模块 A　网管系统管理与性能优化（样题）

（共 40 分）

一、竞赛注意事项

（1）禁止选手携带和使用任何移动存储设备、计算器、通信工具及参考资料进入考场。

（2）不得随意离开比赛工位，有问题举手示意裁判，需要一名以上的专家裁判到比赛工位解决。

（3）操作过程中，需要及时保存设备配置。

（4）竞赛结束后，所有设备保持运行状态，竞赛设备、软件和赛题请保留在座位上，禁止将竞赛所用的所有物品（包括试卷和草纸）带离赛场。

（5）竞赛相关的工具软件及文档都放在 PC 桌面上。

（6）竞赛结束后，需要保持所有的服务器正常运行。

（7）网络虚拟化系统实训平台中的实例 IP 参数设置请按照“表 1.网络虚拟化系统实训平台网络信息表”的要求设定。

（8）所有服务器要求虚拟机系统重新启动后，均能正常启动和使用。

（9）题目中所有未指明的密码均参见“表 3.云主机和服务器密码表”，禁止自行设置其他密码。

二、实训平台相关说明

网络虚拟化系统实训平台管理网口为：ETH1；业务网口为：ETH2；管理 ip 地

址为 172.16.1.100，登陆账号为 mingdian，密码为 md123456，选手禁止修改实训平台账号密码及管理 ip 地址。网络虚拟化系统实训平台智能平台管理接口（IPMI 口）地址为 172.16.1.250，登录账号为 mingdian，密码为 md123456。

所有 Linux 云主机默认开启 SSH 功能，可以通过 CRT 软件连接进行操作。Linux 系统软件安装源文件位于/dev/myiso/目录下，yum 源已开机自动挂载。本次竞赛提供 1 条 Console 调试配置线缆、4 根 RJ45 网络跳线，所有网络设备使用这条 Console 线缆对设备进行调试，选手需要根据任务要求配置赛场提供的三层交换机，以实现网络虚拟化系统实训平台与 PC 机互联互通来完成竞赛任务。

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
Centos7.9	root	mdteccloud	是	否

要求在实训平台中保留竞赛生成的所有虚拟主机。

表 1：网络虚拟化系统实训平台网络信息表

网络名称	Vlan 号	是否共享	子网名称	子网网络地址	网关 IP	激活 DHCP	地址池范围
Vlan301	301	是	Gd301	192.168.21.0/24	192.168.21.254	是	192.168.21.10-20
Vlan302	302	是	Gd302	192.168.22.0/24	192.168.22.254	是	192.168.22.10-20
Vlan303	303	是	Gd303	192.168.23.0/24	192.168.23.254	是	192.168.23.10-20

表 2：网络虚拟化系统实训平台实例信息表

实例名称	镜像模板（源）	配置列表	VCPU 数量	内存、硬盘信息	网络名称	IP 地址
云主机 1	Centos7.9	Linux-2440	2	4G、40G	Vlan301	192.168.21.11
云主机 2	Centos7.9	Linux-2440	2	4G、40G	Vlan301	192.168.21.12
云主机 3	Centos7.9	Linux-2440	2	4G、40G	Vlan302	192.168.22.13
云主机 4	Centos7.9	Linux-2440	2	4G、40G	Vlan302	192.168.22.14
云主机 5	Centos7.9	Linux-2440	2	4G、40G	Vlan303	192.168.23.15
云主机 6	Centos7.9	Linux-2440	2	4G、40G	Vlan303	192.168.23.16

表 3.云主机和服务器密码表

题目中所有未指明的密码	Mdtec@cloud（注意区分大小写）

任务一、网络虚拟化系统实训平台配置（1 分）

平台配置要求：

1、按照“表 1 网络虚拟化系统实训平台网络信息表”创建 VLAN 网络，并根据“表 2 网络虚拟化系统实训平台云主机信息表”创建云主机。

2、创建 7 个卷，大小均为 5G，依次命名为“HT1”至“HT7”。

注意事项：

（1）在分离卷之前要保证在该卷的 Linux 主机中，已经不存在该卷的任何挂载点，否则会造成分离失败，或是一直显示“分离中”状态。

（2）在实训平台中可以创建多个卷，一个虚拟主机可以同时连接多个卷，但一个卷同时只能给一个虚拟主机作为扩展硬盘使用。

（3）网络虚拟化系统实训平台中的实例 IP 地址及相关参数，默认由 DHCP 进行分配，系统中的 IP 地址一般情况下需要与 DHCP 获取的地址相同，否则会造成网络无法连通。

