使用harbor搭建私有仓库

Harbor项目是帮助用户迅速搭建一个企业级的registry 服务。

它以Docker公司开源的registry为基础，提供了管理UI, 基于角色的访问控制(Role Based Access Control)，AD/LDAP集成、以及审计日志(Audit logging) 等企业用户需求的功能，同时还原生支持中文。

1. 下载地址

https://github.com/vmware/harbor/releases

2.安装需求

- kernel 3.10+
- python 2.7+
- docker-engine1 1.10 +
- Docker Compose 1.6+

3. 安装docker compose

由于从github在线安装速度很慢，采用下载离线安装包的方式安装

```
#下载docker compose 安装包
wget
https://github.com/docker/compose/releases/download/1.8.1/docker-
compose-Linux-x86_64

chmod +x docker-compose-Linux-x86_64

mv docker-compose-Linux-x86_64 /usr/bin/docker-compose
```

4. 安装harbor说明

```
#下载harbor最新版本离线安装包
wget
https://github.com/vmware/harbor/releases/download/0.4.1/harbor-
offline-installer-0.4.1.tgz
```

```
tar -zxvf harbor.offline-installer-0.4.1.tgz

cd harbor/

vi harbor.cfg  修改hotsname，邮件等信息，修改`ui_url_protocol = https`
hostname: 用于访问UI和registry服务的主机名，必须是IP或者FQDN。！ 不要使用
localhost或者127.0.0.1
ui_url_protocol: http or https. Default is http,访问UI的协议和
token/notification service。如果启用Notary，该参数将被设置为https。
db_password: mysql数据库的root密码。
max_job_workers:  (default value is 3)最大工作副本数量，增大数值以分配更多
的任务副本，但是会增加network/CPU/IO资源的小号
customize_crt:（on or off. Default is on）是否生成证书，如果设
为on，prepare脚本创建新的root证书和私钥给registry登录使用。如果设置为off将使
用默认的root证书。
ssl_cert：nginx的SSL证书存放路径，只有访问协议为https时才会生效。
ssl_cert_key：nginx的SSL密钥存放路径，只有访问协议为https时才会生效。
secretkey_path：密钥存放路径
可选参数：
- email设置：email_server，email_server_port，email_username，
email_password，email_password，email_password
- harbor_admin_password:  admin密码，默认admin/Harbor12345
- auth_mode：认证模式，本地库(db_auth)或ldap（ldap_auth）
- ldap认证设置：ldap_url，ldap_searchdn，ldap_search_pwd，ldap_basedn，
ldap_filter，ldap_uid，ldap_scope，ldap_timeout
- self_registration:  （on/off）  用户是否可以自己注册，默认on
- token_expiration
- project_creation_restriction
- verify_remote_cert
```

配置后端存储（可选）

默认情况，Harbo将镜像存储在本地文件系统，通过修改`common/templates/registry/config.yml`配置文件的storage节点配置后端存储。参加docker的registry设置

5. 设置ssl认证

```
mkdir -p /etc/docker/certs.d/$servername/

生成证书

openssl req -newkey rsa:4096 -nodes -sha256 -keyout ca.key -x509 -
days 3650 -out ca.crt ##"输入国家名，省份，城市，组织名，组织单元名,主机
```

```
名"主机名要和harbor配置文件中的一样

openssl req -newkey rsa:4096 -nodes -sha256 -keyout
docker.yyk.com.key -out docker.yyk.com.csr  ##"输入国家名，省份，城市，
组织名，组织单元名"主机名要和harbor配置文件中的一样，要和ca的内容一样

#如果服务器没有域名需要执行下面的操作
echo subjectAltName = IP:registry host IP > extfile.cnf

#生成证书
openssl x509 -req -days 3650 -in docker.yyk.com.csr -CA ca.crt -
CAkey ca.key -CAcreateserial -out docker.yyk.com.crt -extfile
extfile.cnf

#复制证书和私钥
cp docker.yeeyk.com.crt  docker.yeeyk.com.key /data/cert/

#修改harbor.cfg
ssl_cert = /data/cert/docker.yeeyk.com.crt
ssl_cert_key = /data/cert/docker.yeeyk.com.key

#生成配置文件
./prepare

#安装
 ./install.sh

#把ca证书复制到/etc/docker/certs.d/$server/下
cp ca.crt /etc/docker/certs.d/$server/


#重启
docker-compose stop
docker-compose rm
##docker-compose down相当于上面两部
docker-compose up -d
```

登录管理界面 http://ip 账号 admin 默认密码： Harbor12345