Born2beroot

Cos'è una macchina virtuale (VM)?
Una macchina virtuale è un software che offre le stesse potenzialità di un computer fisico, cioè esegue un sistema operativo (OS) e delle applicazioni, attraverso la creazione di un ambiente isolato e virtuale all'interno di un host fisico. Solitamente, viene utilizzata per specifiche attività che sono potenzialmente rischiose da eseguire direttamente sul computer fisico o per l'esecuzione di più sistemi operativi sullo stesso hardware fisico.
Una macchina virtuale è quindi un software che crea un ambiente virtuale separato dal computer fisico e che simula il comportamento di un sistema informatico grazie all'assegnazione di risorse hardware (porzioni del disco rigido, RAM, processore…). Tutto quello che accade all'interno della macchina virtuale non ha ripercussioni fuori da essa: l'hardware di base viene condiviso con il computer fisico, ma le risorse utilizzate sono completamente protette e isolate.

Vantaggi:
- Facili da gestire
- Possibilità di eseguire più sistemi operativi isolati sullo stesso computer
- Possibilità di testare applicazioni in un ambiente controllato, aumentando così la sicurezza

Svantaggi:
- Prestazioni instabili del computer in caso di aggiunta di molte macchine virtuali a causa del carico significativo delle risorse
- Più lente e meno efficienti di un computer fisico

Cos'è il *Logical Volume Manager* (LVM)?
Il LVM è un software di gestione dello spazio su disco (alloca spazio in modo dinamico), che è disponibile su sistemi operativi come quelli basati su Linux. L'obiettivo principale del LVM è fornire una maggiore flessibilità nella gestione delle risorse di archiviazione, superando le limitazioni delle partizioni tradizionali. Il LVM consente di aggregare "volumi fisici" (dischi, partizioni) in uno o più "gruppi di volumi", che costituiscono una sorta di pool di archiviazione che può essere suddivisa in "volumi logici", che funzionano come partizioni virtuali. Il vantaggio è che questi volumi logici possono essere facilmente ridimensionati e spostati senza dover modificare la struttura fisica dello spazio su disco e senza dover spostare fisicamente i dati.

Vantaggi del LVM
- Flessibilità: è possibile ridimensionare i volumi logici nell'immediato, senza la necessità di smontare il filesystem o di interrompere i servizi
- Snapshot: è possibile creare snapshot istantanei dei volumi logici, cioè copie istantanee di un volume logico in un determinato momento, che risultano utili per i backup o per mantenere uno stato consistente dei dati prima di apportare modifiche significative
- Migrazione dei dati: è possibile spostare i dati da un disco fisico a un altro senza interruzioni
- Gestione semplificata: offre una gestione centralizzata dello storag*e*, rendendo più semplice l'amministrazione di grandi quantità di spazio su disco. È inoltre possibile estendere facilmente lo spazio di archiviazione aggiungendo nuovi volumi fisici al gruppo di volume

In sintesi, il LVM offre una maggiore flessibilità e facilità di gestione dello spazio su disco, rendendo più agevole l'amministrazione dei sistemi Linux in ambienti in continua evoluzione.

Rocky vs Debian
Rocky e Debian sono entrambi sistemi operativi open-source basati su Linux (Linux è il *kernel*, cioè il nucleo del sistema operativo, di entrambe le distribuzioni).

Rocky è una distribuzione Linux più recente e basata su RHEL (*Red Hat Enterprise Linux)*, che è nata con lo scopo di sviluppare un sistema operativo orientato alle imprese e con una buona comunità di supporto (progetto *community driven*). Essendo una distribuzione recente, supporta anche i compilatori più recenti, ma risulta più complessa per un singolo utente.

Debian è una delle distribuzioni Linux più antiche, più stabili e più diffuse, infatti ha una vasta comunità di sviluppatori. Offre una vasta repository di pacchetti software (vasta gamma di applicazioni e strumenti) ed è noto per la sua flessibilità, attenzione alla privacy e interfaccia grafica user-friendly (anche se non troppo moderna), garantendo così all'utente un'esperienza affidabile, sicura e intuitiva. Tuttavia, può richiedere alcune configurazioni aggiuntive per adattarsi alle esigenze specifiche del gaming o per supportare hardware più recenti e altamente specializzati.

