UNIVERSITAT ROVIRA i VIRGILI

CLOUDLAB

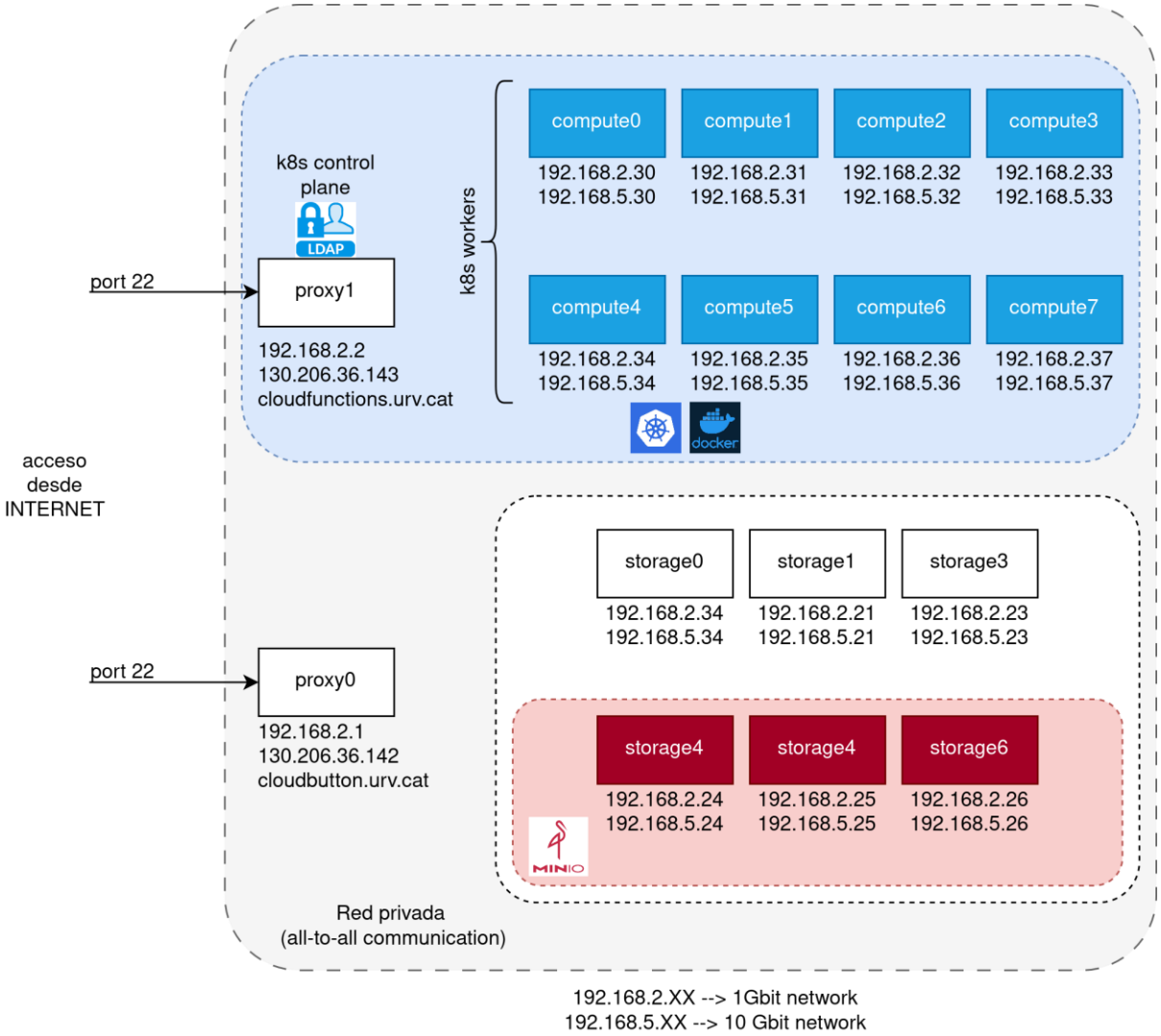
Cloud and Distributed Systems Lab

Manual de primera conexión al rack

Versión	Fecha	Descripción
1.0	20/10/2023	Configuración desde cero de todas las máquinas (ubuntu 22.04 + OpenSSH) K8s cluster configurado Docker en compute nodes + proxies Minio distribuido en storage{4,5,6} LDAP para la gestión de usuarios

Estructura del rack

En la siguiente imagen podemos observar de manera muy gráfica el cluster:



- Tenemos dos puertas de acceso (proxy0 y proxy1) a las que solamente se puede acceder desde internet por el puerto 22 (ssh).

- Existe un grupo de nodos llamados “computeX”. Su misión es ejecutar las cargas de trabajo necesarias.

- El grupo de nodos llamado “storageX” tiene como misión el almacenamiento de datos.

Primera conexión al rack

Para poder utilizar el rack, por favor ponerse en contacto con enrique.molina@urv.cat o aitor.arjona@urv.cat y solicitar un nuevo usuario. Debe enviar la clave pública, ya que el acceso a los proxies del rack sólo será permitido por verificación de clave ssh:

Desde su terminal, ejecute:

```
ssh <username>@cloudfunctions.urv.cat
```

Ya está dentro del proxy1.

