# 第三阶段面试题

## 一、云网服务管理

### 1. 缓存DNS与权威DNS有什么区别？一般用户在上网时，DNS解析过程是怎样的？

**答案：**

权威/官方DNS：至少管理一个DNS区域,，需要IANA等官方机构授权；比如根域DNS、一级域DNS、二级域DNS服务器等等。

缓存DNS：无需管理任何DNS区域，但是能够替客户机查询，通过缓存、复用查询结果来提高客户机体验的响应速度；比如ISP服务商、企业局域网。

用户上网时的DNS解析过程，按照优先顺序如下：

1. 首先检查本机的DNS缓存（内存中的记录）
2. 然后检查本机的hosts文件
3. 然后向网络配置中指明的首选DNS服务器（企业或ISP的缓存DNS）提交查询
4. 由首选DNS发起递归查询（问另一个缓存DNS）或迭代（问根、一级、二级、……DNS）查询，最终返回解析结果

### 2. 动态网站与静态网站有什么区别，http平台要支持PHP程序需要具备哪些条件？

**答案：**

静态网站：浏览器通过URL访问到的网页内容固定不变，对应服务端静态提供的资源文件，主要包括.txt文本、.html网页、.jpg|.png图片、.zip|.tar.gz压缩文件等等。

动态网站：浏览器通过URL访问到的网页内容动态变化，对应服务端的网页程序动态生成的资源文件，主要包括 .php、.jsp、.asp、.wsgi等不同网页语言编写的程序。

支持PHP程序：安装 httpd、php、php-mysql软件包

### 3. 是否了解Zabbix监控系统，它是如何获取路由交换设备或Linux主机信息的？

**答案：**

Zabbix是一套集中展示网络设备、主机信息的开源监控平台，通过C/S模式采集数据，通过B/S模式在WEB端展示和配置。

由zabbix server通过SNMP，zabbix agent，ping，端口监视等方法获取被监控设备信息。

zabbix agent需要安装在被监控的目标服务器上，主要完成硬盘、内存、CPU等硬件信息的收集。

而对于路由器、交换机等网络设备，则通过SNMP协议向zabbix server提供监控信息。

### 4. 如何配置httpd服务器支持多个网站？

**答案：**

在同一套Web服务器上提供多个网站的技术称为虚拟主机，标配的httpd并不支持虚拟主机。

若需要httpd支持多个Web网站，需要添加如下配置（每一个站点添加一段）：

<VirtualHost \*:80>

ServerName 此虚拟站点的DNS名称

DocumentRoot 此虚拟站点的网页根目录

</VirtualHost>

### 5. 在CentOS 6.x系统中，主要通过什么命令来管理系统服务的开启和关闭？

**答案：**

CentOS 6.x系统中，使用service工具：

# service 服务名 start //开启服务

# service 服务名 stop //停止服务

# service 服务名 restart //重启服务

# service 服务名 status //查看服务状态

# service 服务名 reload //重新加载服务配置

### 6. 在CentOS 7.x系统中，主要通过什么命令来管理系统服务的开启和关闭？

**答案：**

CentOS 7.x系统中，使用systemctl工具：

# systemctl start 服务名.. .. //开启服务

# systemctl stop 服务名.. .. //停止服务

# systemctl restart 服务名.. .. //重启服务

# systemctl status 服务名.. .. //查看服务装

### 7. 在CentOS 6.x系统中，如何将某个服务设置为开机自动运行？

**答案：**

CentOS 6.x系统中，使用chkconfig或ntsysv工具：

# chkconfig 服务名 on //设置开机自启

# chkconfig 服务名 off //禁止开机自启

或者

# ntsysv --level //通过交互工具配多个服务

### 8. 在CentOS 7.x系统中，如何将某个服务设置为开机自动运行？

**答案：**

CentOS 7.x系统中，使用systemctl工具：

# systemctl status 服务名XX .. .. //查看XX服务的状态

# systemctl restart 服务名XX .. .. //重启XX服务

### 9. 如何为一台CentOS7或RHEL7服务器添加新的软件源？

**答案：**

# vim /etc/yum.conf

.. ..

