

**MANUAL DE INSTALACIÓN DEL SERVIDOR SSH**

Administración de Servicios en Red

Equipo 5:

Campos Gómez Fernanda Ivette

Hernández López César Erick

Ruiz Pérez Alejandro

**ÍNDICE**

|  |  |
| --- | --- |
| 1. Protocolo SSH | 2 |
| Características | 2 |
| ¿Por qué usar SSH? | 3 |
| 2.- Open SSH | 3 |
| 3.- Instalación | 4 |
|  |  |
|  |  |
|  |  |

**Marco Teórico**

# **Protocolo SSH**

SSH™ (o *S*ecure *SH*ell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

SSH está diseñado para reemplazar los métodos más viejos y menos seguros para registrarse remotamente en otro sistema a través de la shell de comando, tales como **telnet** o **rsh**. Un programa relacionado, el **scp**, reemplaza otros programas diseñados para copiar archivos entre hosts como **rcp**. Ya que estas aplicaciones antiguas no encriptan contraseñas entre el cliente y el servidor, evite usarlas mientras le sea posible. El uso de métodos seguros para registrarse remotamente a otros sistemas reduce los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto.

**Características de SSH**

El protocolo SSH proporciona los siguientes tipos de protección:

* Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.
* El cliente transmite su información de autenticación al servidor usando una encriptación robusta de 128 bits.
* Todos los datos enviados y recibidos durante la sesión se transfieren por medio de encriptación de 128 bits, lo cual los hacen extremamente difícil de descifrar y leer.
* El cliente tiene la posibilidad de reenviar aplicaciones X11 desde el servidor. Esta técnica, llamada *reenvío por X11*, proporciona un medio seguro para usar aplicaciones gráficas sobre una red.

Ya que el protocolo SSH encripta todo lo que envía y recibe, se puede usar para asegurar protocolos inseguros. El servidor SSH puede convertirse en un conducto para convertir en seguros los protocolos inseguros mediante el uso de una técnica llamada *reenvío por puerto*, como por ejemplo POP, incrementando la seguridad del sistema en general y de los datos.

Red Hat Enterprise Linux contiene el paquete general de OpenSSH (openssh) así como también los paquetes del servidor OpenSSH (openssh-server) y del cliente (openssh-clients). Consulte el capítulo titulado *OpenSSH* en el *Manual de administración del sistema de Red Hat Enterprise Linux* para obtener instrucciones sobre la instalación y el desarrollo de OpenSSH. Observe que los paquetes OpenSSH requieren el paquete OpenSSL (openssl). OpenSSL instala varias bibliotecas criptográficas importantes, permitiendo que OpenSSH pueda proporcionar comunicaciones encriptadas.

## **¿Por qué usar SSH?**

Los usuario nefarios tienen a su disposición una variedad de herramientas que les permiten interceptar y redirigir el tráfico de la red para ganar acceso al sistema. En términos generales, estas amenazas se pueden catalogar del siguiente modo:

* *Intercepción de la comunicación entre dos sistemas* — En este escenario, existe un tercero en algún lugar de la red entre entidades en comunicación que hace una copia de la información que pasa entre ellas. La parte interceptora puede interceptar y conservar la información, o puede modificar la información y luego enviarla al recipiente al cual estaba destinada.
* Este ataque se puede montar a través del uso de un paquete sniffer — una utilidad de red muy común.
* *Personificación de un determinado host* — Con esta estrategia, un sistema interceptor finge ser el recipiente a quien está destinado un mensaje. Si funciona la estrategia, el sistema del usuario no se da cuenta del engaño y continúa la comunicación con el host incorrecto.
* Esto se produce con técnicas como el envenenamiento del DNS o spoofing de IP (engaño de direcciones IP).

Ambas técnicas interceptan información potencialmente confidencial y si esta intercepción se realiza con propósitos hostiles, el resultado puede ser catastrófico.

Si se utiliza SSH para inicios de sesión de shell remota y para copiar archivos, se pueden disminuir estas amenazas a la seguridad notablemente. Esto es porque el cliente SSH y el servidor usan firmas digitales para verificar su identidad. Adicionalmente, toda la comunicación entre los sistemas cliente y servidor es encriptada. No servirán de nada los intentos de falsificar la identidad de cualquiera de los dos lados de la comunicación ya que cada paquete está cifrado por medio de una llave conocida sólo por el sistema local y el remoto.

