

测试项目 – 试题

世界技能大赛网络系统管理项目

国家集训队阶段性考核

模块 A-Linux 环境

目 录

《测试项目》简介	3
介绍	3
登录所有虚拟机和设备:	3
系统环境要求:	3
项目和任务的描述	5
Part 1 – GZ2024.GD Domain	5
ROUTER1.GZ2024.GD	5
MANAGE.GZ2024.GD	6
DEVELOP.GZ2024.GD	7
Part 2 – DY2024.GZ Domain	8
ROUTER2.DY2024.GZ	8
SERVER1.DY2024.GZ	9
SERVER2.DY2024.GZ	10
SERVER3.DY2024.GZ	10
SERVER4.DY2024.GZ	11
SERVER5.DY2024.GZ	11
SERVER6.DY2024.GZ	12
SERVER7.DY2024.GZ	13
SERVER8.DY2024.GZ	13
Part3 – Public Internet Network	14
ISP	14
INET	14
REMOTE	14
所需的设备、机械、装置和材料	16
网络表	16
网络图	18

《测试项目》简介

以下是提交的所有《测试项目》提案中必须包含的章节或信息清单。

- 目录，包括组成《测试项目》的所有文件、图纸和照片的清单
- 介绍/概述
- 项目和任务的简短描述
- 选手须知
- 完成《测试项目》所需的设备、机械、装置和材料
- 《评分方案》（包括评估标准）
- 其他

介绍

此《测试项目》由以下文档/文件组成：

- 模块A-Linux-试题.docx

随着业务的不断增长，保障应用系统持续稳定性一直是信息技术的挑战。当事情变得复杂，现有系统的架构无法满足高性能、可扩展以及安全可靠的需求。Delix 公司决定处理这个问题，并雇佣你来对他们的基础设施进行现代化改造，强化和拓展。

所有的虚拟机都已经预安装了Debian Linux操作系统。你可以使用这些虚拟机来开发及测试你的工作。

登录所有虚拟机和设备：

用户名： root / skills

密码： GZSkills-2024

如果以下未特别说明，账号的密码均为“GZSkills-2024”（不含引号）。

系统环境要求：

Time zone: Asia/Shanghai

Locale: en_US.UTF-8

Keymap: us

所有主机按照网络表完成初始化设置。

当任务需要配置SSL或者TLS时，应该要隐藏所有客户端警告，当用户访问任何网页服务时，如果连接不安全，系统应自动将其重定向至安全连接。

请严格按照任务要求进行配置，不要安装和运行与题意不符的服务或程序，若题意未明确要求请使用默认设置(如服务端口)。

出于测试目的，所有主机都应该安装以下测试工具：curl, wget, lynx, nslookup, dig, ftp, lftp, showmount, smbclient, ssh, telnet, traceroute, ntpdate, lsof, nmap, mail, host

项目和任务的描述

Part 1 – GZ2024. GD Domain

ROUTER1.GZ2024.GD

Routing

- 在该服务器上开启路由转发功能
- 使用BGP协议作为公网的动态路由协议

NAT

- 使用nftables配置NAT：
 - 为GZ2024. GD域的所有主机配置PAT
 - 为服务配置端口转发
 - 为MANAGE. GZ2024. GD配置静态NAT。当它与公网通信时，它的IP地址需要被转换为213.110.3.10

Nftables

- 默认情况下，filter表中所有的链默认策略均为DROP
- 始终允许来自192.168.100.0/24、192.168.103.0/24、172.16.10.0/24、172.31.10.0/24网络的流量
- 来自MANAGE主机的所有流量中，应该只允许服务所需的流量通行
- 从internet网络发送到MANAGE主机的所有流量中，应该只允许服务所需的流量通行
- 可以ping其他任何主机，但不允许被ping

DHCP

- 在“GZ2024. GD”内部网络中为192.168.100.0/24网络的主机配置DHCP服务。
 - 使用192.168.100.151 – 199作为IP分配范围
 - 根据网络拓扑添加必要的网络选项
 - A和PTR记录应该自动更新