gpgcheck = 0 //禁止软件签名检查

# yum-config-manager --add-repo 软件源的URL网址 //添加新配置

# yum repolist //确认仓库列表

### 10. 在CentOS 7.x系统中，如何为新增加的网卡eth1添加网络连接配置？

**答案：**

可以使用nmcli工具添加连接：

# nmcli connection add con-name eth1 ifname eth1 type Ethernet

然后为此网卡配置IP地址参数（DHCP方式）：

# nmcli connection modify eth1 ipv4.method auto connection.autoconnect yes

或者，配置静态IP地址参数：

# nmcli connection modify eth1 ipv4.method manual ipv4.addresses IP地址/掩码位数 ipv4.gateway 默认网关地址 ipv4.dns DNS服务器地址 auto connection.autoconnect yes

### 11. 在CentOS 6.x系统中，如何为网卡eth0配置静态网络参数？

**答案：**

可以直接修改网卡eth0的配置文件/etc/sysconfig/network-scripts/ifcfg-eth0：

# /etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=eth0 //网卡设备名称

TYPE=Ethernet //网卡类型为以太网

ONBOOT=yes //启动时是否激活

BOOTPROTO=static //协议类型（static|dhcp）

IPADDR=192.168.1.90 //网络IP地址

PREFIX=24 //掩码位数

GATEWAY=192.168.1.1 //默认网关地址

BROADCAST=192.168.1.255 //广播地址

HWADDR=00:0C:29:FE:1A:09 //网卡MAC地址

然后，重新启动network服务即可：

# service network restart

### 12. 在CentOS或RHEL系统中，如何安装从第三方下载的.rpm软件包？

**答案：**

如果没有其他依赖关系，可以使用rpm命令直接安装：

# rpm -ivh 软件名-版本.架构.rpm .. ..

如果存在依赖关系，而且可以通过本机已知的软件源解决，可以使用yum命令安装：

# yum -y install 软件名-版本.架构.rpm .. ..

或者

# yum -y localinstall 软件名-版本.架构.rpm .. ..

### 13. 公司采用Nginx作为Web服务器，简述源代码编译安装Nginx的操作？

**答案：**

选择源代码编译方式来安装软件的话，好处是方便获取软件的最新版、可以灵活配置软件安装；不足是安装过程比rpm等方式要繁琐，而且需要有可用的编译环境。

比如，首先确保安装有可用的C语言编译环境（厨房）：

# yum -y install gcc gcc-c++ make

然后，需要从软件官方网站获取nginx软件的源代码文件（买菜，比如nginx-1.15.6.tar.gz）。

后续编译安装过程如下。

1）解包（取出菜）

# tar -xf nginx-1.15.6.tar.gz

2）配置（洗菜、配菜）

# cd nginx-1.15.6/

# ./configure //可以 ./configure --help获取帮助

3）编译（炒菜）

# make

4）安装（装盘上桌）

# make install

安装完成后，nginx程序的默认路径位于 /usr/local/sbin/nginx 。

### 14. Linux中第一个光盘驱动器的设备文件是sr0，第一个SATA接口硬盘的设备文件是？

**答案：**

SATA接口的硬盘类别为sd，老式IDE接口的硬盘类别为hd，硬盘设备的顺序按字母顺序排列，

因此第一个SATA接口的硬盘设备是 sda。

### 15. 分区的格式类型中可以作为Linux根分区格式的是？

**答案：**

EXT3 —— 比如，RHEL 5.x/CentOS 5.x系列操作系统

EXT4 —— 比如，RHEL 6.x/CentOS 6.x系列操作系统

XFS —— 比如，RHEL 7.x/CentOS 7.x系列操作系统

### 16. 在CentOS 6.x/7.x系统中，默认的防火墙服务分别是什么？

**答案：**

iptables、firewalld

### 17. 在CentOS 6.x/7.x系统中，开启什么服务可以提供对此主机的远程连接？

**答案：**

在Linux主机开启sshd服务，默认即允许从其他主机（使用Putty/Xshell/SecureCRT等支持SSH协议的客户端软件）远程连接。

### 18. 如果忘记了zabbix监控平台的管理员密码，应该怎么办？

**答案：**

为了避免监控数据丢失，可以使用zabbix数据库账号进入系统，想办法修改zabbix库users表中别名为admin的密码记录（比如改成某个已知密码的md5加密字串），从而通过新密码取回Web平台的管理权限。

