AZTERKETA ERREPASOA

0. ARIKETA: https://www.siteground.es/kb/generar-clave-ssh-linux/

Gakoak sortu:

ssh-keygen -t rsa

Defektuz /home/USER/.shh karpetan sortuko dira, kontuz izenekin (beste gako batzuk badaude)

Gakoak ikusteko eta kopiatzeko (cd /home/USER/.ssh):

more id_rsa.pub

Agertzen den guztia kopiatu eta google cloud-era igo (compute engine, configuracion, metadatos, editar)

1. ARIKETA:

Konexioa egiteko: ssh -i id_rsa.pub user@konexioIp

Dena egin behar bada:

-Virtual Host eraikitzeko: https://www.digitalocean.com/community/tutorials/como-configurar-virtual-hosts-de-apache-en-ubuntu-16-04-es

-HTTPS berbidalketa eta SSL sinaketa https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-20-04

Index html aldatzeko:

sudo nano gzuazo

Conf artxiboa ikusteko (por si acaso):

sudo nano /etc/apache2/sites-available/labo4.conf

2. ARIKETA:

(la note del segundo link de la ariketa 2)

Ziurtagiri autofirmatu batek enkriptatuko du zerbitzariaren eta edozein bezeroren arteko komunikazioa. Hala ere, web-nabigatzaileetan eta sistema eragileetan sartutako konfiantza-ziurtagirien agintariek sinatu ez dutenez, erabiltzaileek ezin dute ziurtagiria erabili zerbitzariaren identitatea automatikoki baliozkotzeko. Ondorioz, erabiltzaileek segurtasun-akats bat ikusiko dute beren lekua bisitatzean.

Muga hori dela eta, ziurtagiri autofirmatuak ez dira egokiak publikoaren zerbitzurako produkzio ingurune baterako. Normalean, erabiltzaile bakar batek edo erabiltzaile-talde txiki batek erabiltzen

dituen zerbitzu ez-kritikoak probatzeko edo ziurtatzeko erabiltzen dira, eta komunikazio-kanal alternatiboen bidez ziurtagiriaren baliagarritasunean konfiantza ezar dezakete.

Produkziorako ziurtagiri-irtenbide egokiagoa lortzeko, begiratu bat Let's Encrypt ziurtagiri libreko agintaritzari. How To Secure Apacheren tutoretzan Let-en enkriptatze-ziurtagiri bat deskargatzen eta konfiguratzen ikas dezakezu, Ubuntu 20.04ko tutorialean Let's Encripta erabiliz.

Entender eso y explicar algo asi:
Nabigatzaileak dio konexioa ez dela pribatua zertifikatua guk sinatu dugulako eta ez zertifikazio autoritate batek, beraz, erabiltzaileek ezin dute ziurtagiria erabili zerbitzariaren identitatea automatikoki konprobatzeko.

Hau konpontzeko, zertifikazioa autoritateak sinatu beharko luke, adibidez, Let's Encrypt, honek doainik sinatuko luke SSL zertifikatua eta web orrialdea segurua izatera pasatuko litzateke.

3. ARIKETA:

Info: https://extassisnetwork.com/tutoriales/como-ejecutar-trabajos-cron-cada-5-10-o-15-minutos/

Cron irekitzeko (beharrezkoa bada):

crontab –e

Vi-ekin editatzeko: i sakatu

Vi-rekin editatzeari uzteko: esc sakatu

Vi-rekin egindako aldaketak gordetzeko: ZZ sakatu (mayuscula)

Vi-rekin ez bada, beti bezala, CTRL+X etc

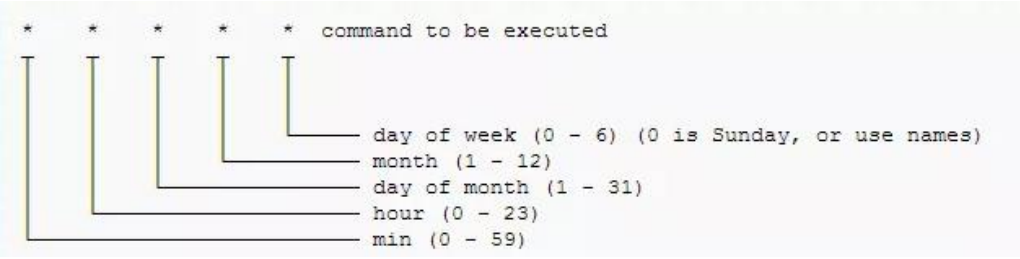
Crontab fixtategia:

#To define the time you can provide concrete values for minute (m), hour (h), day of month (dom), month (mon), and day of week (dow) or use '' in these fields (for 'any').*

#m h dom mon dow   command

*/5 = 0,5,10,15,20,25,30,35,40,45,50,55,

* * * * * path/script.sh



Script-ari baimenak eman behar badira:

chmod u+x script.sh

4. ARIKETA:

Kontuan hartu: /home/USER/Segurtasuna(/?)