任务二、Linux 基础配置（3 分）

1、根据下表配置“云主机 1”~“云主机 6”的主机名称。编辑所有云主机的网络适配器配置文件，设置 DNS 服务器的 IP 地址，使其指向“云主机 1”和“云主机 2”的 IP。要求所有 Linux 云主机都能够免密码 ssh 登录到其他 Linux 云主机的 root 用户。

实例名	完全域名
云主机 1	dns.2025skills.com
云主机 2	file.2025skills.com
云主机 3	mail.2025skills.com
云主机 4	mariadb.2025skills.com
云主机 5	ntp.2025skills.com
云主机 6	monitor.2025skills.com

2、在网络管理员的日常管理维护工作中，经常需要实现快速批量的操作系统进行操作。请在“云主机 1”上创建 99 个用户，用户名从 "Admin01" 到 "Admin99"，设置密码全部为 Guangdong2025,要求每个用户在密码过期之前警告的天数为 7 天，然后将用户添加到 Guangdong 组中，设置账户从不过期和失效。

3、将 HT1 和 HT2 共 2 个卷挂载到“云主机 5”中，将其加入到名为“GzVG”的卷组中，从中创建一个大小为 8G 的逻辑卷“GzLV”，格式化逻辑卷为 xfs 文件系统并开机自动挂载到/mnt/HT1 目录。

任务三、域名服务配置（3 分）

4、在“云主机 1”中安装 bind 服务，配置该云主机为主域名服务器，添加 2025skills.com 区域，根据主机名称添加对应的主机记录，依次指向“云主机 1”至“云主机 5”，每个记录均需完成正、反向解析，并配置 notify 加快同步速度。

5、在“云主机 2”中安装 bind 服务，配置该主机为备份域名服务器，与主域名服务器实时同步，将区域文件存储路径设置为/var/named/slaves/。

6、为增加 DNS 区域传输的安全性，要求使用 TSIG 密钥机制对主服务器和备份服务器

之间的区域传输进行身份验证，密钥值在主服务器中手动生成并保存在/root 目录下，身份验证算法为 HMAC-SHA256，只有使用名为“tsig-key”的 TSIG 密钥进行授权的请求才能进行区域传输。

任务四、证书服务配置（2 分）

1、配置“云主机 1”为 CA 服务器，使用 4096 位密钥和 SHA256 算法，为云主机颁发证书。CA 私钥文件名为 Ca.key。私钥文件存放于/etc/pki/CA/private 目录；CA 根证书使用系统默认文件名：/etc/pki/CA/Ca.crt，有效期 10 年，公用名 dns.2025skills.com。

2、在 CA 服务器中申请并颁发一张供云主机使用的证书：2025Skills.crt ，私钥为 2025Skills.key，证书有效期 3 年，证书基本信息：国家=“CN”，省份=“GD”，市/县=“GZ”，组织=“GDskills”，组织单位=“GDskills_org”，公用名 ca.2025skills.com。证书可以用于服务器和客户端身份认证,存放于/var/open_ssl。

任务五、网站服务配置（3 分）

1、在“云主机 1”中安装配置 Apache 服务，搭建 Web 网站，首页文档为 index.html，内容为“欢迎访问 CA 证书下载站点!”，目录为/var/www/ca_web/，网站访问域名为 www.2025skills.com。

2、为确保证书安全传输，在 CA 服务器启用 HTTPS 服务,CA 的签发证书全部要用 CURL 命令工具安全下载，存放在需要证书的云主机的/etc/ssl 目录下。

3、为确保访问安全，在网站服务器中配置用户登录验证，访问网站时需要验证的用户名称为：httpuser，验证方式为口令模式，当用户访问网站时的提示信息“请输入账号认证访问！” 。

4、当访问“云主机 1”中 Web 网站时，访问 2025skills.com 自动跳转到 www.2025skills.com，使用 http 访问自动跳转到 https，使用 HTTP 和 HTTPS 站点均指向同一主页。

任务六、SAMBA 服务配置（3 分）

1、在“云主机 2”上安装 Samba 服务，新建用户 chinasmb，创建共享路径为/etc 共享名为“china-smb”的共享目录，该共享目录对正在浏览的用户可见，只允许用户 chinasmb 访问。在“云主机 3”上设置开机自动挂载“china-smb”的共享目录到/smb-file。

2、在 Samba 服务器上创建共享路径为/home/project,共享名为“gd-smb”的共享目录，该共享目录对正在浏览的用户可见，可以被 users 组写入。

3、在“云主机 2”中添加三个用户，名称为 smbuser1, smbuser2, smbuser3 ，且均加入 users 为次要群组。加入 users 这个群组的用户可以使用云主机 2 的 gd-smb 共享资源，且在该目录下 users 群组的使用者具有写入的权限。在“云主机 3”中安装配置 samba-client 客户端用于测试。