### 19. 对Linux系统熟悉么，请列举几个你在Linux主机上配置过的网络应用？

**答案：**

Web网站（httpd）、数据库（MariaDB）、FTP（vsftpd）、yum软件源、邮件发送（postfix）、DHCP地址分配（dhcp）、PXE装机（tftp-server）、监控平台（zabbix）、……

### 20. 在一台CentOS 7.x主机上使用yum安装软件时，老出现如下提示，你会怎么办？

Existing lock /var/run/yum.pid: another copy is running as pid 3053.

Another app is currently holding the yum lock; waiting for it to exit...

The other application is: PackageKit

Memory : 37 M RSS ( 82 MB VSZ)

.. ..

**答案：**

首先，会尝试理解一下提示信息的含义，必要时借助翻译软件。

这段提示信息的含义大致是有另一个进程正在使用yum（所以加了占用锁），所以导致用户的yum操作无法执行；如果只是立即解决问题的话，可以尝试杀死那个进程（提示已指出进程名 PackageKit，进程编号为3053），比如执行pkill -9 PackageKit或者kill -9 3053。

如果是平时总出现类似提示的话，应该想办法阻止PackageKit进程反复出现，一般我会上网查找类似问题的解决办法，比如上度娘搜索“yum packagekit”，基本上都会有解决办法。

此列解决方法：

/etc/yum/pluginconf.d/refresh-packagekit.conf改为如下：

enabled=0

### 21. 在Linux主机中如何干掉某个正运行的程序？

**答案：**

如果知道这个进程的名字，可以执行 killall -9 进程名；

如果知道这个进程的一部分名字，可以执行 pkill -9 进程名关键词；

如果知道这个进程的编号（PID），可以执行 kill -8 进程号。

### 22. 适合用来搭建网站服务器的软件有哪些，各自有什么特点？

**答案：**

IIS，微软公司的Internet Information Server，适合小型企业的Windows网站服务器。

Apache HTTP Server，开源网站软件，市场占有率高。适合搭LAMP动态网站服务器，支持PHP或Python网页程序和MySQL数据库。

Nginx，开源网站软件，市场占有率这几年上升非常快，据说并发处理能力非常厉害；适合搭LNMP动态网站服务器，支持PHP或Python网页程序和MySQL数据库。

Tomcat，也是Apache项目组的一个网站项目吧，可以支持Java网页程序。

Jboss，红帽公司的Java网站服务器软件。

WebSphere，IBM公司的Java网站服务器软件。

### 23. 给你一台Linux服务器，如何加快它的开机启动速度？

**答案：**

1）减少不必要运行的程序和系统服务，设置不要开机自动运行。

# systemctl disable 服务名 .. .. --now

2）如果平时的管理主要是远程维护，还可以设置系统在纯字符模式下运行（不开桌面）。

# systemctl set-default multi-user.target //设置默认运行模式

# systemctl isolate multi-user.target //立即切换到字符模式

### 24. 如何查看Linux主机的路由表？

**答案：**

# route -n

### 25. 如何查看Linux主机上的网络连接情况？

使用netstat诊断工具，比如：

# netstat -antpu

.. ..

