**安全web服务**

PKI，公钥基础设施

公钥：主要用来加密数据

私钥：主要用来解密数据（与相应的公钥匹配）

数字证书：证明拥有者的合法性/权威性（单位名称、有效期、公钥、颁发机构及签名、......）

CA，数字证书授权中心：负责证书的申请/审核/办法/鉴定/撤销等管理工作

实现HTTPS加密的条件

HTTPS机密web通信（TCP443端口）

SSL，安全套接字层

TLS，安全传输协议

实现条件

启用SSL模块支持

部署好机密素材：网站服务器的数字证书、网站服务器的私钥、根证书（CA管理机构的证书）



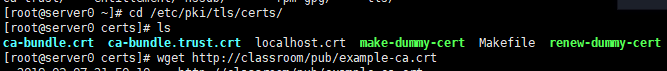


部署证书、密钥相关文件

证书、密钥文件的部署路径

/etc/pki/tls/certs/证书文件.crt

/etc/pki/tls/private/私钥文件.key







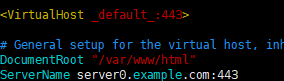
调整web服务配置

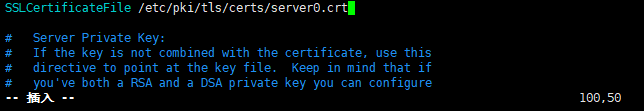
配置要点

指定ssl虚拟站点的DNS名称、网页根目录

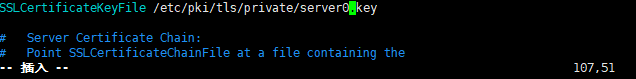
指定站点证书/根证书/站点密钥的位置







指定网站证书



指定密钥

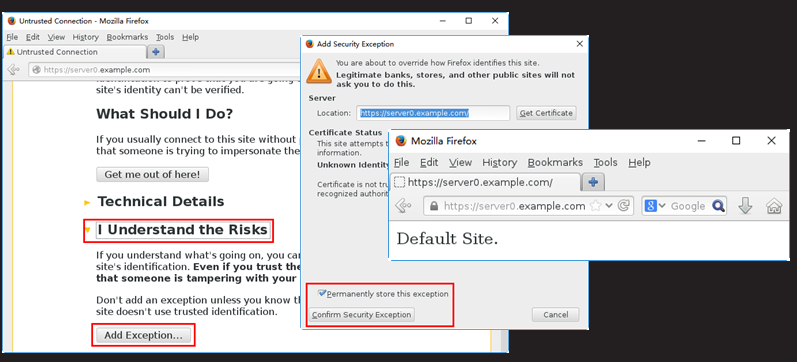


指定根证书



访问站点

<https://server0.example.com>



**准备交换分区**

parted分区工具

使用fdisk操作>2.2TB的磁盘时，超出容量的磁盘将无法识别，导致分区失败

原因分析：

主要受限于msdos分区模式

要支持大容量（18EB），需改用gpt分区模式（只有primary分区，可超过四个，可有128个主分区）

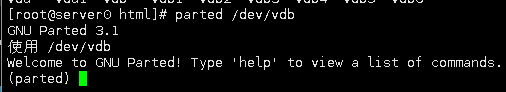
解决办法：

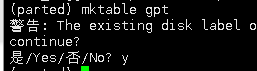
使用gdisk分区工具，用法与fdisk类似

使用parted分区工具：

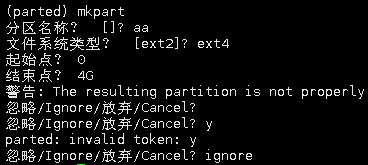
mktable gpt重建分区表

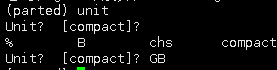
mkpart primary（分区名） 文件系统类型 起始位置 结束位置



指定分区的模式

输出磁盘信息

分区

选择单位

什么是交换空间（缓解物理内存的压力）

相当于虚拟内存

