Private docker registry

在開始前有幾個重點:

每一台都可這樣設定

先設domain /etc/hosts

127.0.0.1 localhost

127.0.1.1 dev-rancher-server-26

10.10.1.26 dev-rancher-server-26.hubdomain dev-rancher-server-26

10.10.1.21 uat-rancher-server-21.uatdomain

10.10.1.27 pro-rancher-server-27.prodomain

/etc/hostname

dev-rancher-server-26.hubdomain

# 部署私有Docker Registry

Docker在2015年推出了[distribution](https://github.com/docker/distribution)項目，即Docker Registry 2。相比於[old registry](https://github.com/docker/docker-registry)，Registry 2使用[Go](http://tonybai.com/tag/golang)實現，在安全性、性能方面均有大幅改進 Registry設計了全新的Rest API，並且在image存儲格式等方面不再兼容於old Registry。去年8月份，docker官方hub使用Registriy 2.1替代了原先的old Registry。如果你要與Registry2交互，你的Docker版本至少要是Docker 1.6。

1. Insecure Registry

Registry的文檔還是相對詳盡的。在文檔中，我們找到了[Insecure Registry](https://github.com/docker/distribution/blob/master/docs/insecure.md)，即接收plain http訪問的Registry的配置和使用方法，雖然這不是官方推薦的。

實際上對於我們內部網絡而言，Insecure Registry基本能滿足需求，部署過程也避免了secure registry的那些繁瑣步驟，比如製作和部署證書等

修改/etc/default/docker Registry server上的Docker daemon的配置，為DOCKER\_OPTS增加–insecure-registry：

DOCKER\_OPTS="--insecure-registry dev-rancher-server-26.hubdomain:5000

重啟Docker Daemon，啟動Registry容器：

$ sudo service docker restart

$ sudo docker run -d -p 5000:5000 -v `pwd`/data:/var/lib/registry --restart=always --name registry registry:2

嘗試再次Push image:

docker tag ubuntu:latest dev-rancher-server-26.hubdomain:5000/nexcom/ubuntu:latest

$ docker push dev-rancher-server-26.hubdomain:5000/nexcom/ubuntu

在Private Registry2中查看或檢索Repository或images，[將不能用docker search](https://github.com/docker/distribution/blob/master/ROADMAP.md#indexing-search-and-discovery)：

$ docker search dev-rancher-server-26.hubdomain:5000/nexcom/ubuntu

Error response from daemon: Unexpected status code 404

但通過v2版本的API，我們可以實現相同目的：

$curl http://dev-rancher-server-26.hubdomain:5000/v2/\_catalog

$curl http:// dev-rancher-server-26.hubdomain:5000/v2/nexcom/ubuntu /tags/list

在其他主機上，我們嘗試pull

如果採用insecure registry的模式，那麼所有與Registry交互的主機上的Docker Daemon都要配置：–insecure-registry選項。我們按照上面的配置方法，修改/etc/default/docker，重啟Docker daemon，再執行pull/push就會得到正確的結果：

1. Secure Registry

Docker官方是推薦你採用Secure Registry的工作模式的，即transport採用tls。這樣我們就需要為Registry配置tls所需的key和crt文件了

我們首先清理一下環境，將上面的Insecure Registry停掉並rm掉；將各台主機上Docker Daemon的DOCKER\_OPTS配置中的–insecure-registry去掉，並重啟Docker Daemon

1. 製作自簽署證書

$ openssl req -newkey rsa:2048 -nodes -sha256 -keyout certs/domain.key -x509 -days 365 -out certs/domain.crt

Generating a 2048 bit RSA private key ..............+++ ............................................+++ writing new private key to 'certs/domain.key' ----- You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. ----- Country Name (2 letter code) [AU]:CN

State or Province Name (full name) [Some-State]:Liaoning

Locality Name (eg, city) []:shenyang

Organization Name (eg, company) [Internet Widgits Pty Ltd]:foo Organizational Unit Name (eg, section) []:bar

