安全问题有：

http://192.10.27.91/es/	192.10.27.91	目录遍历	目录遍历	中危	通过修改配置文件，去除Web容器的文件目录索引功能。
http://192.10.27.91:8087,9870,8086,8084,9864	192.10.27.91	未授权访问	未授权访问	高危	添加访问权限或设置本地访问。
http://192.10.27.92:9095,9868,9864	192.10.27.92	未授权访问	未授权访问	高危	添加访问权限或设置本地访问。
http://192.10.27.93:8085	192.10.27.93	未授权访问	未授权访问	高危	添加访问权限或设置本地访问。
http://192.10.27.94:8001/#/Dashboards	192.10.27.94	未授权访问	未授权访问	高危	添加访问权限或设置本地访问。

1. http://192.10.27.91/es/
2. http://192.10.27.91:8087,9870,8086.8084.9864
3. http: //192.10.27.92:9095,9868,9864
4. http://192.10.27.93:8085
5. http://192.10.27.94:8001/#/Dashboards

处理方式

问题1

成因 ： 改路径下资源是在安装服务时，为了统一部署启用的httpd服务，安装完成后，已可不再使用.

处理方式: 直接停用

```
systemctl stop httpd //关闭
systemctl status httpd //inactive状态
```

问题2、3、4

成因：内部服务生成的应用的动态或静态端口

处理方式： 通过防火墙策略限制91、92、93的内部服务只能被94访问。

```
## 91/92/93

yum install firewalld

systemctl enable firewalld
firewall-cmd --zone=public --add-rich-rule 'rule family="ipv4" source
address="192.10.27.94" accept' --permanent
```

```
结果为 success,也可能是其它返回结果，不用管
firewall-cmd --zone=public --add-service ssh --permanent
结果为 success，也可能是其它返回结果，不用管
firewall-cmd --reload
结果为 success,也可能是其它返回结果，不用管

systemctl start firewalld
systemctl status firewalld
结果包含 active (running )
firewall-cmd --state
结果为 running
```

问题5

成因：演示用的静态资源

处理方式：停用

```
## 94服务器
 mv /data/services/nginx/config/hyl.conf /root
docker exec -it nginx nginx -s reload
```