当物理内存不够时，使用磁盘空间来模拟内存

在一定程度上缓解内存不足的问题

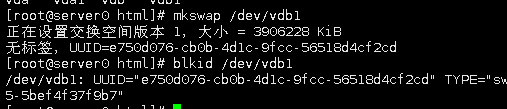
交换分区：以空闲分区充当交换空间

交换文件：以文件模拟的设备充当的交换空间

如何建立一个交换分区

将提供的设备按swap类型进行格式化

mkswap 空闲分区或设备

格式化交换空间并查看块设备ID

交换空间的启用与控制

手动管理操作

swapon 交换设备 启用

swapon -s 查看

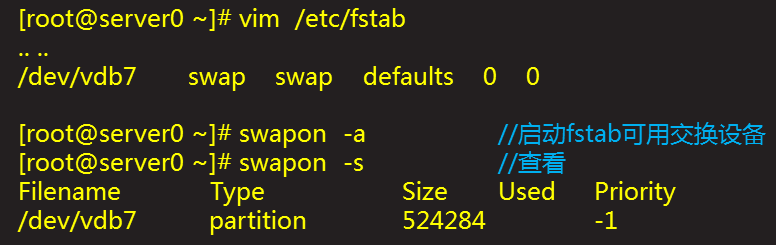
swaponoff 交换设备 停用

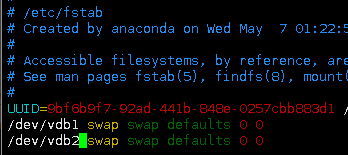




修改/etc/fstab配置文件

交换设备 swap swap defaults 0 0



swapon -a用于检测/etc/fstab的信息并挂载

**基础邮件服务**

**SMTP（用户传输协议 端口25）：用户发邮件协议**

**pop3（用户收邮件协议 端口110）：用户收邮件协议**

电子邮件通信

电子邮件服务器的基本功能

为用户提供电子邮件存储空间（用户名@邮件域名）

处理用户发出的邮件 传递给收件服务器

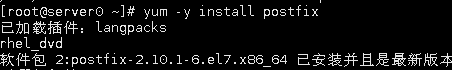
处理用户收到的邮件 投递到邮箱

快速部署postfix邮件服务器

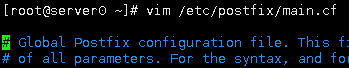
装包、配置、起服务

默认的标准配置即可为本机提供发/收邮件服务

若有必要，可扩大范围（邮件域）

默认已经安装

改配置文件/etc/postfix/main.cf



默认的域名后缀，是@后面的部分

允许本机所有网卡提供邮件服务，只要能ping通，就能利用该网卡发邮件

判断为本域邮件（当收件人的域名后缀与目的地址一致时，判断为本域邮件）  
 默认随机自动

使用mail命令发信/收信

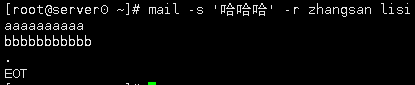
mail发信操作

mail -s ‘邮件标题’ -r 发件人 收件人[@收件域]...

步骤1：创建用户



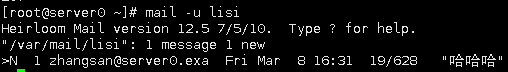
步骤2：发邮件



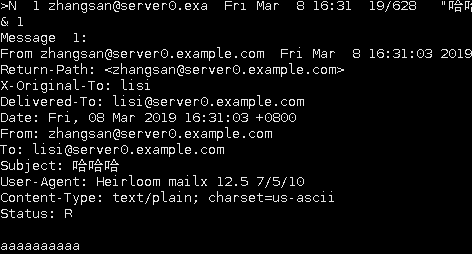
-s主题，-r源头，指发件人，不写后缀即默认后缀，遇到.结束

mail 收信操作

mail [-u用户名]



N代表新邮件，输入数字1并回车就可以看到邮件



所有用户的邮件在/var/spool/mail/