Site-to-Site VPN

- 配置GRE over IPsec VPN
 - 使用预共享密钥作为认证方式
 - 使用tun0作为接口的名称

MANAGE.GZ2024.GD

NTP

- 安装和配置chrony服务作为“GZ2024.GD”和“DY2024.GZ”区域的时间服务器
- 所有设备都应与其进行时间同步，在timedatectl中能够显示出时间同步的状态
- 最精准的时间源源自于顶级服务器INET

DNS

- 安装和配置bind作为“GZ2024.GD”区域的DNS服务器
 - 为GZ2024.GD域的所有服务器配置静态A记录
 - 创建反向区域并且添加PTR记录
 - 创建所有对外服务的静态A记录
 - 创建服务所需的CNAME记录
 - 创建邮件服务所需的MX记录
- 使用SERVER1.DY2024.GZ来配置转发器
- 配置INET作为根提示

Certificate Authority

- 配置根证书颁发机构
 - 使用者名称：C=CN, O=RCA, CN=GZ2024-CA
 - CA目录：/etc/ssl/rca
 - 证书以服务器的FQDN与扩展名(.key, .crt)命名
- 能够通过INET吊销列表服务器检测签发证书的有效性
- 本测试项目中所有应用所需的证书均由此根证书签发

OpenLDAP

- 安装和配置OpenLDAP服务器

- 根据附件：Linux-users添加用户对象
- 不要使用明文密码作为用户密码
- 禁止匿名用户来获取对象的信息

FreeRADIUS

- 安装和配置FreeRADIUS服务器
 - FreeRADIUS应能够从OpenLDAP数据库中获取账户信息作为使用
 - 使用“GZ2024-Radius”作为预共享密钥

E-Mail

- 安装和配置邮件服务器
 - 配置GZ2024.GD域的SMTPS和IMAPS/POP3S服务支持SSL/TLS，不允许非加密的连接
 - 所有用户都应该能够使用邮件服务自由地发送电子邮件
 - 使用OpenLDAP对象作为登录凭据
 - 使用证书颁发机构GZ2024-CA颁发的证书

Ansible

- 配置为Ansible control node
 - inventory文件为/etc/ansible/inventory.yml
 - 能够控制“DY2024.GZ”区域LAN1的SERVER3和SERVER4, LAN2的SERVER7和SERVER8执行自动化任务
 - playbook存储在/ansible/{task name}.yaml
 - 测试时使用ansible-playbook /ansible/linux.yml

DEVELOP.GZ2024.GD

Client

- 安装CA证书到Firefox和终端
- 确保OpenLDAP的对象用户能够登录到客户端
- 自动与NTP服务器同步时间
- 正确解析域名
- 访问Web应用

- 访问邮件服务
 - 使用evolution客户端
 - 配置为用户James@gz2024.gd的邮箱
 - 使用thunderbird客户端
 - 配置为用户zhangsan@dy2024.gz的邮箱
- 通过VSCode免密连接到MANAGE.GZ2024.GD控制节点，使其作为开发机进行开发

Part 2 – DY2024.GZ Domain

ROUTER2.DY2024.GZ

Routing

- 在该服务器上开启路由转发功能
- 使用BGP协议作为公网的动态路由协议

NAT

- 使用nftables配置NAT：
 - 为DY2024.GZ域的所有主机配置PAT
 - 为服务配置端口转发

Iptables

- 仅允许访问对外提供的服务
- 可以ping其他任何主机，但不允许被ping
- 允许VPN客户端访问LAN1网络
- 仅允许内网访问ssh，且连续访问3次不成功（每次只允许输入一次密码），则禁止访问1分钟
- INPUT, FORWARD默认策略为DROP

SSL/TLS Certificate

- 使用GZ2024-CA签名的证书
 - 国家(C)为“CN”
 - 公用名(CN)为“ROUTER2.DY2024.GZ”

