Tabla 10.2 Opciones de la línea de comandos de configure *(continuación)*

Opción	Función
--without-idea	Especifica que ssh debe crearse sin compatibilidad con IDEA. *International Data Encryption Algorithm* (IDEA) es un eficaz algoritmo de cifrado de bloques que funciona con una clave de 128 bits y cifra los datos más rápidamente que DES y es mucho más seguro.
--without-rsh	Especifica que ssh no debe utilizar nunca rsh.
--with-path=PATH	Especifica la ruta en que entra un usuario cuando inicia la sesión con el cliente ssh (de forma predeterminada, los usuarios entran en su directorio inicial).
--with-securid[=PATH]	Especifica que ssh debe crearse con compatibilidad con la tarjeta Security Dynamics SecurID.
--with-socks	Especifica que ssh debe crearse con compatibilidad con *firewalls* SOCKS.
--with-socks4	Especifica que ssh debe crearse con compatibilidad con *firewalls* SOCKS, versión 4.
--with-socks5	Especifica que ssh debe crearse con compatibilidad con *firewalls* SOCKS, versión 5.
--with-tis[=DIR]	Especifica que ssh debe crearse con compatibilidad con el servidor de autenticación de Trusted Information Systems.
--with-x	Agrega compatibilidad con X.

Configuración de servidores ssh

Tras crear ssh, el siguiente paso es verificar (o cambiar si fuera necesario) las opciones de los archivos de configuración de ssh. Dichos archivos son:

- /etc.sshd_config (el archivo de configuración del servidor ssh).
- /etc/ssh_config (el archivo de configuración del cliente ssh).

/etc/sshd_config: el archivo de configuración del servidor ssh

/etc/sshd_config: es el archivo de configuración del servidor ssh. De forma predeterminada, este archivo es:

```
# This is ssh server systemwide configuration file.
Port 22
ListenAddress 0.0.0.0
```

```
HostKey /etc/ssh_host_key
RandomSeed /etc/ssh_random_seed
ServerKeyBits 768
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin yes
IgnoreRhosts no
StrictModes yes
QuietMode no
X11Forwarding yes
X11DisplayOffset 10
FascistLogging no
PrintMotd yes
KeepAlive yes
SyslogFacility DAEMON
RhostsAuthentication no
RhostsRSAAuthentication yes
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords yes
UseLogin no
# CheckMail no
# PidFile /u/zappa/.ssh/pid
# AllowHosts *.our.com friend.other.com
# DenyHosts lowsecurity.theirs.com *.evil.org evil.org
# Umask 022
# SilentDeny yes
```

La Tabla 10.3 muestra estas opciones y otras, y explica sus funciones.

Tabla 10.3 Opciones de /etc/sshd_config

Opción	Función
AllowGroups [grupos]	Esta opción se establece para controlar los grupos que pueden acceder a los servicios de ssh (ejemplo: AllowGroups sysadmin accounting). Los grupos se pueden especificar de forma explícita o utilizando comodines. Separe los *hosts* con espacios en blanco, no mediante comas.
AllowHosts [hosts]	Esta opción se establece para controlar los *hosts* que pueden acceder a los servicios de ssh (ejemplo: AllowHosts shell.ourcompany.net). Los *hosts* se pueden especificar de forma explícita o utilizando comodines y por nombre de *host* o dirección IP. Separe los *hosts* con espacios en blanco, no mediante comas.

