Ingeniería de Servidores (2020-2021)
Grado en Ingeniería Informática
Universidad de Granada

Práctica 2 : Instalación y configuración de servicios

Índice

Índice de figuras

Índice de tablas

OBJETIVOS MÍNIMOS

1. Saber instalar nuevas aplicaciones y conocer los distintos sistemas de gestión de paquetes en Linux.
2. Poder configurar de manera sencilla el cortafuegos.
3. Poder acceder a un servidor de manera segura con ssh.
4. Conocer el concepto de pila *stack* software e instalar una (LAMP).
5. Conocer una interfaz web para administrar servicios.
6. Conocer herramientas para hacer copias de seguridad (backups) y control de versiones.

Lecciones

1. SSH
2. Copias de seguridad y control de versiones
3. Instalación Servidor Web

Competencias que se trabajarán

Competencias Básicas

1. CB2. Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.

Específicas de la Asignatura

1. R1. Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.
2. R2. Capacidad para planificar, concebir, desplegar y dirigir proyectos, servicios y sistemas informáticos en todos los ámbitos, liderando su puesta en marcha y su mejora continua y valorando su impacto económico y social.
3. R5. Conocimiento, administración y mantenimiento de sistemas, servicios y aplicaciones informáticas.

Competencias Específicas del Título:

1. E4. Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas.

Competencias Transversales o Generales:

1. T2. Capacidad de organización y planificación así como capacidad de gestión de la Información.

1. Introducción

Una vez que el sistema operativo está instalado, podemos pasar a configurar la máquina para que dé servicios. Por ejemplo, se podría programar un servicio personalizado y escuchar por el puerto correspondiente pero, ¿está accesible? ¿Cómo se puede averiguar? Son preguntas básicas que se podrán contestar tras la realización de la práctica.
No obstante, antes de pensar en programar un servicio, en el mundo Linux hay muchas implementaciones que nos pueden servir (por ejemplo, un servidor web, FTP, etc.). Por tanto lo primero que haremos será aprender el uso de los gestores de paquetes más importantes (aunque ya hay alternativas propuestas).
Tras haber instalado el software necesario, pasaremos a configurar y aprender a usar el servicio de *Secure SHell* (SSH) que nos permitirá la administración remota de nuestra máquina, así como algunas utilidades prácticas para usarla adecuadamente y unos mecanismos de seguridad básicos para evitar ciertos problemas.
Por último, aprenderemos a instalar un servidor web que nos permita alojar sitios dinámicos.

2. Instalando software

Para poder instalar nuevos servicios, existen gestores de paquetes que permiten realizar esta tarea de una manera muy sencilla. Aunque estas aplicaciones tienen una Graphical User Interface (GUI), es recomendable saber utilizarlas en la consola. En el caso de Windows, muchos servicios proporcionados por Microsoft pueden gestionarse mediante una ventana de configuración. En esta sección se aprenderá cómo utilizar estas herramientas desde la línea de comandos (aunque también existen GUIs que permiten la gestión de paquetes) que nos permiten instalar los servicios de manera fiable y segura.

2.1. yum y apt

Tanto yum como apt son dos gestores de paquetes que permiten conectarse a repositorios (servidores que suministran paquetes) e instalar software resolviendo las dependencias con otros paquetes. Al igual que es sencillo realizar la instalación, también nos permiten más opciones como buscar y desinstalar paquetes. Además, también podremos añadir nuevos repositorios siempre que queramos.
Los paquetes pueden tener un sistema de firma que nos garantiza la fiabilidad de que no estamos cogiendo el paquete equivocado o adulterado.

Por tanto, se considera necesario que usted sepa realizar las operaciones descritas anteriormente con los gestores de paquetes de las distribuciones que estamos usando.

2.2. Futuro (no tan lejano)

Con el objetivo de converger a un gestor de paquetes hay dos propuestas que usted debe conocer: DNF [2] y Snap [3].
Aunque su uso no es necesario ponerlo en práctica, sí debe ser consciente de que algunas distribuciones como Fedora ya usan una de estas alternativas.

3. Gestionando el cortafuegos

Tanto Ubuntu Server como CentOS disponen de un *front-end* para el cortafuegos que permite definir cómodamente las reglas para iptables.
Independientemente de que estudie o no el uso de iptables en otra asignatura, es muy útil conocer el uso adecuado del Uncomplicated FireWall (ufw) en Ubuntu Server así como el firewall-cmd en CentOS. Se espera que usted sea capaz de abrir y cerrar puertos así como de comprobar su estado. Para ello, no solo usaremos las opciones de estos comandos sino que haremos un escaneo de puertos con el comando nmap.

