**第三部分：服务搭建与运维（500分）**

一、虚拟主机信息表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 虚拟主机名称 | 镜像模板(源) | 云主机类型(flavor) | VCPU数量 | 内存、硬盘信息 | 网络名称 |
| Windows1 | Windows Server 2022 | windows | 2 | 4G、40G | Vlan工位号 |
| Windows2 | Windows Server 2022 | windows | 2 | 4G、40G |
| linux1 | Rocky9.2 | Rocky | 1 | 2G、20G |
| linux2 | Rocky9.2 | Rocky | 1 | 2G、20G |
| linux3 | Rocky9.2 | Rocky | 1 | 2G、20G |
| linux4 | Rocky9.2 | Rocky | 1 | 2G、20G |

二、云平台配置

云平台相关说明：

每个工位上有个网线连接的电脑，IP地址是本工位号（如：工位号,地是1，地址为192.168.100.101/24），访问云平台地址为192.168.100.100/dashboard。考试账号和密码现场发放。

云实训平台中提供镜像环境，镜像的默认用户名密码以及镜像信息如下表所示。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 用户名 | 密码 | SSH | RDP |
| Windows Server 2022 DataCenter | Administrator | Pass-1234 | 否 | 是 |
| Rocky9.2 | root | Pass-1234 | 是 | 否 |

所有windows主机实例在创建之后通过remmina远程桌面连接操作，Rocky9.2可以通过remmina软件进行ssh连接操作，所有linux主机都默认开启了ssh功能，Linux系统软件镜像位于”/opt”目录下。

要求在云实训平台中保留竞赛生成的所有虚拟主机。云实训平台安装与运用创建虚拟主机按照“虚拟主机信息表”所示，按要求生成虚拟主机；

三、计算机操作系统安装与管理

1.PC1 系统为 ubuntu-desktop-amd64系统 (已安装，语言为英文 ) ，登录用户为xiao，密码为Key-1122。启用root用户，密码为Key- 1122。

2.安装remmina软件，用该软件连接云服务器上的虚拟机，并配置虚拟机上的相应服务。

3.安装qemu和virtinst。

4.创建 Windows Server 2022 虚拟机，虚拟机信息如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 虚拟机名称 | vcpu | 内存 | 硬盘 | IPv4 地址 | 完全合格域名 |
| Windows3 | 2 | 4096MB | 40GB | 10.13.11.101/24 | Windows3.skills.lan |

5.安装windows3，系统为Windows Server 2022 Datacenter Desktop，网络模式为桥接模式，网卡、硬盘、显示驱动均为 virtio，安装网卡、硬盘、显示驱动并加入到 Windows AD中。在 windows3 中添加 3 块5GB的硬盘 (硬盘驱动为 virtio ) ，初始化为GPT配，置为raid5。驱动器盘符为 D。

6.从U盘启动PC2，安装kylin桌面操作系统（安装语言为英文），安装时创建用户为xiao，密码为Key-1122。启用root用户，密码为Key-1122。

7.配置minicom，用该软件连接网络设备，并对网络设备进行配置。

四、Windows云服务配置

1．域服务

(1)域服务 任务描述：请采用域环境，管理企业网络资源。

(1)配置windows2 为skills.lan域控制器；安装dns服务，配置dns正反向区域在active directory中存储，负责该域的正反向域名解析。

(2)把skills.lan域服务迁移到windows1；安装dns服务，配置dns正反向区域在active directory中存储，负责该域的正反向域名解析。

(3)把其他windows主机加入到 skills.lan域。所有windows主机(含域控制器 )用 skills\Administrator 身份登陆。

在 windows1 上安装证书服务，为 windows 主机颁发证书，证书颁发 机构有效期为 10 年，证书颁发机构的公用名为 windows1.skills.lan。 复制“计算机”证书模板，名称为“计算机副本”，申请并颁发一张供 windows 服务器使用的证书，证书友好名称为 pc，（将证书导入到需 要证书的 windows 服务器），证书信息：证书有效期=5 年，公用名 =skills.lan，国家=CN，省=Beijing，城市=Beijing，组织=skills， 组织单位=system，使用者可选名称=\*.skills.lan 和 skills.lan。 浏览器访问 https 网站时，不出现证书警告信息。

在 windows2 上安装从属证书服务，证书颁发机构的公用名为 windows2.skills.lan。

(4)启用所有 windows 服务器的防火墙。

(2)在 windows1上新建名称为manager、dev、sale的3个组织单元；每个组织单元内新建与组织单元同名的全局安全组；每个组内新建20个用户：行政部 manager00-manager19 、开发部 dev00-dev19 、营销部 sale00-sale19，不能修改其口令，密码永不过期。manager00 拥有域管理员权限。

2．组策略

( 1)添加防火墙入站规则，名称为icmpv4，启用任意IP地址的icmpv4 回显请求。

(2)允许manager组本地登录域控制器，允许manager00 用户远程 登录到域控制器；拒绝dev组从网络访问域控制器。

(3)登录时不显示上次登录，不显示用户名，无须按 Ctrl+Alt+Del。

(4)登录计算机时，在桌面新建名称为chinaskills的快捷方式,目标为 http://www.chinaskills-jsw.org，快捷键为 Ctrl+Shift+F6。