Ahora, usted probablemente quiera acceder a más nodos del rack via ssh. Para poder acceder, ejecute el script

```
./init_ssh.sh
```

E introduzca su contraseña de usuario cuando sea solicitada. Se generará un par de claves, y se copiará la clave pública a todos los servidores ssh de la red. Para comprobar que ha tenido éxito, acceda a algún nodo via ssh; por ejemplo:

```
ssh compute7
```

Dentro de la red privada, podrá acceder entre hosts de manera libre (están conectados todos con todos).

Cambio de contraseña

La contraseña que se le proporcionará deberá ser cambiada por usted tras realizar la primera conexión al rack. Para ello, ejecute en su terminal

```
passwd
```

Y cree una nueva contraseña.

Comprobación de Docker

Para comprobar que usted tiene suficientes permisos de uso de docker, puede ejecutar:

```
docker run hello-world
```

Y ver si la comanda tiene éxito.

Su usuario habrá sido agregado al grupo de docker en10 todos los hosts que lo tengan instalado, así que debería poder utilizar docker en todas las máquinas que lo tengan instalado.

Comprobación de Kubernetes

Usted podrá usar kubernetes desde su usuario. Verifique que desde el proxy1 puede acceder a la API de k8s ejecutando:

```
kubectl get nodes
```

Al crear su usuario, la config de k8s ha sido clonada en su directorio de usuario para que pueda utilizar kubernetes.

Conexión con Minio

Para conectar con el servidor de Minio, los datos necesarios son especificados a continuación:

- SERVIDOR MINIO
  - http://storage4-10Gbit:9000 (http://192.168.2.24:9000)
  - User (or access_key_id): lab144
  - Password (or secret_access_key): astl1a4b4
- PANEL ADMIN WEB
  - http://storage4-10Gbit:9001
  - User (or access_key_id): lab144
  - Password (or secret_access_key): astl1a4b4

Lo superior funciona si accede dentro de la red privada. Si quiere conectarse desde fuera, tenga en cuenta que deberá configurar un túnel SSH (explicado más adelante).

Establecer un túnel SSH

Quizá en algún momento usted quiera conectarse desde su PC (fuera de la red privada del rack) con algún servicio del rack. Imagine que desea entrar al panel web de Minio desde su PC. Para poder acceder a él desde su PC, creara un túnel ssh:

```
ssh -N -L 44444:storage4-10Gbit:9001<username>@cloudfunctions.urv.cat
```

Y accederá al servidor web en su navegador a través de http://localhost:44444 (habrá establecido un túnel seguro entre el puerto 44444 de su localhost y el puerto 9001 de storage4).

Utilice túneles ssh para acceder a los servicios (servidos en puertos) del rack.

Permisos de usuario

El usuario creado para usted no cuenta con permisos de superusuario. Usted podrá realizar con normalidad la mayoría de sus acciones sin estos permisos (uso de docker+kubernetes+minio..., despliegues, ejecución de workloads...)

En caso de que necesite elevar sus permisos, por favor, póngase en contacto con un administrador.

Entrar al dashboard de Kubernetes

Para entrar al dashboard de kubernetes, tenemos que generar un token con la siguiente comanda:

```
kubectl -n kubernetes-dashboard create token admin-user
```

Y el token devuelvo será usado para iniciar sesión en el panel web.

Después, para poder acceder al dashboard desde nuestro PC personal, por favor, cree un túnel ssh. Tenga en cuenta que el proxy corre en el proxy1 en el puerto 8001.

Entre al dashboard desde su navegador en

http://localhost:<port>/api/v1/namespaces/kubernetes-dashboard/services/https:kubernetes-dashboard:/proxy/#/login

Clonar repositorios privados de Github

Recordamos que desde hace ya un tiempo, la auth mediante username & password con Github desde CLI fue deshabilitada.

Entonces, para clonar repositorios privados de Github, lo más probable es que usted piense en hacerlo mediante una conexión SSH. Este método NO funcionará, desde el rack parece que no se puede conectar con servidores SSH externos.

Para interaccionar con sus repos de Github, por favor utilice el método que usa Personal Access Tokens y HTTPS. Más información de cómo hacerlo en: https://www.wwwinsights.com/webinfra/git/clone-a-github-private-repository/. Siga este tutorial y resolverá sus problemas conectando con Github desde el rack.

Transferir archivo local a un nodo X

Actualmente los nodos del rack no comparten un sistema de ficheros común. Los archivos deben transferirse a cada nodo individualmente.

La siguiente comanda permite copiar un archivo al nodo computeX sin necesidad de copiarlo previamente al nodo proxy1.

```
scp -J USER_NAME@cloudfunctions.urv.cat FILE_PATH USER_NAME@computeX:DEST_PATH
```

Para evitar poner cada vez el parametro -J, se puede añadir lo siguiente al fichero de configuración de ssh (/etc/ssh/ssh_config o /home/stepii/.ssh/config):

```
Host compute*
  ProxyJump cloudfunctions.urv.cat
```