任务七、FTP 服务配置（3 分）

1、在“云主机 2”中安装配置 FTP 服务器，设置监听 TCP 端口 2121，设置会话超时为 2 分 30 秒，启用被动传输模式，客户端端口范围为 31000 到 31500。

2、在FTP服务器中,创建不可登录系统的本地用户 viruser,Home 目录为/opt/viruser。创建两个虚拟用户 lily 与 lisa 的登录目录为/data1 与/data2，分别在目录内创建 lily.txt 与 lisa.txt;将登录目录的所有者设置为 viruser。创建虚拟用户的文本文件，建立支持虚拟用户登录时进行验证的 PAM 认证文件;为虚拟用户 lily 与 lisa 分别建立满足各自要求的配置文件，其中 lily 用户可以下载、上传、删除文件和创建目录，禁止上传后缀名为.exe 的文件，lisa 用户可以浏览、且仅能下载文件资料。

3、在宿主机上新建测试文件 file.exe 和 lily.pdf。

任务八、NFS 服务配置（2 分）

1.在“云主机 3”中安装 NFS 服务，创建并共享文件夹/data/nfs 和/data/backup,并分别创建 nfs.txt 和 backup.txt。其中/data/nfs 共享文件夹除了为网域内的工作站提供数据服务，同时为 Internet 提供数据服务。/data/backup 共享文件夹保存服务器相关的备份数据。同时，对 NFS 服务进行访问控制，规则如下：

范围	权限
192.168.21.11（云主机 1）	读写，禁止删除文件
192.168.22.14（云主机 4）	读写，禁止删除文件
0.0.0.0/0（Internet）	只读

2、配置“云主机 1”为 nfs 客户端,利用 autofs 按需挂载“云主机 3”上的 /data/nfs

到/autonfs 目录，挂载成功后在该目录创建 Gdskills_nfs 目录。

3、配置“云主机 4”为 nfs 客户端，按需挂载“云主机 3”上的 /data/backup 到 /backup 目录，保障挂载目录随时正常访问。

任务九、邮件服务配置（3 分）

1、在“云主机 3”中安装和配置 Postfix 邮件服务器。配置“云主机 1”的域名服务器负责完成域的邮件域名解析，实现区域内的邮件收发。

2、在邮件服务器中启用 SSL/TLS，使用“云主机 1”CA 服务器签名的证书。

3、在邮件服务器中创建用户 mail01 至 mail99 共 99 个用户，用户密码均为 Guangdong2025，创建邮件群发组，组名为 mailusers；将 mail01 至 mail100 用户都加入到 mailusers 群组中，并给 mailusers 群发一封邮件，主题为“Hello，Guangdong”，内容为“技能成才！”。

4、在邮件服务器中开启邮件过滤，要求拒绝接收主题中带有“A funny game”关键词的所有邮件，并登记为 virus mail。

任务十、磁盘配额限制配置（2 分）

1、在“云主机 3”中安装配置 quota 服务，将 HT3 卷挂载到“云主机 3”中，格式化为 ext4 文件系统，并开机自动挂载到“云主机 2”的/data/HT2 目录分区下,在根文件系统之后检查；创建 quotauser2 至 quotauser100 用户（用户名称连续不中断，共 99 个用户），密码为 Guangdong2025，同时隶属组 quotagrp；将 quotauser2 至 quotauser100 的所有 99 个用户的磁盘配额限制配置为软限制 100MB、硬限制 200MB。

2、在“云主机 3”中编写/opt/quota_warn.sh 的 shell 脚本,实现当任一 quotauser 用户超出磁盘限额值时，给 root 发送一份超额警告邮件，邮件主题为“磁盘限额通知”，内容为“警告: 用户 i 已经超出磁盘限额值！”（i 代表实际超出限额的用户）。在用户 quotauser3 中使用 dd 命令生成一个 270M 的 bigfile 文件，用以测试超警告邮件的发送。

任务十一、ISCSI 服务配置（2 分）

1、将 HT4-HT7 四个卷创建为一个具有热备盘的 RAID5，块设备名称为 md0，将最后一块磁盘设置为热备盘。

2、在“云主机 4”中安装配置 ISCSI 服务，磁盘名称为 disk0，服务端 IQN 名称为：iqn.2025-04.com.2025skills:server ， 客 户 端 IQN 名 称 为 ：

iqn.2025-04.com.2025skills:client。

3、在“云主机 5”中安装配置 ISCSI 客户端服务，通过 IQN 和 IP 地址查找并登录 ISCSI 服务器。客户端连接上后，将此磁盘进行分区，格式为 xfs 文件系统格式，系统开机联网后自动挂载到/ISCSI 目录下。