**Versiones del protocolo SSH**

El protocolo SSH permite a cualquier programa cliente y servidor construído a las especificaciones del protocolo, comunicarse de forma segura y ser usado de intercambiable.

Existen dos variedades de SSH actualmente (versión 1 y versión 2). La versión 1 de SSH hace uso de muchos algoritmos de encriptación patentados (sin embargo, algunas de estas patentes han expirado) y es vulnerable a un hueco de seguridad que potencialmente permite a un intruso insertar datos en la corriente de comunicación. La suite OpenSSH bajo Red Hat Enterprise Linux utiliza por defecto la versión 2 de SSH, la cual tiene un algoritmo de intercambio de llaves mejorado que no es vulnerable al hueco de seguridad en la versión 1. Sin embargo, la suite OpenSSH también soporta las conexiones de la versión 1.

**OpenSSH**

OpenSSH es la principal herramienta de conectividad para el inicio de sesión remoto con el protocolo SSH. Cifra todo el tráfico para eliminar las escuchas ilegales, el secuestro de conexiones y otros ataques. Además, OpenSSH proporciona un gran conjunto de capacidades de túneles seguros, varios métodos de autenticación y sofisticadas opciones de configuración.

La suite OpenSSH consta de las siguientes herramientas:

* Las operaciones remotas se realizan utilizando ssh, scp y sftp.
* Administración de claves con ssh-add, ssh-keysign, ssh-keyscan y ssh-keygen.
* El lado del servicio consiste en sshd, sftp-server y ssh-agent.

OpenSSH es desarrollado por unos pocos desarrolladores del Proyecto OpenBSD y está disponible bajo una licencia de estilo BSD.

OpenSSH está incorporado en muchos productos comerciales, pero muy pocas de esas compañías ayudan a OpenSSH con fondos.

Las contribuciones para OpenSSH se pueden enviar a la Fundación OpenBSD.

