Open Source Day 2013

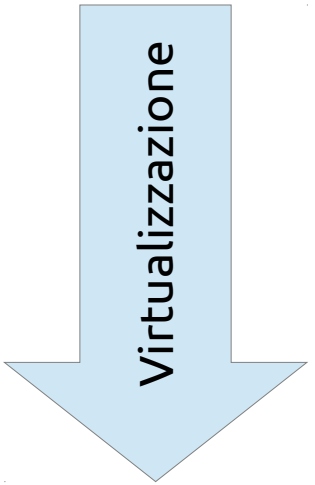
La sicurezza negli ambienti virtualizzati

Marco Vanino
mvan@spin.it

Spin internetworking

Sicurezza in ambiente virtualizzato

1 computer fisico = 1 computer logico



1 computer fisico = N computer logici

Spin internetworking

Sicurezza in ambiente virtualizzato

Implicazioni di sicurezza

- maggiore impatto in caso di guasti, sovraccarico, violazione del host/hypervisor
- maggiore superficie di attacco

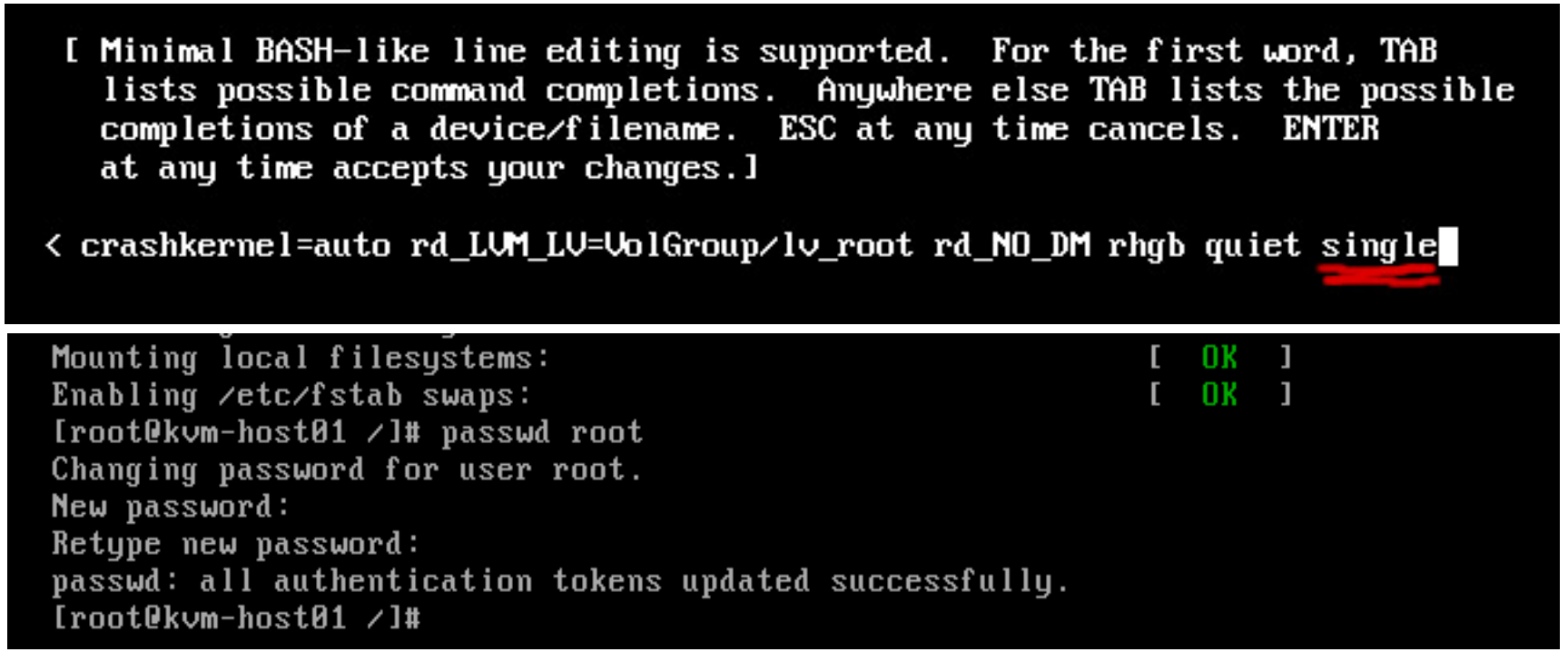
Sicurezza in ambiente virtualizzato

Il livello di sicurezza di un sistema virtualizzato è dipendente dai livelli di sicurezza di ogni suo singolo componente

- Host e Hypervisor
- Storage
- Rete
- Gestione del sistema

Sicurezza fisica

Chiunque abbia accessibilità diretta agli host, ai dispositivi di storage e agli apparati di rete può potenzialmente ottenere autorizzazioni privilegiate



Spin internetworking

Sicurezza fisica

controllo dell'accesso a locali e/o armadi

- serrature “tradizionali”
  - chiavi
  - lucchetti
  - combinazioni
- controllo elettronico
  - codici di accesso
  - dispositivi di identificazione personale

Sicurezza fisica

registrazione degli accessi

- registri cartacei
- log
  - file
  - database

Data	Nome	Ingresso	Uscita	Motivo
29/11/2013	Marco Vanino	08:30	09:30	Upg. RAM SRV023
29/11/2013	Mario Rossi	09:45	12:15	Collegamento nuovo datastore
29/11/2013	Laura Bianchi	14:00	14:15	Test manuale UPS