Cosa sono Apt (*Advanced Packaging Tool*) e Aptitude?
Apt e Aptitude sono gestori di pacchetti per Debian.

- Apt:

"apt" è il comando base per gestire i pacchetti di un sistema *Debian-based*, poiché è incluso nel pacchetto di base del sistema operativo. Apt è più recente e user-friendly, ma non supporta un'interfaccia grafica (solo riga di comando). Per installare un pacchetto tramite apt è necessario digitare il nome del pacchetto preceduto dal comando "sudo apt install". I comandi legati ad apt permettono di gestire meglio il sistema e di gestire eventuali update, disinstallazioni, modifiche e/o rimozioni.

- Aptitude:

Aptitude è uno strumento simile ad apt, ma offre funzionalità più dettagliate. Non è inserito di default nel sistema operativo, quindi va installato usando apt. Offre la possibilità di gestire i pacchetti anche con un'interfaccia grafica direttamente nel terminale.

Cos'è APPArmor?
APPArmor (*Application Armor*) è un insieme di strumenti, politiche e procedure progettato per il controllo degli accessi basato sul *kernel* di Linux. Il suo scopo è quello di limitare ciò che un'applicazione può fare: definisce quali risorse una certa applicazione è autorizzata a utilizzare e quali azioni può compiere. In pratica, il *kernel* interroga APPArmor prima di ogni chiamata di sistema per sapere se una data applicazione è autorizzata a eseguire una data operazione. Quindi, APPArmor è un sistema di sicurezza Linux che protegge il sistema operativo limitando le capacità dei programmi applicando una serie di regole su ciascuno.

Cos'è SUDO (*Super User Do*)?
Il comando "sudo" consente, nei sistemi operativi Linux, ai normali utenti privilegi di amministratore tramite specifici comandi: gli utenti possono usare questo comando come se fossero gli amministratori del sistema.

Cos'è un *Firewall*?
Un *firewall* è un dispositivo per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinite di regole di sicurezza per consentire o bloccare gli eventi. Dal punto di vista del funzionamento, il *firewall* è una sorta di filtro che controlla il traffico dei dati e blocca le connessioni indesiderate e/o potenzialmente pericolose. Si interpone tra la rete esterna, che comprende internet, e la rete interna, che può essere quella dell'azienda o quella della propria abitazione.

UFW (*Uncomplicated Firewall*) è l'applicazione predefinita dei sistemi operativi basati su Linux, come Ubuntu, per la gestione del *firewall*. UFW fornisce un'interfaccia semplificata e più user-friendly (riga di comando) per configurare le regole del *firewall*, rendendo più facile agli utenti definire le regole di filtraggio del traffico in entrata e in uscita e prevenendo accessi non autorizzati. UFW fornisce inoltre regole già preconfigurate per alcune applicazioni comuni, come SSH.

Cos'è SSH (*Secure Shell*)?
La SSH è un protocollo di rete crittografato che svolge un ruolo cruciale nella sicurezza e nella gestione dei sistemi informatici, fornendo un mezzo affidabile per operare in modo sicuro su reti non sicure come Internet: fornisce un canale sicuro attraverso il quale è possibile accedere e comunicare con un computer da remoto, cioè stabilisce una connessione sicura alla *shell* di un altro computer, facilitando la gestione dei server, il trasferimento di dati e di file in modo sicuro, la creazione di backup e la manutenzione a distanza di un computer.

Cos'è CRON?
Cron è un servizio di pianificazione del tempo per sistemi operativi come quelli basati su Linux. Consente agli utenti di programmare l'esecuzione automatica di comandi o script a intervalli regolari. Un *cronjob* è un'attività pianificata che viene eseguita automaticamente dal sistema operativo in un determinato momento o a intervalli specifici. Il *crontab* è il file di configurazione in cui gli utenti possono definire i loro *cronjob*. Utlizzando il comando "crontab" gli utenti possono gestire e interagire con questi *cronjob* (cioè visualizzare, modificare o rimuovere il *crontab*).
Solitamente i *cronjob* sono supportati da tre elementi:

1) Lo script da eseguire, cioè un insieme di istruzioni o comandi
2) Il comando che esegue lo script al tempo impostato
3) L'output dello script