### 26. 如何知道CentOS 7.x系统中一共安装了大概多少个软件包？

**答案：**

使用yum list installed可以列出已安装的软件包，结合管道和wc -l操作可以统计行数，从而获知大约安装的软件包总数量。比如：

[root@localhost ~]# yum list installed | wc -l

1602

### 27. 简述httpd服务配置中ServerName、DocumentRoot、Listen、DirectoryIndex语句的含义？

**答案：**

ServerName：设置本网站注册的DNS名称（即完整域名）。

DocumentRoot：设置本网站的网页根目录。

Listen：设置监听Web服务的本机IP地址及端口。

DirectoryIndex：设置从网页目录中提取网页时优先查找的网页文件名。

### 28. 在一台DNS服务器来看，递归查询和迭代查询分别表示什么？

**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）。

### 29. 使用zabbix监控平台时，如何获得被监控主机网卡eth0的入站、出站流量？

**答案：**

需要为被监控主机分别添加入站流量、出站流量监控项，参考键值如下：

入站流量监控，键值为net.if.in[eth0]；

出站流量监控，键值为net.if.out[eth0]。

### 30. 管理Linux主机时，最常用的文件编辑器是什么？如何把开头5行移动到文件末尾去？

**答案：**

最常用的文件编辑器：vi，或者vim。

使用vim打开一个文件后，在第1行处按5dd可以剪切5行内容，然后按G移动到文件最后一行，再按p可以粘贴刚刚剪切的5行内容，完成。

## 二、数据库管理

### 1. 对于MySQL或MariaDB数据库服务器，如何为管理账号root设置密码？

**答案：**

可以使用mysqladmin工具，修改密码参考如下操作：

# mysqladmin -uroot -p旧密码 password '旧密码'

### 2. 管理MySQL或MariaDB数据库服务器时，如何创建新库并授权用户？

**答案：**

以管理账号root连接数据库，建库、授权操作分别使用CREATE、GRANT，例如：

MariaDB [(none)]> CREATE DATABASE 数据库名;

MariaDB [(none)]> GRANT all ON 数据库名.表名 TO 用户名@客户机地址 IDENTIFIED BY '密码';

### 3. 使用SQL指令在工资表salary中查询月薪资yuexin超过10000元的员工名单？

**答案：**

MariaDB [(none)]> SELECT \* FROM salary WHERE yuexin > 10000;

### 4. 在MySQL或MariaDB数据库服务器上，如何删除密码为空的root用户记录？

**答案：**

MariaDB [(none)]> DELETE FROM mysql.user WHERE User='root' AND Password='';

### 5. 如果忘记了MySQL或MariaDB数据库的管理密码，如何恢复？

**答案：**

基本恢复思路：

1. 首先停止数据库系统服务
2. 然后绕过授权直接开启mysqld\_safe程序（比如mysqld\_safe --skip-grant-tables）
3. 然后使用mysql连接数据库，通过grant重新为用户root授权，刷新授权表
4. 最后关闭mysqld\_safe进程，正常启动数据库系统服务

### 6. 简述MySQL或MariaDB数据库的备份与恢复操作？

**答案：**

备份操作使用mysqldump命令，例如：

# mysqldump -u 用户名 -p 数据库名 > 备份.sql

恢复操作使用mysql命令，例如：

# mysql -u root 数据库名 < 备份.sql

### 7. 请列出你知道的数据库产品？

**答案：**

MS SQLServer，微软公司的数据库商业软件。

Oracle，甲骨文公司的数据库商业软件，鼎鼎有名的，主要用在大型企业。

MySQL，非常流行的开源数据库软件，后来被SUN公司收购，又后来SUN公司被Oracle收购，所以现在MySQL也是Oracle公司的一款产品，暂未商业化。

MariaDB，与MySQL的亲缘关系非常紧密的一款开源数据库软件，出自于原MySQL数据库的主力作者之手，所以与MySQL数据库的相似度非常高。

其他还有听过IBM DB2、PostgreSQL、Infomix、Sybase等等，不太熟悉。

### 8. 数据库中的varchar和char类型有什么区别？

**答案：**

1）char为定长字符串型

可指定为1~255字符，当字段的值不够指定长度时，会在右边用空格补齐。

2）varchar为变长字符串型

可指定为1~255字符，当字段的值不够指定长度时，按实际字符数分配存储空间。

### 9. 如何为表格a增加一个名为score的列，此列作为第1列，并设置默认值75？

**答案：**

MariaDB [(studb)]> ALTER TABLE a ADD score float(5,2) DEFAULT 75 FIRST;

