

Exemplo 4. Conexión SSH sen contrasinal

Exemplo 4. Conexión SSH sen contrasinal

ESCENARIO: Servidor SSH configurado do seguinte xeito (ver a seguinte ligazón: [Exemplo1](#) para configurar un Servidor SSH):

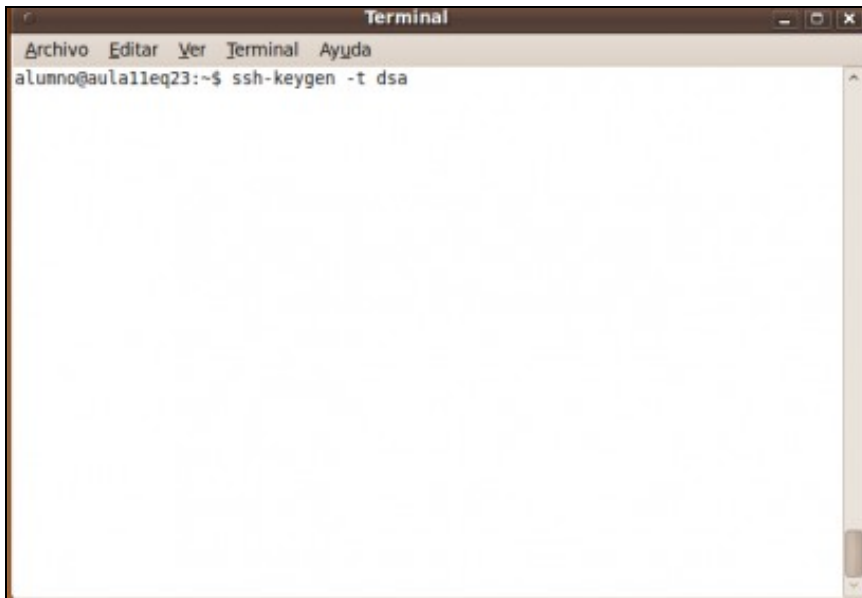
1. IP/MS: 192.168.120.100/24
2. Porto conexión: 22
3. Usuario/Contrasinal da conexión: root/toor

Configuración do Cliente da Conexión SSH

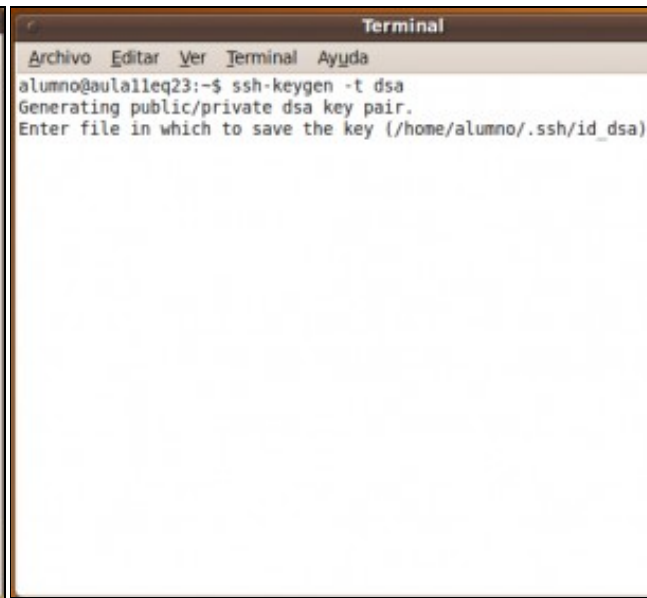
Para poder conectar mediante SSH sen contrasinal debemos crear certificados: chave pública e chave privada. Así:

1. O certificado de **chave pública** é o que debe posuir o **Servidor SSH**
2. O certificado de **chave privada** é o que debe posuir o **Cliente da conexión SSH**.

Proceder do seguinte xeito:



```
Terminal
Archivo  Editar  Ver  Terminal  Ayuda
alumno@aulalleg23:~$ ssh-keygen -t dsa
```



```
Terminal
Archivo  Editar  Ver  Terminal  Ayuda
alumno@aulalleg23:~$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/alumno/.ssh/id_dsa)
```

a. Crear un par de claves: pública e privada.

No comando emprégase o algoritmo de cifrado **dsa** (**D**igital **S**ignature **A**lgorithm), que por defecto a non ser que o modifiquemos co parámetro **-b n°_bits** é de **1024bits**.

```
Terminal
Archivo Editar Ver Terminal Ayuda
alumno@aula11eq23:~$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/alumno/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

b. Elixir o cartafol onde gardar as claves.

Pulsamos **Enter** para deixar por defecto o cartafol **.ssh/id_dsa** deno usuario: **/home/alumno**

```
Terminal
Archivo Editar Ver Terminal Ayuda
alumno@aula11eq23:~$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/alumno/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/alumno/.ssh/id_dsa
Your public key has been saved in /home/alumno/.ssh/id_dsa.pub
The key fingerprint is:
46:51:32:2b:b1:a6:4b:9d:22:b0:c9:7e:43:9c:81:53 alumno@aula11eq23
The key's randomart image is:
+--[ DSA 1024]-----+
| E . +.. |
| o o = |
|.o . + o |
|. +o o+ + |
|o..++ o S |
|. .o o . |
|. o. |
|. . |
+-----+
alumno@aula11eq23:~$
```

c. Passphrase nulo. Se aquí pomos un contrasinal, frase ou similar, cando queiramos conectarnos ao **Servidor SSH** en vez de pedir o contrasinal do usuario da conexión pedirá iste **passphrase**, mais como cando queremos conectarnos queremos facelo de forma directa sen petición de contrasinal ou passphrase, entón **pulsamos 2 veces Enter** para que a conexión se faga sen contrasinal.

d. Chave pública e privada creadas. Fingerprint. Creáronse no cindicado (ver imaxe b.) a **clave privada id_dsa** e a **clave pública**. Tamén creouse o **fingerprint da chave pública**, e dicir, a **identificación da chave pública correspondente ao usuario alumno do equipo cl**