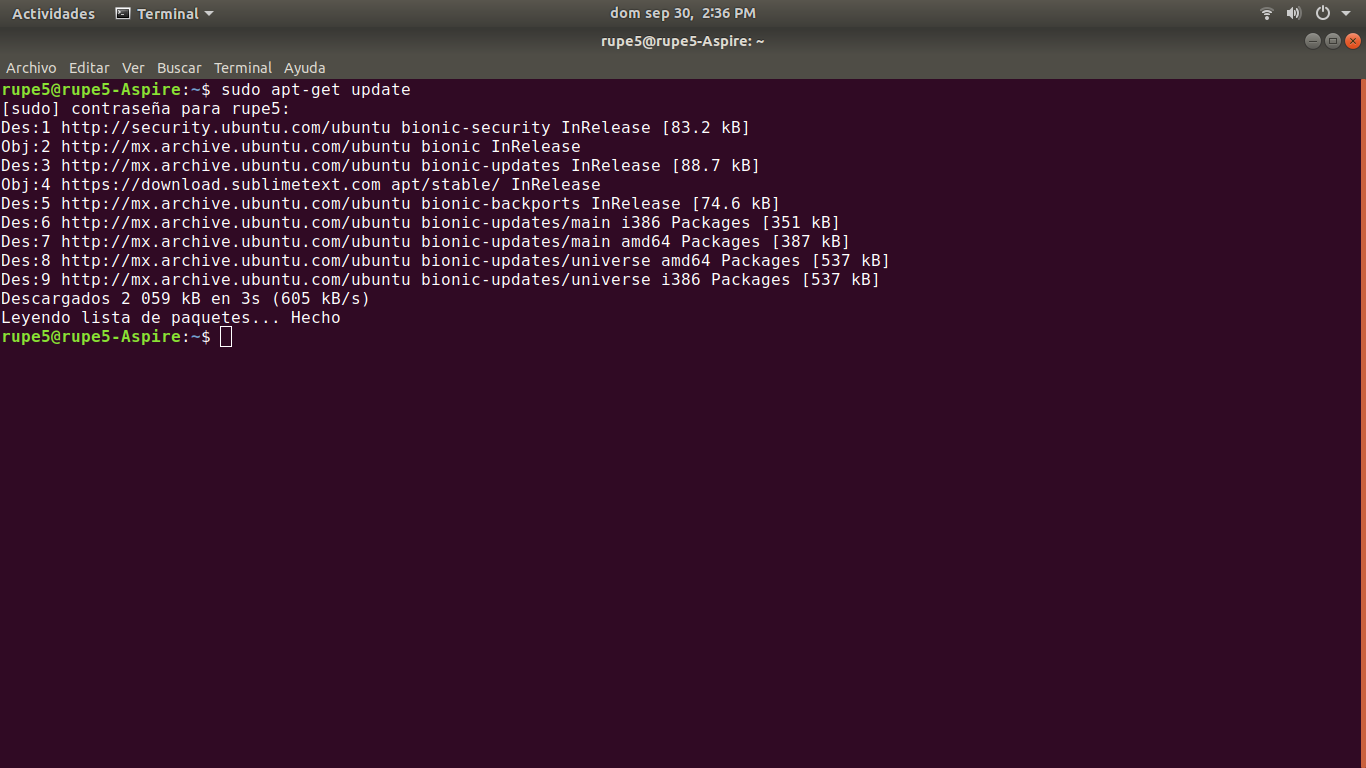
**Instalación**

****

1.- Instalar proFTPd

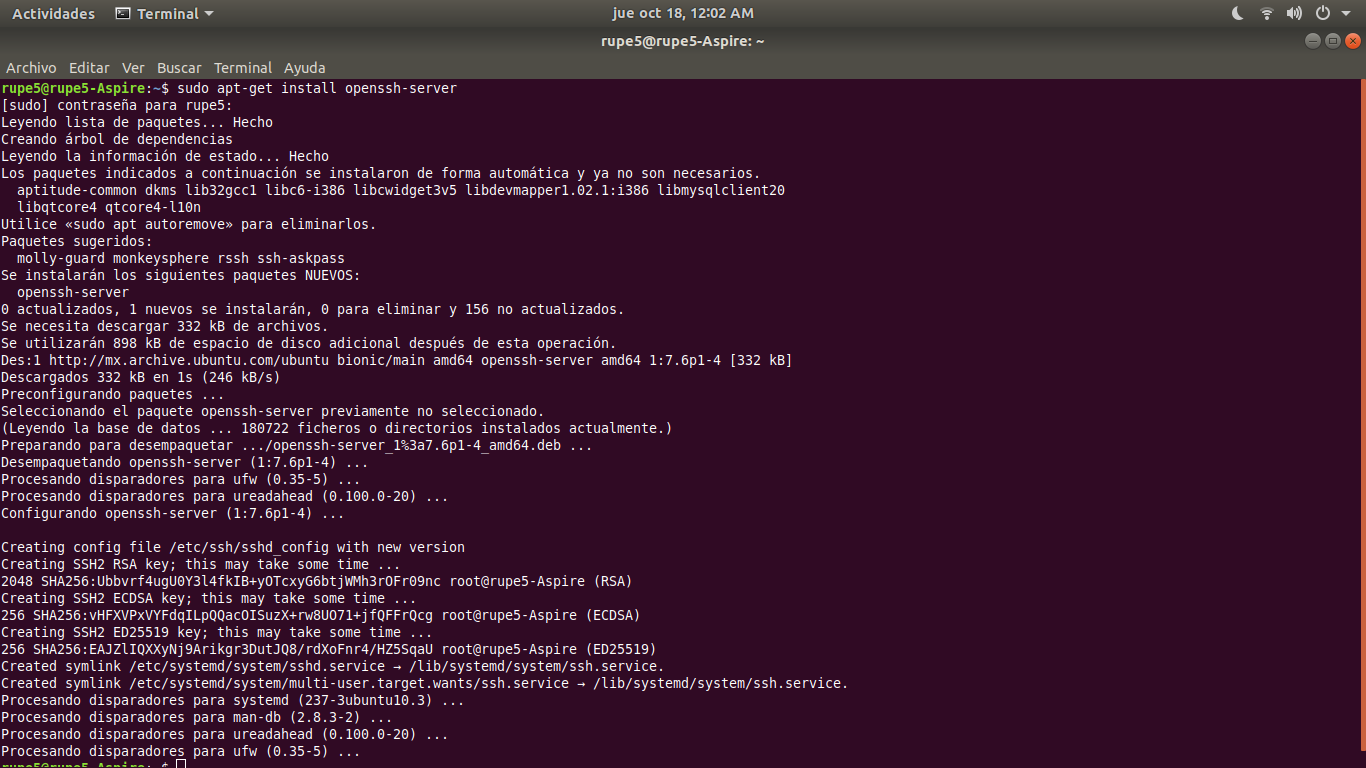
Primero, debemos actualizar nuestras dependencias.