### 10. 数据表的主键指的是什么，如何实现自动增长的主键字段？

**答案：**

1）主键特点及要求

每一张表只能有一个主键字段，通常把能够唯一标识一条记录的字段设为主键字段，主键字段不允许出现重复的记录值，且不允许赋NULL值。

2）AUTO\_INCREMENT自动增长

将字段值设置为自动增加，无需手动赋值，适用于整数值字段，通常与 PRIMARY KEY 连用。比如：

MariaDB [(studb)]> ALTER TABLE stuinfo MODIFY 学号 char(13) PRIMARY KEY;

## 三、网络安全

### 1. ARP欺骗、中间人攻击是基于哪种方式实现的？

**答案：**

这两种方式都是针对ARP地址解析协议实施的，主要见于企业局域网环境。

交换网络中主机之间的通信依赖于ARP缓存表，其中记录了网络内不同IP地址的MAC地址以及交换机接口，而ARP缓存表的更新比较被动（来源于通信发起方主机），非常容易受到攻击者干扰。

如果攻击者针对受害主机发送大量的虚假“IP->MAC”记录，就可能导致受害主机的网络通信异常，构成ARP欺骗攻击。

如果攻击者针对通信双方同时进行ARP欺骗，可以进一步诱使通信双方把信息都转发给攻击者主机，从而构成ARP中间人攻击，这种攻击方式可能导致敏感信息泄露。

### 2. 是否熟悉华为防火墙，其默认的安全区域有哪些？

**答案：**

* Untrust(非受信任区域)：安全级别为5，通常用于定义互联网流量。
* DMZ（非军事化区域）：安全级别50，通常用于定义服务器所在区域。
* Trust(受信任区域):安全级别85，通常用于定义内网所在区域。
* Local(本地区域)：安全级别100，该区域主要定义，设备自身发启的流量，或者是抵达设备自身流量。比如Telnet、SNMP、NTP、IPsec VPN等流量。

### 3. DoS攻击、DDoS攻击分别指的是什么？

**答案：**

DoS即Deny of Service（拒绝服务），指的是通过任何一种方式，最终导致目标系统失去响应，从而无法为正常用户提供服务或资源的攻击。DDoS即Distribute DoS（分布式拒绝服务），指的是从分散在互联网各地的大量主机同时发起针对同一个目标的DoS攻击。

DoS 攻击中比较常见的是洪水方式，如 SYN Flood。

SYN Flood 攻击利用 TCP 协议三次握手的原理，发送大量伪造源 IP 地址的 SYN，服务器每收到一个 SYN 就要为这个连接信息分配核心内存并放入半连接队列，然后向源地址返回 SYN＋ACK，并等待源端返回 ACK。由于源地址是伪造的，所以源端永远都不会返回 ACK。如果短时间内接收到的 SYN 太多，半连接队列就会溢出，操作系统就会丢弃一些连接信息。 这样正常的客户发送的SYN请求连接也会被服务器丢弃。

### 4. VPN指的是什么，主要用在什么场合？

**答案：**

VPN即Virtual Private Network（虚拟专用网），指的是在两个网络实体之间建立的一种长距离、受保护的专用连接。这两个实体可以通过点到点的链路直接相连，也可以跨越不安全的Internet相连。