-Slash-ekin: Segurtasuna karpetaren barruan dagoena kopiatzen da.

-Slash gabe: Segurtasuna karpeta kopiatzen da (eta barruan dagoena).

Segurtasun kopia osoa egiteko:

rsync –av <jatorri_path> <helmuga_path>

rsync -av /home/USER/Segurtasuna /var/tmp/Backups

Segurtasun kopia inkrementalak egiteko: (HEMEN / GABEEEE)

rsync -av --link-dest=<last_backup_konparatzekoa> <jatorri_path> <helmuga_path>

rsync -av --link-dest=/var/tmp/Backups/SegurtasunaLinkDest . /var/tmp/Backusp/gaur

“.” path- a /home/USER/Segurtasuna da

5. ARIKETA:

Konparatu behar dituzun path-ean (cd /nombre):

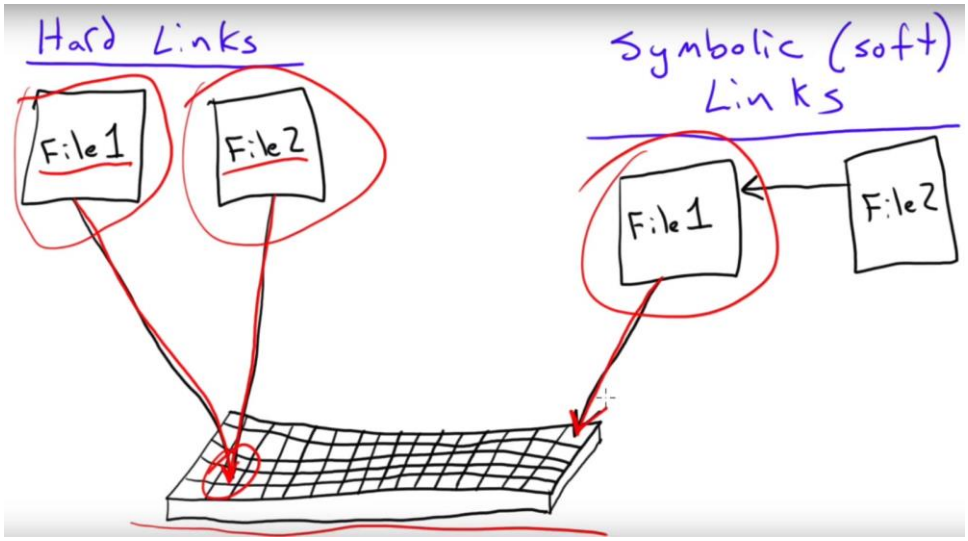
ls –ali edoo ls –li

ls –li bi karpetetan

Ikusi dezakegunez, errepikatzen diren i-nodo zenbakiak ditugu, honek esan nahi du fitxategi berdinak direla eta karpeta ezberdinetan esteka gogorra dutela.

(esto de abajo ns si hace falta)

Gainera, fitxategi bakoitzak dituen esteka kopurua ikusi dezakegu (baimenen ostean dagoen zenbakia), i-node berdina duten fitxategiek, kasu honetan, 2 esteka dituzte, hau da, fitxategi horietara bi esteka gogor apuntatzen dute.



6. ARIKETA

Ireki hardlink artxibo bat eta aldatu bertan edukia, gero ireki benetazko artxiboa bere direktorioan eta ikusi nola aldatu den.

Si cambias un artxibo del hardlink (gaur/A y bihar/A), el gaur/A por ejemplo, el bihar/A también se cambia:

Path1-eko A artxiboa editatzeko:

sudo nano path1/A

edo cd path1--> echo “aaa” > A

Ikusteko path2-ko A artxiboa ere aldatzen dela:

cd path2--> cat A

(agian egin behar da ls –li ikusteko aldaketa orduak eta hardlink-ak)