Host e Hypervisor

Hardware

- rimuovere o disabilitare i dispositivi non necessari

Sistema operativo

- installazione minimale del sistema operativo
  - kernel e relativi moduli
  - applicazioni
  - utility
- disinstallare o disabilitare i servizi non necessari
- configurare policy di sicurezza (SELinux/AppArmor)
- aggiornamento costante

Host e Hypervisor

Management

- limitare l'accesso diretto con credenziali privilegiate
- interfaccia di rete dedicata
  - subnet dedicata out-of-band o VLAN separata
- filtri (ACL) a livello IP
  - limitare l'accesso ai soli amministratori
  - permettere il collegamento solamente ai dispositivi strettamente necessari alla gestione
- accesso dall'esterno via VPN

Storage

Array di dischi

- Sicurezza dati
  - RAID6/RAIDZ2
  - RAID7/RAIDZ3
- Sicurezza dati e prestazioni
  - RAID10/ZFS Striped mirror
  - Soluzioni precedenti + SSD caching

Storage

Immagini dei dischi virtuali su file

- indipendenza dal hardware
- facilità di copia/esportazione
- ripristino in tempi rapidi delle VM
- furto dei dati semplificato

Storage

Reti dedicate

- migliori prestazioni
- maggiore sicurezza

Ridondanza delle connessioni

- multipath
- interface bonding

Storage

Accesso controllato a LUN e/o condivisioni di rete

- iSCSI
  - ACL per IP
  - LUN masking (IQN/EUI/NAA)
  - CHAP (unidirezionale/bidirezionale)
- NFS
  - exports (IP, nome DNS)
- Fiber Channel
  - zoning (port o WWN)
  - LUN masking (WWN)

Storage

backup

- piano di backup/recovery
  - cosa copiare
  - come copiare (immagini dischi, file, dump db)
  - policy di retention e archiviazione
- conservazione copie
  - locali o edifici esterni
  - siti remoti

Storage

backup

- copie applicazioni “complesse” (db, AD, MS-Exchange)
  - database dump
  - agenti
  - Volume Shadow Copy
- replica/sincronizzazione remota
- protezione e cifratura copie
- verifica restore

Spin internetworking

Rete

- VLAN dedicata per management
- Accesso controllato agli apparati
  - Autenticazione, Autorizzazione e Accounting (AAA)
    - RADIUS, LDAP, TACACS
- Ridondanza dei collegamenti LAN/WAN
  - gestione failover
  - incremento delle prestazioni

Rete

Protezione VM

- zone di sicurezza (VLAN, switch e firewall virtuali)
- ACL sulle porte degli switch virtuali

Perimetro e accesso remoto

- Firewall/UTM
  - controlli a L3 o superiore
- VPN
  - IPSec, SSL
  - controllo accessi (RADIUS, LDAP)

Rete

- gestione di QoS
- monitoraggio apparati fisici e virtuali
  - SNMP, NetFlow/IPFIX, SPAN/RSPAN
- gestione centralizzata degli apparati
  - SDN (OpenFlow)

Gestione del sistema

Amministrazione

- limitare l'accesso diretto alla console
- separazione dei ruoli amministrativi
  - hypervisor
  - datastore
  - rete
  - VM
- politiche di accesso *role based* (RBAC)

Gestione del sistema

Amministrazione

- assegnazione pool di risorse per utente/gruppo
  - numero massimo di istanze
  - CPU
  - memoria
  - storage
  - Networking
- controllo centralizzato degli accessi
  - AD, LDAP (389 Directory Server, FreeIPA)

Gestione del sistema

Evitare la proliferazione incontrollata delle VM

- definire il ciclo di vita delle macchine virtuali
- mantenere un inventario aggiornato
- documentare (e mantenere aggiornate le informazioni)
- utilizzo di Configuration Management Database (CMDB)

Gestione del sistema

monitoraggio dell'utilizzo delle risorse

- CPU
- RAM
- storage
- rete

gestione avvisi e allarmi

- email
- SMS

bilanciamento del carico

- distribuzione delle risorse sugli hypervisor

Gestione del sistema

gestione dei log

- log centralizzati
- sincronizzazione dell'orario via NTP
- analisi sistematica dei log

utilizzo di IDS/IPS

- individuare attacchi o infezioni dovute a malware
- individuare traffico di rete anomalo

Gestione del sistema

Amministrazione VM

- limitare l'utilizzo diretto alla console delle VM
  - preferire l'accesso via RDP o SSH
- aggiornamenti
  - sistemi operativi
  - applicativi

Gestione del sistema

Amministrazione VM

- Protezione
  - antivirus
  - antimalware
  - firewall interno
- Resilienza
  - configurazioni high availability
    - gestite dal sistema di virtualizzazione
    - cluster (heartbeat)

Piano di emergenza

sito di ripristino

- disponibilità hardware (server, SAN/NAS, dispositivi di rete)

kit di ripristino

- tastiera, mouse, monitor, USB hub, HBA, cavi, adattatori, chiavi/contatti per l'accesso ai locali
- supporti di installazione (CD, DVD, USB key)
- software di supporto (driver, software di restore)
- documentazione cartacea aggiornata

Piano di emergenza

kit di ripristino: documentazione

- definizione dei compiti (chi deve fare, cosa deve fare)
- come e dove recuperare l'hardware (server, SAN/NAS, apparati di rete)
- come e dove recuperare le copie e come utilizzarle
- credenziali
- priorità di ripristino dei servizi
- descrizione delle operazioni
- check list post installazione