4. SSH

Una vez que ya se disponen de las herramientas para instalar servicios y abrir la puerta para que presten servicio, vamos a trabajar con la administración remota.
Es importante ser conscientes de la ambigüedad de que ssh es tanto un cliente como un servicio. En algunos sistemas es sencillo ya que para denotar al servicio, se utiliza una d (de daemon) al final. Debe prestar especial atención cuando edite los archivos de configuración.
Tras ver la lección correspondiente, se espera que usted sea capaz de instalar, configurar y "asegurar" el servicio SSH, limitando el acceso por contraseña, cambiando el puerto por defecto y prohibiendo que el usuario root tenga acceso al sistema.

4.1. screen, terminator y tmux

De cara a abrir una sesión con una shell y poder cerrar la conexión sin que la shell termine, podemos usar los comandos screen y tmux. Gracias a estos comandos, podemos tener varias sesiones abiertas y reconectarnos a ellas aunque la conexión se haya perdido.
Por otra parte, terminator es una consola que en modo gráfico (tmux para modo texto) permite tener varias terminarles abiertas en una única ventana así como hacer operaciones de *broadcast*, es decir, teclear en una ventana y que el texto aparezca en otras.
Usted deberá saber hacer uso de screen usando la opción más común como es la de recuperar una "ventana" y "desmarcarla" de otro sitio.

4.2. Un poco de seguridad: fail2ban y rkhunter

Para evitar ataques de fuerza bruta podemos usar fail2ban [1] que mete en una lista negra (encarcela) las IPs que han intentado iniciar sesión de manera errónea varias veces seguidas en un intervalo de tiempo predefinido.
RootKit Hunter (`http://rkhunter.sourceforge.net/`) es un software que permite analizar el sistema para ver si hay software malicioso instalado en la máquina (*rootkits, backdoors, exploits*, etc.).
Se espera que usted sea capaz de instalar, configurar y gestionar la funcionalidad básica de fail2ban así como de ejecutar rkhunter y determinar si hay alguna amenaza en el sistema.

5. Instalando un servidor web básico

Uno de los servicios más comunes que se suelen instalar en un servidor es un programa para servir páginas web. Incluso hay entornos de desarrollo que se basan en éste (p.ej. jupyter).
Por tanto, se espere que usted sepa configurar un servidor web con la funcionalidad básica que consiste en tener un servidor web (Apache) un gestor de bases de datos (MariaDB) y los interpretes de lenguajes de uso común para la web como pueden ser PHP y Python, todo ésto conocido comúnmente por LAMPP.
Debe demostrar su funcionamiento mediante un script (en uno de los dos lenguajes citados) que involucre a todos los actores enunciados.

5.1. Webmin

Como utilidad inmediata para la administración, mencionamos un ejemplo de una interfaz web que nos permite administrar el sistema: Webmin (`http://www.webmin.com/`).
Existen otras alternativas de paneles de administración: C-Panel, Parallels Plesk, DirectAdmin, etc. (C-Panel y Parallels Plesk son los más populares) pero suelen ser de código cerrado y comerciales.
Usted debe saber instalar y dejar en funcionamiento Webmin además de razonar ventajas y desventajas de usar Webmin frente a SSH.

6. Copias de seguridad y control de versiones

El mantener la información del sistema así como la de los usuarios es algo crucial cuando estamos trabajando con servidores.
Los comandos esenciales para esta tarea son: tar y rsync (aunque también existen otros bastante usados como dd y cpio) [4].
Existen también otras soluciones más complejas (y completas) para gestionar las copias de seguridad como Amanda (`http://www.amanda.org/`) y Bacula (`https://blog.bacula.org/`).

Además de la copia de los datos, siempre que modifiquemos un archivo de configuración deberemos hacer un "backup" de éste por si introducimos algún error. Hay muchas formas de hacerlo pero es interesante considerar el control de versiones así como para mantener los scripts de administración.
Usted debe saber realizar una copia de seguridad usando tar y rsync así como las operaciones básicas de git para controlar versiones y restaurar un error.

Referencias

[1] Cyril Jaquier et al. Fail2ban. `https://www.fail2ban.org/wiki/index.php/Main_Page`, 2016. [Online; consultada 14-Feb-2018].

[2] Fedora. Dnf. `https://fedoraproject.org/wiki/DNF?rd=Dnf`, 2017. [Online; consultada 14-Feb-2018].

[3] Canonical Ltd. Sanpcraft. `https://snapcraft.io/`, 2018. [Online; consultada 14-Feb-2018].

[4] W. Curtis Preston. *Backup & Recovery*. O'Reilly Media, Inc., 2006.