3．文件共享

任务描述：请采用文件共享，实现共享资源的安全访问。

( 1)、在windows1的C:\盘分区划分2GB的空间，创建NTFS分区，驱动器号为D:\。创建用户主目录共享文件夹：本地目录为 D:\share\home，共享名为home，允许所有域用户完全控制。在本目录下为所有用户添加一个以用户名命名的文件夹，该文件夹将设置为所有域用户的home目录，用户登录计算机成功后，自动映射挂载到H卷。禁止用户在该共享文件中创建“\*.exe”文件，文件组名和模板名为my。

(2)、创建 目录 D:\share\work，共享名为work，仅manager组和Administrator组有完全控制的安全权限和共享权限，其他认证用户有 读取执行的安全权限和共享权限。在AD DS中发布该共享。

4.FPT

任务描述：请采用 ftp 服务器，实现文件安全传输。

1.把 windows3 配置为 ftp 服务器，ftp 站点名称为 ftp，站点绑定本机 ip 地址，站点根目录为 C:\ftp。

2.站点通过 active directory 隔离用户，用户目录为 C:\ftp，用户目录名 称与用户名相同，使用 dev00 和 dev01 测试。

3.设置 ftp 最大客户端连接数为 1000，控制通道超时时间为 3 分钟,数据通 道超时时间为 1 分钟。

5. iscsi 服务

任务描述：请采用 iscsi，实现集中管理存储。

1.在 windows2 上添加 4 块硬盘，每块硬盘大小为5G。初始化为 gpt 磁盘，配置 raid5，创建 1 个 iscsi 磁盘，存放在 E:\iscsi，磁盘名称和目标名称分别为 file，磁盘大小为动态扩展 5GB，目标的 iqn 名称为 iqn.2022-05.lan.skills:server 使用 dns 名称 建立目标。发起程序的 iqn 名称为 iqn.2022-05.lan.skills:client。 2.windows3 使用 FQDN 连接 windows2 的 iscsi 磁盘，初始化为 GPT 分区表，创建 NTFS 分区，驱动器号为 E。

6. ASP服务

任务描述：请采用IIS搭建web服务，创建安全动态网站，。

( 1)、把windows2配置为ASP网站，网站仅支持 dotnet clr v4.0，站点名称为asp。

(2)、http 和 https 绑定本机与外部通信的 IP 地址，仅允许使用域名访问 （使用“计算机副本”证书模板）。客户端访问时，必需有 ssl 证书 （浏览器证书模板为“管理员”）。

(3)、网站目录为 C:\iis\contents ， 默认文档index.aspx内容为 "Helloaspx"。

(4)、使用windows3测试。

五、Linux 云服务配置

1．DNS服务

任务描述：创建DNS服务器，实现企业域名访问。

( 1)所有linux主机启用防火墙，防火墙区域为 public，在防火墙中放行对应服务端口。

(2)利用chrony，配置linux1为其他linux主机提供NTP服务。

(3)所有 linux主机之间 (包含本主机 )root用户实现密钥ssh认证，禁用密码认证。

(4)利用bind，配置linux1为主DNS服务器，linux2为备用DNS服务器。为所有linux主机提供冗余DNS正反向解析服务。

2．Apache服务

任务描述：请采用Apache 搭建企业网站。

(1)、配置linux1为CA服务器，为linux主机颁发证书。证书颁发机构有效期10年，公用名为linux1.skills.lan。申请并颁发一张供linux服务器使用的证书，证书信息：有效期=5年，公用名=skills.lan，国家=CN，省=Beijing，城市=Beijing，组织=skills，组织单位=system，使用者可选名称=\*.skills.lan和skills.lan。将证书skills.crt和私钥skills.key复制到需要证书的linux服务器/etc/ssl目录。

(2)、配置linux1为Apache服务器，使用skills.lan或any.skills.lan(any代表任意网址前缀，用linux1.skills.la和web.skills.lan测试)访问时，自动跳转到 www.skills.lan。禁止使用IP地址访问，默认首页文档 /var/www/html/index.html 的内容为"apache"。浏览器访问https网站时，不出现证书警告信息。

3．tomcat 服务

任务描述：采用 Tomcat 搭建动态网站。

(1)配置linux2为nginx 服务器，默认文档 index.html 的内容为 “hellonginx”；仅允许使用域名访问，http访问自动跳转到https。

(2)利用nginx反向代理，实现linux3和linux4的tomcat负载均衡，通过 https//tomcat.skills.lan 加密访问 Tomcat

(3)配置linux3和linux4为tomcat服务器，网站默认首页内容分别为“tomcatA”和“tomcatB”，仅使用域名访问80端口的http服务。

4．samba 服务

任务描述：请采用 samba 服务，实现资源共享。

(1)在 linux3上创建user00-user19共20个用户；user00和user01添加到manager组 ， user02和user03添加到dev组。 把用户user00-user03添加到samba 用户。

