

LEZIONE 3 – GESTIONE DELLE MACCHINE VIRTUALI

- In questa lezione approfondiamo in modo operativo la gestione delle Virtual Machine (VM).
- Non ci limitiamo a crearle, ma impariamo a mantenerle, modificarle e controllarle nel tempo.
- L'obiettivo è acquisire un metodo professionale applicabile in ambienti enterprise.



CICLO DI VITA DI UNA VM



Ogni VM attraversa diverse fasi: creazione, configurazione, utilizzo e dismissione.



Questo processo è chiamato Lifecycle (ciclo di vita).



Una gestione corretta riduce errori operativi e vulnerabilità di sicurezza.

PROVISIONING

- Provisioning significa creare e configurare una nuova macchina virtuale.
- Include assegnazione di CPU virtuali (vCPU), RAM e spazio disco.
- In ambienti aziendali spesso è automatizzato tramite template o script.

TEMPLATE

- Un Template è un modello preconfigurato di VM.
- Contiene sistema operativo aggiornato e configurato.
- Permette di distribuire nuove VM in modo rapido e standardizzato.

CLONE

- Clonare significa creare una copia di una VM esistente.
- Può essere Full Clone (indipendente) o Linked Clone (dipendente).
- È molto usato in laboratorio e ambienti di test.

SNAPSHOT



Uno Snapshot è una fotografia dello stato della VM in un momento preciso.



Salva lo stato del disco e opzionalmente della memoria RAM.



Permette di tornare indietro rapidamente in caso di errore.

SNAPSHOT VS BACKUP

- Lo Snapshot è interno alla VM e dipende dall'host.
- Il Backup è una copia indipendente dei dati.
- Uno snapshot non protegge da guasti hardware dell'host.

DISCHI VIRTUALI

- I dischi virtuali sono file memorizzati sull'host.
- Formati comuni: qcow2 (QEMU), VMDK (VMware), VDI (VirtualBox).
- Possono essere dinamici (Thin) o preallocati (Thick).



THIN PROVISIONING

- Alloca spazio disco solo quando effettivamente utilizzato.
- Ottimizza l'uso dello storage.
- Richiede monitoraggio per evitare saturazione.

THICK PROVISIONING

- Alloca immediatamente tutto lo spazio definito.
- Offre prestazioni più prevedibili.
- Richiede maggiore spazio iniziale.



GESTIONE CPU E RAM

- Le vCPU (virtual CPU) sono core logici assegnati alla VM.
- La RAM virtuale viene allocata dall'host.
- Un'allocazione eccessiva può degradare le performance globali.

OVERCOMMIT

- Overcommit significa assegnare più risorse virtuali di quelle fisiche.
- Funziona perché non tutte le VM usano il 100% delle risorse contemporaneamente.
- Richiede monitoraggio costante per evitare colli di bottiglia.

RETE VIRTUALE

- Ogni VM ha una Virtual Network Interface Card (vNIC).
- Può operare in modalità NAT, Bridged o rete isolata.
- La configurazione influisce direttamente sulla sicurezza.

SPEGNIMENTO CORRETTO

- La VM deve essere spenta tramite shutdown interno.
- Evitare spegnimento forzato (power off).
- Riduce il rischio di corruzione del file system.

FILE SYSTEM

- Un file system è il componente del sistema operativo che organizza, memorizza e gestisce file e directory su dispositivi di archiviazione
- **Tipi Comuni:**
- **NTFS:** Utilizzato principalmente in Windows.
- **FAT32/exFAT:** Comune per chiavette USB e compatibilità tra sistemi.
- **APFS/HFS+:** Standard per i dispositivi Apple.
- **ext4/Btrfs:** Usati comunemente in Linux

FILE SYSTEM JOURNALED

- è un tipo di file system che garantisce l'integrità strutturale dei dati memorizzati su un disco, utilizzando un registro speciale chiamato "**journal**" (diario) per tracciare le modifiche prima che vengano applicate definitivamente al file system principale

COME FUNZIONA IL JOURNALING

- **Registrazione (Journaling):** Scrive la modifica prevista (meta-dati) nel "journal", che è una zona circolare del disco riservata a questo scopo.
- **Commit:** La modifica viene contrassegnata come "completata" nel journal.
- **Scrittura (Checkpointing):** Le modifiche vengono trasferite dal journal alla loro posizione definitiva nel file system principale.

SAVE STATE

- Il Save State salva lo stato della memoria su disco.
- Alla riaccensione la VM riparte dallo stesso punto.
- Non equivale a uno snapshot completo.

MIGRAZIONE VM

- La migrazione consente di spostare una VM su un altro host.
- Può essere offline o live.
- È tipica degli ambienti clusterizzati.

MONITORAGGIO

- Utilizzare strumenti come top o htop sull'host Linux.
- Controllare carico CPU, RAM e I/O disco.
- Identificare VM che consumano eccessivamente.

HARDENING VM

- Hardening significa rafforzamento della sicurezza.
- Disabilitare servizi non necessari.
- Limitare accesso amministrativo e aggiornare regolarmente.

BEST PRACTICE

- Pianificare risorse prima di creare VM.
- Monitorare utilizzo nel tempo.
- Documentare configurazioni e fare backup periodici.

ERRORI COMUNI

- Creare troppe VM inutili.
- Non eliminare snapshot vecchi.
- Allocare tutte le risorse a una sola VM.

RIEPILOGO

- La gestione delle VM è competenza fondamentale per un tecnico cybersecurity.
- Snapshot utili ma non sostituiscono backup.
- Organizzazione e disciplina sono chiave in ambienti virtualizzati.

APPROFONDIMENTO OPERATIVO

- Analisi dettagliata dell'argomento trattato.
- Esempi pratici applicati a KVM e Windows Server.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.

MONITORAGGIO RISORSE HOST

- Monitoraggio risorse host: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.

MONITORAGGIO INTERNO VM

- Monitoraggio interno VM: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.

LOGGING E TROUBLESHOOTING

- Logging e troubleshooting: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.

HARDENING VM

- Hardening VM: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.

AGGIORNAMENTI E PATCHING

- Aggiornamenti e patching: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.



GESTIONE UTENTI E PRIVILEGI

- Gestione utenti e privilegi: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.

DOCUMENTAZIONE CONFIGURAZIONI

- Documentazione configurazioni: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.



NAMING CONVENTION PROFESSIONALE

- Naming convention professionale: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.

BEST PRACTICE GENERALI

- Best practice generali: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.

ERRORI COMUNI IN LABORATORIO

- Errori comuni in laboratorio: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.



SCENARIO AZIENDALE REALE

- Scenario aziendale reale: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.



LABORATORIO: CREAZIONE TEMPLATE

- Laboratorio: creazione template: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.



LABORATORIO: CLONE VM

- Laboratorio: clone VM: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.

LABORATORIO: SNAPSHOT E ROLLBACK

- Laboratorio: snapshot e rollback: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.



LABORATORIO: ESPANSIONE DISCO

- Laboratorio: espansione disco: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.



ANALISI PERFORMANCE

- Analisi performance: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.

SICUREZZA NELLA GESTIONE VM

- Sicurezza nella gestione VM: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.

PREPARAZIONE ALLA SEGMENTAZIONE RETE

- Preparazione alla segmentazione rete: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.



RIEPILOGO FINALE

- Riepilogo finale: analisi tecnica e operativa.
- Descrizione dettagliata del concetto applicato in ambienti virtualizzati.
- Implicazioni sulla sicurezza e sulla gestione delle risorse.