR**）

原理：负载均衡器和RS都使用同一个IP对外服务｡但只有DR对ARP请求进行响应,所有RS对本身这个IP的ARP请求保持静默｡也就是说,网关会把对这个服务IP的请求全部定向给DR,而DR收到数据包后根据调度算法,找出对应的RS,把目的MAC地址改为RS的MAC（因为IP一致）并将请求分发给这台RS｡这时RS收到这个数据包,处理完成之后，

由于IP一致以直接将数据返给客户，则等于直接从客户端收到这个数据包无异,处理后直接返回给客户端｡由于负载均衡器要对二层包头进行改换,所以负载均衡器和RS之间必须在一个广播域,也可以简单的理解为在同一台交换机上｡

优点：和TUN（隧道模式）一样，负载均衡器也只是分发请求，应答包通过单独的路由方法返回给客户端。与VS-TUN相比，VS-DR这种实现方式不需要隧道结构，因此可以使用大多数操作系统做为物理服务器。

缺点：（不能说缺点，只能说是不足）要求负载均衡器的网卡必须与物理网卡在一个物理段上。

10 LVS简介？

答案：

LVS 是Linux Virtual Server ，Linux 虚拟服务器；是一个虚拟的服务器集群【多台机器LB IP】。LVS 集群分为三层结构:

负载调度器(load balancer)：它是整个LVS 集群对外的前端机器，负责将client请求发送到一组服务器[多台LB IP]上执行，而client端认为是返回来一个同一个IP【通常把这个IP 称为虚拟IP/VIP】

服务器池(server pool)：一组真正执行client 请求的服务器，一般是我们的web服务器；除了web，还有FTP，MAIL，DNS

共享存储(shared stored)：它为server pool 提供了一个共享的存储区，很容易让服务器池拥有相同的内容，提供相同的服务[不是很理解]

# 常用服务的端口

**HTTP:80 FTP:21 DNS:53 POP3:110 SMTP:25**

**SSH:22 NGINX:80 SQUID:3128 NAGIOS:5666 MEMCHACHED:11211**

**MYSQL:3360 TOMCAT:8080 NFS:2049 TLENET:23 HTTPS:443**

**SAMBA: UDP 138 TCP 139 POSTFIX: 25 IMAP: 143 zabbix：10051 cacti：**

**DHCP：68**