(2)配置 linux3为samba服务器,建立共享目录/srv/sharesmb，共享名与目录名相同。manager组用户对sharesmb共享有读写权限，dev组对sharesmb共享有只读权限；用户对自己新建的文件有完全权限， 对其他用户的文件只有读权限，且不能删除别人的文件。在本机用smbclient命令测试。

(3)在 linux4 修改/etc/fstab,使用用户user00 实现自动挂载linux3的sharesmb共享到/sharesmb。

5. ISCSI服务

（1）为linux3添加4块硬盘，每块硬盘大小为5G，创建lvm卷，卷组名为vg1，逻辑卷名为lv1，容量为全部空间，格式化为ext4格式。使用

/dev/vg1/lv1配置为iSCSI目标服务器，为linux9提供iSCSI服务。iSCSI目标端的wwn为iqn.2023-08.lan.skills:server, iSCSI发起端的wwn为iqn.2023-08.lan.skills:client。

（2）配置linux4为iSCSI客户端，实现discovery chap和session chap双向认证，Target认证用户名为IncomingUser，密码为IncomingPass；Initiator认证用户名为OutgoingUser，密码为OutgoingPass。修改/etc/rc.d/rc.local文件开机自动挂载iscsi硬盘到/iscsi目录。

6．Mysql 服务

任务描述：请安装mysql服务，建立数据表。

(1)配置linux2为mysql服务器，创建数据库用户xiao，在任意机器上对所有数据库有完全权限。

(2)创建数据库userdb；在库中创建表userinfo，表结构如下:

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 数据类型 | 主键 | 自增 |
| id | int | 是 | 是 |
| name | varchar( 10) | 否 | 否 |
| birthday | datetime | 否 | 否 |
| sex | varchar(5) | 否 | 否 |
| password | varchar(200) | 否 | 否 |

(3)在表中插入2条记录，分别为(1,user1，1999-07-01，男) ， (2,user2 ，1999-07-02 ，女)，password 与 name 相同，password字段用md5函数加密。

(4)修改表userinfo的结构，在name字段后添加新字段 height(数据类型为 float)，更新user1和user2 的height字段内容为1.61和1.62。

（5）新建/var/mysqlbak/userinfo.txt文件，文件内容如下，然后将文件内容导入到userinfo表中，passord字段用md5函数加密。

3,user3,1.63,1999-07-03,女,user3

4,user4,1.64,1999-07-04,男,user4

5,user5,1.65,1999-07-05,男,user5

6,user6,1.66,1999-07-06,女,user6

7,user7,1.67,1999-07-07,女,user7

8,user8,1.68,1999-07-08,男,user8

9,user9,1.69,1999-07-09,女,user9

(6) 每周五凌晨 1:00以 root用户身份备份数据库userdb 到 /var/databak/userdb.sql(含创建数据库命令)。

7. ftp 服务

任务描述：请采用 ftp 服务器，实现文件安全传输。

1.配置 linux1 为 ftp 服务器，安装 vsftpd，新建本地用户 xiaoming，本地 用户登陆 ftp 后的目录为/var/ftp/pub，可以上传下载。

2.配置 ftp 虚拟用户认证模式，虚拟用户 ftp1 和 ftp2 映射为 ftp，ftp1 登 录 ftp 后的目录为/var/ftp/vdir/ftp1，可以上传下载,禁止上传后缀名为.sh 的 文件；ftp2 登录 ftp 后的目录为/var/ftp/vdir/ftp2，仅有下载权限。

3.使用 ftp 命令在本机验证。

8. nfs 服务

任务描述：请采用 nfs，实现共享资源的安全访问。

1. 配置 linux2 为 kdc 服务器，负责 linux3 和 linux4 的验证。
2. 在 linux3 上，创建用户，用户名为 xiao，uid=2000，gid=2000，家目录 为/home/xiaodir。
3. 配置 linux3 为 nfs 服务器，目录/srv/sharenfs 的共享要求为：linux 服务器所在网络用户有读写权限，所有用户映射为 xiao，kdc 加密方 式为 krb5p。
4. 配置 linux4 为 nfs 客户端，利用 autofs 按需挂载 linux3 上的 /srv/sharenfs 到/sharenfs 目录，挂载成功后在该目录创建 test 目录。

9. mail 服务

任务描述：请采用 postfix 邮件服务器，实现安全的邮件服务。

1.配置 linux4 为 mail 服务器，安装 postfix 和 dovecot。

2.仅支持 smtps 和 pop3s 连接。

3.创建用户 mail1 和 mail2，向 all@skills.com 发送的邮件，每个用户都 会收到。

4.使用本机测试。

10．shell 脚本

任务描述：请采用 shell 脚本,实现快速批量的操作。

1. 在 linux4 上编写/root/createfile.sh的shell脚本，创建20个文件/root/shell/file00至/root/shell/file19，如果文件存在，则删除再创建； 每个文件的内容同文件名， 如file00文件的内容为“file00”。
2. 用/root/createfile.sh命令测试。