Tabla 10.3 Opciones de /etc/sshd_config *(continuación)*

Opción	Función
AllowSHosts [hosts]	Esta opción se utiliza para especificar los *hosts* de .shosts o .rhosts que pueden acceder a los servicios de sshd. Los *hosts* se pueden especificar de forma explícita o utilizando comodines y por nombre de *host* o dirección IP. Separe los *hosts* con espacios en blanco, no mediante comas.
AllowTCPForwarding	Esta opción se utiliza para especificar si se permite el envío de TCP. De forma predeterminada, el valor de AllowTCPForwarding es yes.
CheckMail [yes|no]	Esta opción se utiliza para especificar si sshd debe notificar a los usuarios al iniciar la sesión que han recibido correo electrónico (no suele ser necesario, ya que la *shell* ya lo hace). El valor predeterminado (si esta opción se especifica sin ningún valor) es yes.
DenyGroups [grupos]	Esta opción se utiliza para controlar los grupos que pueden acceder a los servicios de ssh (ejemplo: DenyGroups sysadmin accounting denegará el acceso a los grupos sysadmin y accounting). Los grupos se pueden especificar de forma explícita o utilizando comodines. Separe los grupos con espacios en blanco, no mediante comas.
DenyHosts [hosts]	Esta opción se utiliza para denegar a determinados *hosts* el acceso a los servicios de ssh (ejemplo: DenyHosts shell.ourcompany.net). Los *hosts* se pueden especificar de forma explícita o utilizando comodines y por nombre de *host* o dirección IP. Separe los *hosts* con espacios en blanco, no mediante comas.
FascistLogging [yes|no]	Esta opción se utiliza para especificar si sshd debe realizar un registro excesivo.
ForcedEmptyPasswdChange	Utilícela para que los nuevos usuarios tengan que cambiar su contraseña la primera vez que inician una sesión.
HostKey [archivo clave]	Defina esta opción para especificar la ubicación de la clave del host. El valor predeterminado es /etc/ssh_host_key. Esta opción no es necesario que se utilice, salvo que se desee un archivo clave que no sea el predeterminado (a menos que se vayan a utilizar varios archivos de configuración que se lean en momentos distintos).
IdleTimeout [tiempo]	Esta opción se establece para especificar el tiempo tras el que se interrumpen las conexiones inactivas. Dicho tiempo puede definirse en segundos, minutos, horas, días o semanas. La sintaxis es IdleTimeout -tiempo-tiempo de identificador. Por ejemplo, para definir tres horas como tiempo de espera, escriba: IdleTimeout -h 3.

Tabla 10.3 Opciones de /etc/sshd_config *(continuación)*

Opción	Función
IgnoreRhosts [yes|no]	Esta opción se utiliza para especificar si sshd lee archivos .rhosts.
IgnoreRootRhosts	Esta opción se utiliza para especificar si sshd va a utilizar entradas de .rhosts al autenticar *root*.
KeepAlive [yes|no]	Esta opción se utiliza para especificar si sshd debe enviar a los clientes mensajes de que la conexión sigue viva.
LoginGraceTime [time]	Esta opción se define para controlar el tiempo que tardará el servidor en terminar la sesión de un usuario tras una petición de conexión si dicho usuario no consigue iniciar la sesión. Este tiempo se especifica en segundos (el valor predeterminado es 600).
PermitEmptyPasswords	Esta opción se utiliza para especificar si sshd va a permitir a los usuarios iniciar la sesión con una contraseña nula.
PermitRootLogin	Esta opción se utiliza para especificar si *root* puede iniciar la sesión con ssh y, en caso afirmativo, si se utiliza la autenticación de contraseña.
PrintMotd [yes|no]	Esta opción se define para especificar si sshd debe imprimir el mensaje del día la primera vez que los usuarios inician una sesión.
RhostsAuthentication	Esta opción se utiliza para especificar si se puede utilizar solamente la autenticación de rhosts. A menos que exista una buena razón para hacerlo, esta opción no debe utilizarse, ya que la autenticación de rhosts no es segura.
RhostsRSAAuthentication	Esta opción se define para especificar si sshd debe utilizar la autenticación de rhosts y RSA conjuntamente.
RSAAuthentication [y|n]	Esta opción se utiliza para especificar si sshd usa la autenticación de RSA.
ServerKeyBits [bits]	Esta opción se utiliza para especificar el número de bits que se van a utilizar en la clave del servidor.
SilentDeny	Esta opción se establece si se desea que sshd deniegue conexiones sin enviar ninguna notificación a los usuarios rechazados. Es muy útil para los servidores públicos, ya que no da ninguna pista a los usuarios a los que rechaza. Sin embargo, es posible que en redes privadas no sea conveniente establecer esta opción.
StrictModes	Especifique esta opción para establecer que sshd verifique los permisos de los usuarios en su directorio de inicio antes de aceptar el inicio de sesión.
X11Forwarding	Esta opción se especifica para activar X11Forwarding.