任务十二、数据库服务配置（5 分）

在“云主机 4”中安装配置 MariaDB 数据库,修改 MariaDB 数据库的 root 账号密码为“Guangdong2025”；添加 MySQL 用户 sqluser。

2、在数据库服务器中启用 TLS 加密协议，提高 MariaDB 服务器的安全性，加密算法使用 DHE-RSA-AES256-GCM-SHA384，采用 CA 服务器颁发私钥和证书。

3、创建数据库 skills_database，授权用户 sqluser 具有数据库 skills_database 的全部权限；在数据库 skills_database 中创建表 xsda 和 xscj，表结构定义如下表：

xsda 表			
名称	**类型**	**非空**	**备注**
ID	Int	是	主键
Name	varchar(10)	否	
Sex	char(2)	否	
Birthday	date	否	
Phone	varchar(20)	否	
Username	char(10)	是	唯一约束
Password	varchar(100)	是	

xscj 表			
名称	**类型**	**非空**	**备注**
ID	Int	是	主键

Course	char(10)	是	
Score	Int	是	

4、在 xsda 表中创建以下 2 条记录，并对密码字段使用 SHA2 进行加密存储：

(202501，张三，男，2005-1-1，13812345678，zhangsan,12345678),

(202502，李四，男，2005-1-2，13998765432，lisi,12345678)。

5、在 xscj 表中创建以下两条记录：

（202501，计算机基础，90），

（202502，网络操作系统，92）。

6、在 skills_database 数据库上定义一个触发器 xscj_update，当在 xscj 表中插入一条记录时，检查该记录的学号在 xsda 表中是否存在，若该记录的学号在 xsda 表中不存在，则不允许插入操作，错误代码为“45000”并提示“违背数据的一致性，不允许插入该数据！”。

7、为了保护个人数据的安全，创建一个 mask_phone 函数，当执行查询时，对手机号进行隐藏只显示前 3 位和后 4 位，中间用****代替。

任务十三、时间源服务配置（1 分）

1、在“云主机 5”上安装和配置 Chronyd 服务，搭建一个 NTP 服务；搭建一个本地时间源服务器，域名为 ntp.2025skills.com，仅允许“云主机 1”和“云主机 2”的网段来同步时间。

任务十四、服务器监控运维（4 分）

1、某企业私有云服务器（网络虚拟化系统实训平台模拟），你是一家 IT 公司的网络运行管理员，负责管理多台拥有 IPMI 功能的网络服务器。为了测试监控系统的告警功能，你需要在“云主机 6”中注入 IPMI 系统事件并验证系统事件日志是否能够被监控系统正确捕获。

（1）注入事件包括：电压关键下限告警、风扇关键上限告警。

（2）使用 ipmitool 命令查看命令行查看系统事件日志。

（3）测试结束后，清空日志，确保不会影响后续的监控任务

2、假设你是一名网络运行管理员，负责监控和管理公司内部的网络设备。你需要在“云主机 6”中使用 SNMP 协议从一台远程设备上获取 IPMI 设备的运行时间。设备 IP 地址为 172.16.1.250，读团体名为 GDSkills，写团体名为 ChinaSkills。

3、在“云主机 6”中安装并配置 RADIUS 服务器，统一为企业内部网络的网络设备提供统一的认证管理服务，只允许 IPMI 设备同网段的客户端访问 RADIUS 服务器。使用 Radius 用户登陆，并响应如下消息内容：″Hello,<用户名>″。

任务十五、服务器性能优化（3 分）

1、在“云主机 3”上编写/opt/checkhost.sh 的 shell 脚本，自动化实现 ping 云主机 1 至云主机 6 以测试连通性,连通成功输出“主机 $IP 在线”（$IP 代表主机地址），连通失败输出“主机 $IP 不在线”；在每天的 8：00 执行 checkhost.sh 脚本，并将执行后的结果自动发送到 mail01@2025skills.com 邮箱，邮件主题为“主机连通性测试结果”。

2、在“云主机 4”上编写/opt/backupDb.sh 脚本，实现对 skills_database 数据库的定时备份。要求如下：

配置 crontab 定时任务，每天凌晨 1 点自动对数据库进行备份。

备份文件应存储至/backup/目录。

备份文件名格式：database-YYYYMMDDHHMMSS.bak，其中 YYYYMMDDHHMMSS 为执行备份时的当前时间。

在“云主机 5”上编写/opt/createfile.py 的 python3 脚本，创建 20 个文件/opt/python/file00 至/opt/python/file19，如果文件存在，则删除后再创建；每个文件的内容同文件名，如 file00 文件的内容为“file00”。