- 组织(O)为“WSC2024”
- 证书存储在/etc/ssl/tls
- 证书以服务器的FQDN与扩展名(.key, .crt)命名

Site-to-Site VPN

- 配置GRE over IPSec VPN
 - 使用预共享密钥作为认证方式
 - 使用tun0作为接口的名称

Remote Access VPN

- 配置远程访问IKEv2 VPN
 - 使用RSA-SIG作为本地认证方式，使用EAP-MSCHAPv2作为远程认证方式。
 - 使用FreeRADIUS作为身份验证后端
 - 使用GZ2024-CA生成的证书，FQDN为“ravpn.dy2024.gz”
 - VPN客户端从192.168.103.0/24开始分配IP地址
 - VPN客户端连接成功后，应该能够使用gz2024.gd和dy2024.gz域的资源

SERVER1.DY2024.GZ

Ansible

- 配置为ansible managed node
 - 手动配置IP地址，安装SSH, Python后创建开机快照“ansible initialization”,以备评分时使用
- 执行自动化任务
 - task name : init
 - 设置主机名
 - 设置时区为Asia/Shanghai
 - task name : timesync
 - 配置与manage.gz2024.gd同步时间
 - task name : nameserver
 - 配置server2.dy2024.gz为nameserver
 - task name: dns

- 安装和配置bind9
 - 为dy2024. gz的服务提供内部解析

SERVER2.DY2024.GZ

Ansible

- 配置为ansible managed node
 - 手动配置IP地址，安装SSH，Python后创建开机快照“ansible initialization”，以备评分时使用
- 执行自动化任务
 - task name : init
 - 设置主机名
 - 设置时区为Asia/Shanghai
 - task name : timesync
 - 配置与manage. gz2024. gd同步时间
 - task name : nameserver
 - 配置server1. dy2024. gz为nameserver
 - task name: dns
 - 安装和配置bind9
 - 为server1. dy2024. gz的从服务器

SERVER3.DY2024.GZ

SSL/TLS Certificate

- 使用GZ2024-CA签名的证书
 - 国家(C)为“CN”
 - 公用名(CN)为“*. dy2024. gz”
 - 组织(O)为“WSC2024”
 - 证书存储在/etc/ssl/tls
 - 证书以服务器的FQDN与扩展名(. key, . crt)命名

Web

- 安装和配置Apache作为Web服务器
 - 全站启用https
 - 进程用户和组为webadmin
 - 使用http访问会自动跳转(301)到https
 - 访问dy2024.gz以及二级域名同样会自动跳转(301)到www.dy2024.gz
 - www.dy2024.gz
 - 设置网站根路径为/htdocs/html/
 - 在网站根路径创建首页index.html，内容为“The company's web site”
 - 记录访问日志
 - /var/log/nginx/www.dy2024.gz/access.log
 - 记录客户端IP，访问时间，访问资源

Mail

- 安装和配置Postfix, Dovecot
 - dy2024.gz后缀的邮箱
 - 邮箱用户:zhangsan, lisi
 - 启用SSL/TLS配置为SMTPS和IMAPS，不允许非加密的连接
 - 启用邮件群发功能
 - 向all@dy2024.gz邮箱发送邮件，所有人都能收到

SERVER4.DY2024.GZ

NFS Server

- 共享/website目录
- 只允许SREVER3.DY2024.GZ访问
- 存储www.dy2024.gz的网页文件
- 自动挂载到网站根目录

SERVER5.DY2024.GZ

Ansible

- 配置为ansible managed node
 - 手动配置IP地址，安装SSH，Python后创建开机快照“ansible initialization”，以备评分时使用
- 执行自动化任务
 - task name : init
 - 设置主机名
 - 设置时区为Asia/Shanghai
 - task name : timesync
 - 配置与manage.gz2024.gd同步时间
 - task name : nameserver
 - 配置server2.dy2024.gz为nameserver
 - task name: ftp
 - 安装和配置vsftpd
 - 使用域名ftp1.dy2024.gz
 - 配置挂载到/ftp目录
 - 通过Mysql的用户信息作为登录凭据
 - FTP用户：zhangfei、liubei
 - 用于www.dy2024.gz站点上传网页数据

SERVER6.DY2024.GZ

Ansible

- 配置为ansible managed node
 - 手动配置IP地址，安装SSH，Python后创建开机快照“ansible initialization”，以备评分时使用
- 执行自动化任务
 - task name : init
 - 设置主机名
 - 设置时区为Asia/Shanghai
 - task name : timesync

