Pràctiques

Pràctica-1: Desplegament al cloud

Desplegar al Cloud, per exemple a AWS EC2 el servidor LDAP i localment desplegar un contenidor PAM. Configurar-lo per tal de poder autenticar usuaris de LDAP usant el servidor al cloud.

Requirements:

- Iniciar una AMI al Cloud de AWS EC2 i assignar-li el nom *f322hisix*.
- Desplegar al cloud el *servidor LDAP* i un container de la imatge *Portainer* usant un Docker-compose.
- Configurar un *security-wizard* anomenat *ssh-ldap-portainer* que permeti l'accés a aquests tres serveis.
- Desplegar localment un host PAM que permeti autenticació LDAP, per exemple edtasixm06/pam20:auth.
- Configurar interactivament el container PAM modificant el /etc/hosts per indicar l'adreça pública IP de la AMI del Cloud.
- Verificar que el host PAM permet iniciar sessió a usuaris locals i a usuaris de LDAP.
- Verificar que es pot accedir al servei de monitorització de Docker Portainer.

Pràctica-2: Personalització del Cloud

Aquesta pràctica és una continuació de la pràctica anterior.

1. Generar una imatge AMI pròpia basada en la AMI de la pràctica anterior. Ha de tenir docker, docker-compose i git. Desar-la amb el nom *f32base*. Així es podran crear noves AMI basades en aquesta.

2. Assignar a la AMI de la pràctica-1 una adreça IP flotant. Consultar la documentació pròpia de AWS EC2 Floating IP per veure com es pot obtenir una adreça IP pública fixa per a un compte d'usuari. Un cop obtinguda l'adreça associar-la a la AMI *f322hisix*.

3. Modificar interactivament el container PAM (el /etc/hosts) per apuntar a la nova adreça IP pública del servidor LDAP.

Pràctica-3: Servei SSH al Cloud

Desplegar al Cloud amb Docker Compose un servidor LDAP, un servidor SSH i un Portainer. Cal permetre l'accés per ssh al container ssh (per un port dedicat) i iniciar sessió tant d'usuaris locals com d'usuaris LDAP.

Requeriments:

- Desplegar a la AMI *f322hisix* amb Docker Compose un servidor LDAP, SSH i Portainer.
- Verificar que el servei SSH del container es propaga al *port 2022* del host AMI.
- Modificar el security group *ssh-ldap-portainer* per permetre l'accés al port 2022.
- Desplegar locament un container host PAM (per exemple el *edtasixm06/pam20:auth*) i configurar-lo per accedir al servidor LDAP del cloud.
- Verificar que poden iniciar sessió local els usuaris unix locals i usuaris de LDAP.
- Verificar que es pot iniciar sessió remota contra el servidor SSH del cloud i iniciar sessions d'usuaris locals unix d'aquell host.
- Verificar que es poden iniciar sessions remotes contra el servidor SSH del cloud i iniciar sessions remotes d'usuaris de LDAP.
- Establir un accés SSH per *clau pública* d'un usuari local unix a un usuari remot.
- Establir un accés SSH per *clau pública* d'un usuari LDAP a un usuari remot.

Pràctica-4: Muntatge de homes via NFS

Implementar només per a usuaris unix locals que es munti dins del seu home una carpeta amb el seu propi nom amb el contingut del home del mateix usuari que hi ha al servidor SSH.

Així per exemple en un host PAM local en iniciar sessió l'usuari unix01 accedeix al seu home local (creat en crear l'usuari amb useradd) i dins d'aquest home es crea via *pam_mount* un directori amb el nom de l'usuari que munta per ssh el home de l'usuari en el servidor SSH. per tant tindrà /home/unix01/unix01, on aquest segon unix01 és un recurs de xarxa muntat per ssffs i que correspon al home de l'usuari en el servidor SSH.

Requeriments:

- Desplegar al cloud en una AMI de AWS EC2 anomenada *f32hisix* un servidor LDAP, SSH i Portainer usant Docker Compose.
- Desplegar localment una host PAM (per exemple edtasixm06/pam20:auth) i configurar l'accés al servidor SSH modificant el /etc/hosts.
- Configurar pam_mount per muntar *<u>només</u>* per als usuaris locals un recurs dins el seu home corresponent al seu directori home del servidor SSH. Aquest recurs cal muntar-lo via *sshfs*, ha d'estar dins el seu home i s'ha d'anomenar igual que l'usuari.
- *Trick*: un punt clau per al funcionament del muntatge sshfs desatès és que al fitxer *known_hosts* ja exietixi una entrada per al host destí, sinó es fa la pregunta interactiva del fingerprint i no funciona el muntatge.
- Verificar que els usuaris locals del host PAM poden iniciar sessió local i en fer-ho es munta dins el seu home un directori amb el seu nom que és un recurs sshfs.
- Verificar que en iniciar sessió local al host PAM els usuaris de LDAP no es munta el recurs sshfs.

Pràctica-5 Utilitats d'accés per Clau Pública

Hi ha múltiples entorns en que es pot realitzar l'accés via SSH amb Clau Pública, alguns d'ells ja són molt habituals, com els de Git i AWS EC2. En aquesta pràctica es repassen alguns d'aquests procediments.

1. Practicar l'accés al Git amb Clau Pública SSH.

2. Practicar l'accés a una AMI de AWS EC2 usant una Clau Pública SSH de les creades en l'entorn AWS.

3. Crear una parella de claus Pub/Priv SSH i incorporar-les a l'usuari per defecte d'una AMI. Accedir a la AMI no amb la parella de claus estàndard sinó amb la clau pròpia generada.

4. [opcional] Generar una Imatge AMI (base per a altres imatges) que incorpori per a l'usuari per defecte una clau pública propia. Desplegar una AMI basada en aquesta imatge però sense associar-la a cap de les claus de AWS. Verificar que es pot accedir a la AMI amb la clau pròpia.

5. Desplegar una AMI windows i realitzar el procés d'accés al windows amb *Remmina*. Observar el mecanisme de generació del password a través de la clau SSH.

6. En l'entorn de AWS EC2 incorporar una nova Public Key sense generar-la, sinó important-la. Important una de les claus que hem generat manualment. Es requereix openssl i l'acció d'obtenir manualment la part pública de la key.