Docker

Am instalat Docker pe serverul meu Ubuntu 22.04 LTS urmând câțiva pași cheie. Mai întâi, am actualizat sistemul și am instalat pachete necesare pentru a permite instalarea sigură a Docker prin HTTPS. Apoi, am adăugat cheia GPG oficială Docker și repositoriul în sistemul meu pentru a asigura integritatea și sursa autentică a pachetelor Docker. După aceea, am instalat Docker Community Edition, incluzând clienții CLI și runtime-ul containerd.io, facilitând crearea și gestionarea containerelor. În final, verificarea cu un container de test "hello-world" a confirmat că Docker este instalat corect și funcțional pe sistem. Acești pași au pregătit mediul meu pentru dezvoltarea și gestionarea aplicațiilor în containere.

A screenshot of a computer

Description automatically generated

SSH

Am completat cu succes instalarea și configurarea serviciului SSH pe sistemul meu Ubuntu 22.04 LTS, aflat într-o mașină virtuală gestionată prin VirtualBox. Procesul a început prin instalarea pachetului OpenSSH Server, o etapă esențială care mi-a permis să activez capabilitățile de conectare la distanță. Odată ce instalarea a fost finalizată, am verificat activitatea serviciului SSH, asigurându-mă că acesta funcționează corespunzător. Următorul pas a fost să utilizez un client SSH pentru a stabili o conexiune la distanță către serverul Ubuntu, folosind numele meu de utilizator și adresa IP specifică mașinii virtuale. Acest proces a demonstrat eficiența și simplitatea cu care se poate realiza administrarea la distanță a unui sistem Linux, reprezentând un avantaj semnificativ în gestionarea serverelor fără necesitatea accesului fizic direct. Conectivitatea reușită și ușurința cu care am gestionat aceste etape subliniază valoarea SSH ca instrument fundamental în administrarea sistemelor.

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

Apache Server

A screenshot of a computer

Description automatically generatedFail2ban

În cadrul eforturilor noastre continue de a securiza și optimiza serverul Ubuntu aflat într-o mașină virtuală, am realizat cu succes instalarea și configurarea serviciului Fail2ban, un instrument esențial în prevenirea atacurilor brute-force împotriva serviciilor expuse, cum ar fi SSH și serverul web Apache. Inițial, am procedat la instalarea Fail2ban folosind managerul de pachete apt, asigurându-ne astfel că avem cea mai recentă versiune disponibilă și toate dependențele necesare pentru o funcționare optimă.

După instalare, am trecut la pasul crucial de configurare a Fail2ban. Pentru a evita suprascrierea configurațiilor la viitoarele actualizări ale pachetului, am optat pentru crearea unui fișier de configurare jail.local, clonând setările default din jail.conf. Acest pas ne-a permis să personalizăm regulile și acțiunile Fail2ban, adaptându-le specific nevoilor noastre de securitate, fără a risca pierderea modificărilor la un update.

În final, am asigurat pornirea serviciului Fail2ban și l-am configurat pentru a se executa automat la inițializarea sistemului. Verificarea stării serviciului a confirmat activarea și funcționarea corectă acestuia, semnalând o implementare reușită.  
A screenshot of a computer

Description automatically generated