- 配置与manage.gz2024.gd同步时间
- task name : nameserver
 - 配置server2.dy2024.gz为nameserver
- task name: ftp
 - 安装和配置vsftpd
 - 使用域名ftp2.dy2024.gz
 - 配置挂载到/ftp目录
 - 通过Mysql的用户信息作为登录凭据
 - 用于www.dy2024.gz站点上传网页数据

SERVER7.DY2024.GZ

数据存储

- RAID、LVM
 - 添加4块1G物理磁盘，组成RAID5
 - 组号使用md0
 - 使用LVM管理磁盘阵列,命名为/dev/vg0/lv0
 - 开机自动挂载到/iSCSI目录
- iSCSI
 - 安装和配置tgt作为iSCSI服务
 - iqn名称为iqn.2024-01.gz.dy2024.iscsi:server7
 - 提供给SERVER4作为NFS服务的远程存储
 - 提供给SERVER5、SERVER6作为FTP根目录

SERVER8.DY2024.GZ

- Mariadb
 - 存储FTP用户数据
 - 数据库root用户仅能通过密码从本地登录
 - 仅dbadmin用户凭密码可从SERVER5、SERVER6登录
 - 创建库名ftpuser，表名users
 - 使用DES加密存储FTP用户的密码

Part3 – Public Internet Network

ISP

Routing

- 在该服务器上开启路由转发功能
- 使用BGP协议作为公网的动态路由协议

INET

DNS

- 安装和配置dnsmasq为公共互联网提供域名解析
 - 能够解析所有未知的域名
 - 所有未知域名均解析100.100.100.100
 - 为公共互联网区域的所有服务器配置静态A记录
 - 对于“GZ2024.GD”和“DY2024.GZ”域的解析应进行转发

CRL

- 为GZ2024-CA证书颁发机构配置吊销列表
 - 使用crl.internet.com作为站点名称
 - 提供给公共互联网协助验证证书有效性

NTP

- 安装和配置ntp服务作为时间服务器
 - 作为公共互联网中的顶级服务器
 - 只允许MANAGE.GZ2024.GD来同步时间

REMOTE

Client

- 安装CA证书到Firefox和终端
- 自动与NTP服务器同步时间
- 正确解析域名

- 访问Web应用
- 能够通过webmail的方式登录mail.gz2024.gd访问GZ2024.GD的邮件服务
- VPN访问测试

所需的设备、机械、装置和材料

网络表

NO.	HOSTNAME	IP ADDRESS	DESCRIPTION	SERVICES
1	REMOTE	213.110.3.210/25	外网客户端	test
2	INET	213.110.3.129/25	互联网服务提供者	ntp,dns,crl
3	ISP	213.110.3.62/26 213.110.3.126/26 213.110.3.254/25	公网路由	route
4	ROUTER1.GZ2024.GD	213.110.3.1/26 192.168.100.254/24	边界路由/网关	route,nftables
5	ROUTER2.DY2024.GZ	213.110.3.65/26 172.16.10.254/24 172.31.10.254/24	边界路由/网关	route,iptables
6	MANAGE.GZ2024.GD	192.168.100.110/24	内网应用服务器	control node
7	DEVELOP.GZ2024.GD	DHCP For ROUTER1	内网客户端	develop machine
8	SERVER1.DY2024.GZ	172.16.10.101/24	内网应用服务器	managed node
9	SERVER2.DY2024.GZ	172.16.10.102/24	内网应用服务器	managed node

10	SERVER3. DY2024. GZ	172. 16. 10. 103/24	内网应用服务器	web,mail
11	SERVER4. DY2024. GZ	172. 16. 10. 104/24	内网应用服务器	storage
12	SERVER5. DY2024. GZ	172. 31. 10. 101/24	内网应用服务器	managed node
13	SERVER6. DY2024. GZ	172. 31. 10. 102/24	内网应用服务器	managed node
14	SERVER7. DY2024. GZ	172. 31. 10. 103/24	内网存储服务器	Raid, iSCSI
15	SERVER8. DY2024. GZ	172. 31. 10. 104/24	内网存储服务器	Mariadb

网络图