Common Name (e.g. server FQDN or YOUR name) []:dev-rancher-server-26.hubdomain

Email Address []:bigwhite.cn@gmail.com

docker run -d -p 5000:5000 --restart=always --name registry -v `pwd`/data:/var/lib/registry -v `pwd`/certs:/certs -e REGISTRY\_HTTP\_TLS\_CERTIFICATE=/certs/domain.crt -e REGISTRY\_HTTP\_TLS\_KEY=/certs/domain.key registry:2

重新為ubuntu製作一個tag:

$docker tag ubuntu:latest dev-rancher-server-26.hubdomain:5000/nexcom/ubuntu:latest

Push到Registry:

$ docker push dev-rancher-server-26.hubdomain:5000/nexcom/ubuntu

The push refers to a repository [dev-rancher-server-26.hubdomain:5000/ nexcom/ubuntu] (len: 1) unable to ping registry endpoint….: x509: certificate signed by unknown authority

從錯誤日誌來看，docker client認為server傳輸過來的證書的簽署方是一個unknown authority（未知的CA），因此驗證失敗。我們需要讓docker client安裝我們的CA證書：

$ sudo mkdir -p /etc/docker/certs.d/ dev-rancher-server-26.hubdomain:5000 $ sudo cp certs/domain.crt /etc/docker/certs.d/ dev-rancher-server-26.hubdomain:5000/ca.crt

$ sudo service docker restart重启Docker Daemon

再執行Push

1. 外部 pull registry

我們換其他機器試試訪問這個secure registry。根據之前的要求，我們照貓畫虎的修改一下hosts文件，安裝ca.cert，去除–insecure-registry選項，並重啟Docker daemon。之後嘗試從registry pull image：

把ca.cert copy 到每一台上

$ sudo mkdir -p /etc/docker/certs.d/ dev-rancher-server-26.hubdomain:5000 $ sudo cp certs/domain.crt /etc/docker/certs.d/ dev-rancher-server-26.hubdomain:5000/ca.crt

$ sudo service docker restart重启Docker Daemon

docker pull dev-rancher-server-26.hubdomain:5000/nexcom/Ubuntu

1. Registry鑑權管理

在Register server上，為Registry增加nexcom用戶，密碼nexcom123

$ mkdir auth $ docker run --entrypoint htpasswd registry:2 -Bbn nexcom nexcom123 > auth/htpasswd

$ ls auth：（之前需要停掉已有的Registry，並刪除之）

$ docker run -d -p 5000:5000 --restart=always --name registry -v `pwd`/auth:/auth -e "REGISTRY\_AUTH=htpasswd" -e "REGISTRY\_AUTH\_HTPASSWD\_REALM=Registry Realm" -e REGISTRY\_AUTH\_HTPASSWD\_PATH=/auth/htpasswd -v `pwd`/data:/var/lib/registry -v `pwd`/certs:/certs -e REGISTRY\_HTTP\_TLS\_CERTIFICATE=/certs/domain.crt -e REGISTRY\_HTTP\_TLS\_KEY=/certs/domain.key registry:2

我們嘗試push image到Registry：

docker push dev-rancher-server-26.hubdomain:5000/nexcom/ubuntu

The push refers to a repository [dev-rancher-server-26.hubdomain:5000/nexcom/ubuntu] (len: 1) 65e4158d9625: Image push failed Head no basic auth credentials

錯誤信息提示：鑑權失敗。

執行docker login:

$docker login dev-rancher-server-26.hubdomain:5000

再push image到Registry：

前面提到過，通過V2版Rest API可以查詢Repository和images：

curl --cacert /home/danny/docker\_secure\_registry/certs/domain.crt --basic --user nexcom:nexcom123 https://dev-rancher-server-26.hubdomain:5000/v2/\_catalog

{"repositories":["test/ubuntu"]}

#### **Connecting to docker registry with basic authentication and self-signed certificate**

docker run -it -d --restart=unless-stopped -p 8081:8080 --name registry-web --link registry -e REGISTRY\_URL=https://registry:5000/v2 -e REGISTRY\_TRUST\_ANY\_SSL=true -e REGISTRY\_BASIC\_AUTH="bmV4Y29tOm5leGNvbTEyMw==" -e REGISTRY\_NAME=dev-rancher-server-26.hubdomain:5000 -d hyper/docker-registry-web