**Prerrequisitos**

* apt-get install chkconfig
* apt-get install openssh-server

**Obtener llaves privada y pública para evitar uso de contraseñas**

Para esta documentación se utilizó un usuario llamado osticket, en adelante cualquier línea que haga referencia al usuario osticket, tendrá que ser remplazada con el usuario de la máquina donde se esté replicando esta documentación.

**Cliente:**

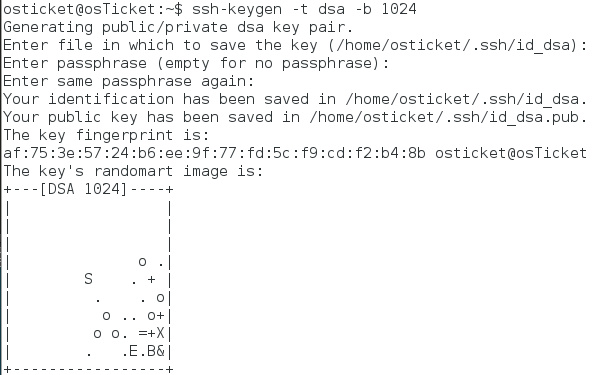
Generar nuestra llave pública y privada

* Comando: **ssh-keygen -t dsa -b 1024**

Nos pedirá una ubicación para guardar las llaves, si presionamos enter las guardará en el directorio por defecto: /home/osticket/.ssh.

Acto seguido, nos pedirá que ingresemos una frase para proteger las llaves.

Al finalizar, nos mostrará algo como lo siguiente:



**Servidor:**

Crearemos una carpeta dentro del home del usuario de donde se estará obteniendo el archivo, esta carpeta se llamará. shh (si es que no existe).

* Comando: **mkdir .ssh**

Asignamos los permisos necesarios para que solo pueda ser visto y editado por el dueño

* Comando: **chmod 700 .ssh**

Entramos a la carpeta /home/osticket/.ssh y crearemos un archivo de llaves autorizadas.

En este archivo estarán todas las llaves (contenido del archivo id\_dsa-pub de cada cliente) que tendrán acceso al servidor, una por línea.

* Comando: **touch authorized\_keys**

Asignamos los permisos necesarios

* Comando: **chmod 600 authorized\_keys**

**Cliente:**

Ahora tendremos que copiar el contenido de nuestra llave publica al archivo de authorized\_keys del servidor, para esto tenemos dos opciones.

Si no tenemos acceso al servidor: Dar el archivo al administrador del servidor y que él lo haga.

Si tenemos acceso al servidor:

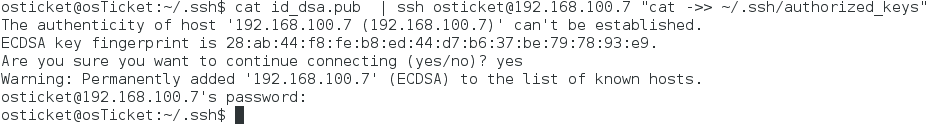
Posicionarnos en donde esta nuestra llave pública:

* Comando: **cd /home/osticket/.ssh**

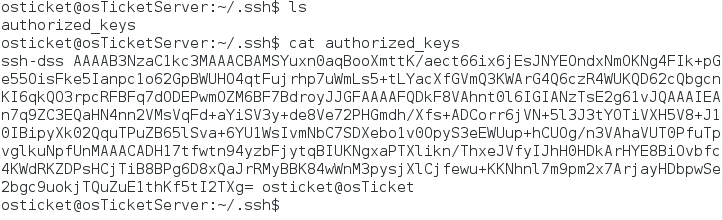
Y copiar el contenido al servidor (necesitaremos nombre de la cuenta, contraseña del servidor y dirección IP o nombre del equipo)

En este caso en vez del nombre del equipo utilizaremos su ip.

Comando: **cat id\_dsa.pub | ssh osticket@192.168.100.7 "cat - >> ~/.ssh/authorized\_keys"**



Con esto se habrá copiado el contenido de la llave publica del cliente al servidor, podemos comprobarlo en el servidor, viendo el archivo authorized\_keys.

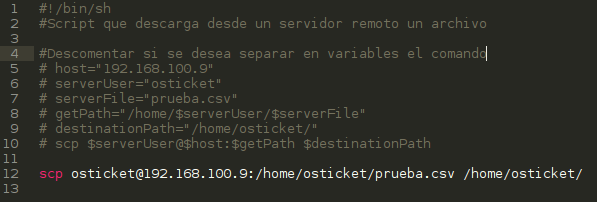


**Script para descargar archivo .csv de servidor remoto**

Es necesario que una vez al día se ejecute nuestro script para obtener el archivo de incidencias.

Para esto se ocupará el demonio cron.

Dentro del cliente, en la ruta **/etc/cron.dayli** se pondrá el siguiente script.



Al estar este archivo dentro de cron.dayli, se ejecutará una vez al día.

**Configuración final**

Para asegurar que todo se estará ejecutando de manera automática, es necesario asegurar que nuestro demonio cron este iniciándose al prender la computadora, para eso podemos modificar el servicio:

* Comando: **chkconfig --level 35 cron on**

Con –level 35 indicamos que se ejecutará siempre en los runes levels 3 y 5, activando el servicio cron.

**Configuración para una hora en especifico**

Si quisiéramos que nuestro servicio se ejecute en algún horario en específico, podríamos utilizar otra sintaxis.

Para ello, podemos utilizar un comando para editar las reglas de cron.

* Comando: **crontab -e**

Y al final agregar del archivo agregar la línea:

**30 2 \* \* \* /home/osticket/script.sh**

Para ver que reglas hay

* Comando: **crontab -l**

Esta línea ejecutara el script ubicado en /home/osticket/ llamado script.sh todos los días a las 2:30

Uso de cron:

\* \* \* \* \* /ruta/script.s

Cada asterisco tiene su función, respectivamente:

* Cada minuto
* De cada hora
* De cada día del mes
* De cada mes
* De cada día de la semana

Ruta -> Donde está ubicado el script

Script -> Script que se ejecutara