```
Terminal
Archivo Editar Ver Terminal Ayuda
alumno@aula11eq23:~$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/alumno/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/alumno/.ssh/id_dsa.
Your public key has been saved in /home/alumno/.ssh/id_dsa.pub.
The key fingerprint is:
46:51:32:2b:b1:a6:4b:9d:22:b0:c9:7e:43:9c:81:53 alumno@aula11eq23
The key's randomart image is:
+--[ DSA 1024]-----+
| E . +.. |
| o o = |
|.o . + o |
|. +o o+ + |
|o..++ o S |
|. .o o . |
|. o. |
|. . |
+-----+
alumno@aula11eq23:~$ ssh-copy-id -i .ssh/id_dsa.pub root@192.168.120.100
```

```
Terminal
Archivo Editar Ver Terminal Ayuda
alumno@aula11eq23:~$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/alumno/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/alumno/.ssh/id_dsa
Your public key has been saved in /home/alumno/.ssh/id_dsa.pub
The key fingerprint is:
46:51:32:2b:b1:a6:4b:9d:22:b0:c9:7e:43:9c:81:53 alumno@aula11eq23
The key's randomart image is:
+--[ DSA 1024]-----+
| E . +.. |
| o o = |
|.o . + o |
|. +o o+ + |
|o..++ o S |
|. .o o . |
|. o. |
|. . |
+-----+
alumno@aula11eq23:~$ ssh-copy-id -i .ssh/id_dsa.pub root@192.168.120.100
Password:
```

e. Copia da chave pública ao Servidor SSH. Para poder establecer a conexión sen contrasinal enviamos unha copia da chave pública ao Servidor SSH. Soamente será posible establecer unha conexión sen contrasinal se posuimos a parella desa chave pública, que non é outra que a chave privada, polo cal, nunca deberíamos desprendernos da chave privada, xa que sen ela a conexión non sería posible ou outro usuario podería suplantarnos no caso de facerse coa chave privada.

```

Terminal
Archivo Editar Ver Terminal Ayuda
The key fingerprint is:
46:51:32:2b:b1:a6:4b:9d:22:b0:c9:7e:43:9c:81:53 alumno@aula11eq23
The key's randomart image is:
+--[ DSA 1024]-----+
|  E . +.. |
|  o  o =  |
|.o . + o  |
|. +o o+ +  |
|o..++ o S  |
|. .o o .   |
|. o.       |
|. .        |
+-----+
alumno@aula11eq23:~$ ssh-copy-id -i .ssh/id_dsa.pub root@192.168.120.100
Password:
Now try logging into the machine, with "ssh 'root@192.168.120.100'", and check i
n:

.ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
alumno@aula11eq23:~$

```

g. Chave pública copiada.

f. Password usuario root: toor. Como aínda non temos copiada a chave pública do usuario root, a conexión pídese o contrasinal do usuario co cal queremos conectar. A password de root é toor.

Agora a conexión sen contrasinal será posible por alumno na máquina Servidor SSH, sendo unha vez establecida o usuario root, con todos os permisos de root na máquina Servidor SSH.

```

Terminal
Archivo Editar Ver Terminal Ayuda
The key fingerprint is:
46:51:32:2b:b1:a6:4b:9d:22:b0:c9:7e:43:9c:81:53 alumno@aula11eq23
The key's randomart image is:
+--[ DSA 1024]-----+
|  E . +.. |
|  o  o =  |
|.o . + o  |
|. +o o+ +  |
|o..++ o S  |
|. .o o .   |
|. o.       |
|. .        |
+-----+
alumno@aula11eq23:~$ ssh-copy-id -i .ssh/id_dsa.pub root@192.168.120.100
Password:
Now try logging into the machine, with "ssh 'root@192.168.120.100'", and check i
n:

.ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
alumno@aula11eq23:~$ ssh root@192.168.120.100

```

h. Conectando ao Servidor SSH.

```

Terminal
Archivo Editar Ver Terminal Ayuda
The key's randomart image is:
+--[ DSA 1024]-----+
|  E . +.. |
|  o  o =  |
|.o . + o  |
|. +o o+ +  |
|o..++ o S  |
|. .o o .   |
|. o.       |
|. .        |
+-----+
alumno@aula11eq23:~$ ssh-copy-id -i .ssh/id_dsa.pub root@192.168.120.100
Password:
Now try logging into the machine, with "ssh 'root@192.168.120.100'", and check i
n:

.ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
alumno@aula11eq23:~$ ssh root@192.168.120.100
Last login: Sat Apr 24 14:27:41 UTC 2010 from 192.168.120.200 on ssh
root@sysresccd /root %

```

i. **Conexión establecida sen contrasinal**

--ricardofc [26/04/10]