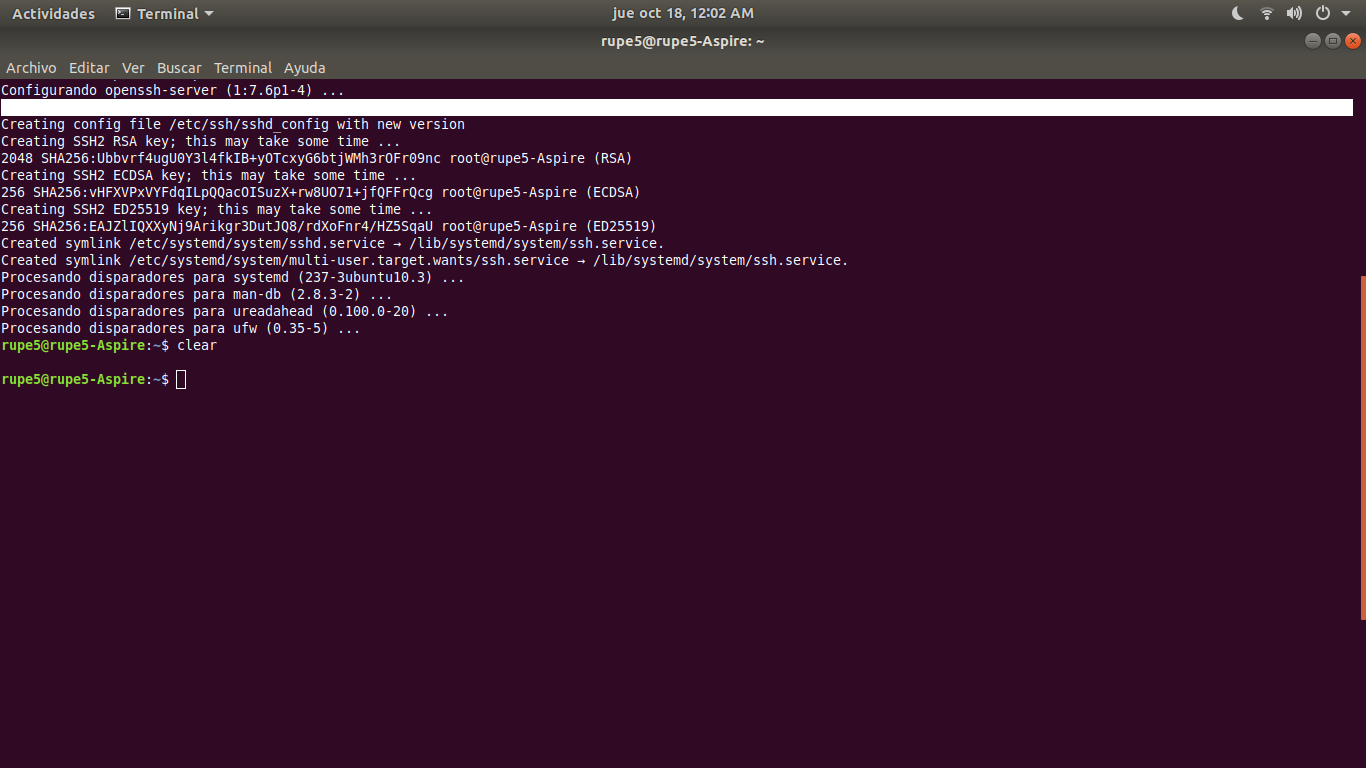
$ sudo apt-get update



Después, instalamos openssh-server.