VPN主要应用于以下场合：

* 跨国企业、跨城市企业的分公司之间的企业内部网络互连
* 移动办公/出差员工与企业总部内部网络的互连
* 基于安全目的需要经过专用/加密通道访问某些特定网站

### 5. IDC与IPS分别指的是什么，两者有什么区别？

**答案：**

入侵检测系统（Intrusion Detection System，IDS）对入侵行为发现（告警）但不进行相应的处理。

入侵防护系统（Intrusion Prevention System，IPS）对入侵行为发现并进行相应的防御处理。

### 6. 防火墙上的QoS管理指的是什么，有什么好处？

**答案：**

QoS即Quality of Service（服务质量），指的是在防火墙对网络中的流量按照一定的规则进行分类，并对这些流量进行带宽的预留和保证的技术。通过QoS管理措施，可以确保特征流量在网络中高效率、低延迟的转发，对垃圾流量进行及时处理。

### 7. 什么是MD5?

**答案：**

MD5即报文一摘要算法，它是一种基于哈西函数的密码算法，以任意长度的消息作为输入，生成128位的消息摘要作为输出，输入消息是按512位的分组处理的，它的最大作用在于，将不同格式的大容量文件信息在用数字签名软件来签署私人秘钥前“压缩”成一种保密格式，关键在于这种“压缩”是不可逆的。

### 8. 什么是防火墙，为什么需要防火墙？

**答案：**

防火墙是在两个网络之间强制实施访问控制的一个系统或一组系统。

如果没有防火墙，则整个内部网络的安全性安全依赖于每个主机，因此，所有主机都必须达到一致的高度安全水平，这在实际操作时非常困难，而防火墙被设计为只运行专用的访问控制软件设备，没有其他的服务，因此也就意味着相对少一些缺陷和安全漏洞，这就使得安全管理变得更为方便，易于控制，也会使内部网络更加安全。

### 9. 什么是DMZ？

**答案：**

DMZ又称为非军事区或者停火区，是在内部网络和外部网络之间增加的一个子网。

### 10. 防火墙有哪些局限性？

**答案：**

1）不能防范内部网络攻击

2）防火墙一般不提供对内部数据的保护

3）无法防范数据驱动型攻击

4）防火墙不能阻止内部泄露的行为

### 11. 网络安全的含义是什么？

**答案：**

它是一个系统性的概念，不仅包括网络信息的存储安全，还有涉及信息的产生、传播和使用过程中的安全，应该说网络节点处的安全和通信链路上的安全共同构成了系统的安全体系。

### 12. 网络安全的本质是什么？

**答案：**

网络安全从其本质上来讲就是网络上的信息安全。

### 13. 建立口令应遵循哪些规则？

**答案：**

1）不使用和用户名相同的口令

2）不使用日期口令

3）不使用英文单词

4）使用长口令和复杂口令

5）经常更换口令

6）不使用个自己一些相关的信息最为口令如电话号码

### 14. 网络安全主要有哪些关键技术？

**答案：**

安全漏洞扫描技术、主机安全技术、安全路由器、防火墙技术、入侵检测技术、身份认证技术、网络攻防技术、网络监控与审计技术。

### 15. 包过滤防火墙的基本思想是什么？

**答案：**

对所接收的每个数据包进行检查，根据过滤规则，然后决定转发或者丢弃该包，包过滤防火墙往往配置成双向的。

### 16. 我国制定实行的信息安全等级各是什么名称？

**答案：**

我国制定施行的信息安全等级分为五级，他们是第一级：用户自主保护级、第二级：系统审计保护级、第三极：安全标记保护级、第四级：结构化保护级、第五级：访问验证保护级。

### 17. 简述SQL注入漏洞的原理？

**答案：**

利用恶意SQL语句（WEB缺少对SQL语句的鉴别）实现对后台的数据库的攻击行为。

### 18. 为什么要研究网络安全？

**答案：**

网络需要与外界联系，同时也就受到许多方面的威胁：物理威胁、系统漏洞造成的威胁、身份鉴别威胁、线缆廉洁威胁和有害程序威胁等（可详细展开）。

### 19. 目前网络基本安全技术有哪些？

**答案：**

目前的网络基本安全措施有数据加密、数字签名、身份认证、防火墙和入侵检测等。

### 20. 网络安全的基本体系包含哪几部分？

**答案：**

网络安全的基本体系由物理安全、信息安全、安全管理三部分组成。