Mòdul de Desplegament: Connectant-nos al Món Real

Una Introducció Pràctica al Desplegament Remot

Escenari de Treball: El VPS

- **No treballarem en local!** Simularem un escenari 100% real on el nostre entorn de treball és una **màquina virtual remota**.
- Imagina que hem contractat un **VPS (Virtual Private Server)**. Aquesta serà la nostra base d'operacions remota, tal com passa en projectes reals.

Què és un Servidor? I un VPS?

- Un **servidor** és un ordinador on el teu proveïdor d'allotjament web emmagatzema els fitxers i les bases de dades del teu lloc web.
- Quan algú visita el teu web, el seu navegador demana aquests fitxers al servidor.
- L'**allotjament VPS** et dona un "servidor al núvol" que simula un servidor físic, però en realitat, la màquina es comparteix entre diversos usuaris.

La Màgia del VPS: Virtualització

- El proveïdor crea una capa virtual sobre el sistema operatiu del servidor.
- Aquesta capa divideix el servidor en **"particions"**.
- Cada usuari pot instal·lar el seu propi sistema operatiu i programari en la seva partició.
- Un **Servidor Privat Virtual (VPS)** és privat perquè tens control absolut sobre ell.
- És com fer particions al teu propi ordinador per tenir Windows i Linux sense haver de reiniciar.

Per què un VPS? Recursos Garantits!

- Amb un VPS, el teu lloc web viu en un **"contenidor" segur**.
- Tens **recursos garantits**: memòria, espai en disc, nuclis de CPU... Ningú els comparteix amb tu!
- Tens **accés de nivell arrel** (com si lloguessis un servidor dedicat), però a un cost molt més baix.
- **Més segur i estable** que l'allotjament compartit.
- Ideal per a llocs web amb trànsit mitjà, que superen els límits de l'allotjament compartit però encara no necessiten els recursos d'un servidor dedicat.

Connectant-nos al VPS: L'SSH

- Encara que la nostra màquina virtual estigui al nostre ordinador, estem simulant un VPS remot.
- La forma més segura i recomanable de connectar-se a una màquina remota és **SSH**.

SSH (Secure Shell): El Teu Canal Segur

- **Protocol de xarxa criptogràfic** per operar serveis de xarxa de forma segura sobre una xarxa no protegida.
- Aplicacions típiques: línia de comandes remota, inici de sessió i execució de comandes remota.
- Funciona amb una arquitectura **client-servidor**.
- Port TCP estàndard: **22**. S'utilitza molt en sistemes Unix/Linux, però també es pot utilitzar a Microsoft Windows.

Utilitats Clau de SSH

- Gestió de servidors remots.
- Transferència segura de fitxers.
- Creació de còpies de seguretat.
- Connexió xifrada d'extrem a extrem entre dos ordinadors.
- Manteniment remot des d'altres equips.

Autenticació amb SSH: Seguretat al Capdavant

- Dos mètodes comuns per autenticar-se:
  - **Contrasenyes (xifrat simètric)**.
  - **Claus SSH (xifrat asimètric o de clau pública)**.
- Les contrasenyes s'envien xifrades, però la seva seguretat depèn de la qualitat de la contrasenya.
- Els **parells de claus pública-privada SSH** són una opció més robusta.
- SSH utilitza un **xifrat híbrid**: xifrat asimètric per intercanviar claus, i després xifrat simètric per a l'intercanvi de dades.

Xifrat Simètric o de Clau Privada

- **Una sola clau** per xifrar i desxifrar la informació.
- Aquesta clau ha de ser **secreta** i només coneguda per l'emissor i el receptor.

Xifrat Simètric: Pros i Contras

Avantatges:

- **Molt ràpids** → el temps de xifrat i desxifrat és reduït.

Inconvenients:

- Si la clau cau en mans equivocades, la comunicació queda exposada.
- Com fem que emissor i receptor coneguin la clau inicialment? No es pot transmetre pel canal insegur, cal un altre canal segur (Exemple: PIN de la targeta del banc).

Xifrat Asimètric o de Clau Pública

- Cada usuari utilitza un parell de claus: una **clau pública** i una **clau privada**.
- Un missatge xifrat amb la clau pública només es pot desxifrar amb la seva corresponent clau privada, i viceversa.

Clau Pública vs. Clau Privada

- La **clau pública** és accessible a qualsevol persona que vulgui consultar-la; no cal que sigui transmesa per un canal segur.
- La **clau privada** només la ha de conèixer el seu amo.

Funcionament del Xifrat Asimètric

1. L'emissor xifra un missatge amb la clau pública del receptor.
2. El receptor rep el missatge i és l'únic que podrà desxifrar-lo, perquè és l'únic que posseeix la clau privada associada.

Xifrat Asimètric: Pros i Contras

Avantatges:

- No es necessita un nou canal independent i segur per transmetre la clau.

Inconvenients:

- Són més lents que els xifrats simètrics.
- Cal protegir molt bé la clau privada i tenir-la sempre disponible per poder desxifrar els missatges (no és una contrasenya).
- Cal assegurar-se que la clau pública és de qui diu ser i no d'un impostor.

En la Pràctica: La Nostra Estratègia d'Autenticació

- Per connectar-nos per primera vegada per SSH i comprovar la connectivitat, utilitzarem el xifrat simètric (una contrasenya).
- Després d'això, simulant un entorn real (per comoditat i seguretat), utilitzarem xifrat asimètric: un parell de claus.