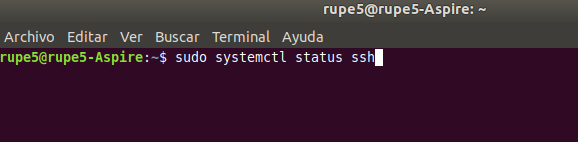
$ sudo apt-get install openssh-server



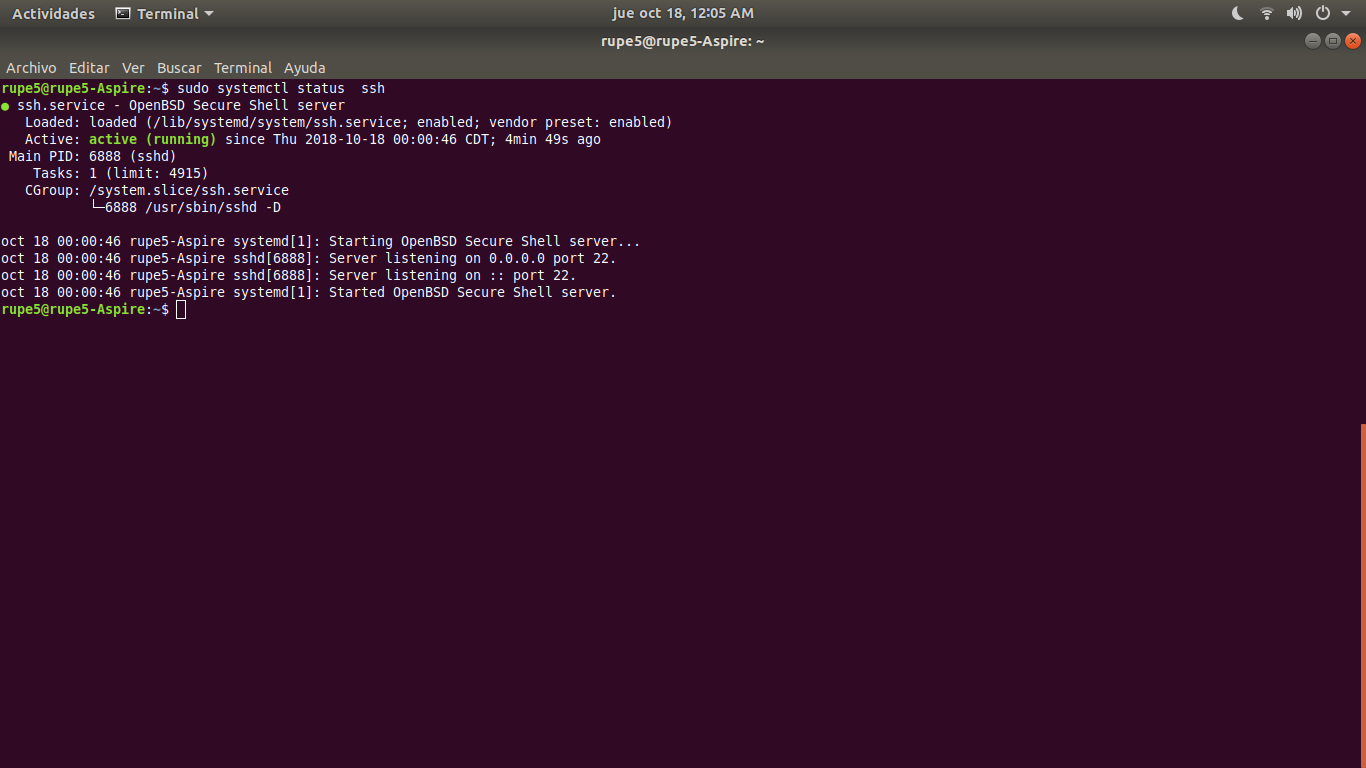


2.- Verificamos el estado del servidor

$ sudo systemctl status ssh



Obtendremos los siguientes datos, lo que significa que el servidor ftp está instalado y funcionando.



**Bibliografía**

[1] https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html

[2] https://www.openssh.com/manual.html