



# PROGETTO "HP FORTRESS" - TECHNICAL DOCUMENTATION

Author: Alessandro Mainardi | Status: Draft | Version: 1.0

---

## 1. Project Overview (Executive Summary)

- 1.1 Scopo del Progetto: Perché esiste questo server? (Lab didattico + Home Production).
- 1.2 Requisiti Funzionali: Cosa deve fare? (NAS, Plex, Backup iOS, SQL Dev, Virtualization).
- 1.3 Vincoli: Budget (<600€), Consumi, Rumorosità.

## 2. Hardware Architecture (Physical Layer)

- 2.1 Bill of Materials (BOM): Lista componenti, costi, link acquisto.
- 2.2 Specifiche Tecniche: CPU, RAM, Storage Topology.
- 2.3 BIOS & Firmware Configuration: Settings critici (Virtualization, C-States, Secure Boot).
- 2.4 Port Map: Cosa è collegato dove (USB, Ethernet).

## 3. Host System Configuration (Hypervisor Layer)

- 3.1 Operating System: Windows Server 2025 Datacenter (Version, Build, Key Source).
- 3.2 Network Configuration (Host): IP Statico, Driver manuali, Virtual Switch (vSwitch) topology.
- 3.3 Storage Strategy (Software Defined Storage):
  - Storage Spaces Direct / Pools.
  - Virtual Disks & Mirroring (RAID 1).
  - ReFS & Volume Configuration.

## 4. File System & Data Governance

- 4.1 Directory Structure: L'albero delle cartelle su D: (MEDIA, FAMILY, DEV).
- 4.2 Identity & Access Management (IAM):
  - Lista Utenti (Locali vs AD).
  - Matrice dei Permessi (ACLs): Chi può leggere/scrivere cosa.
- 4.3 Sharing Protocols: Configurazione SMB/CIFS (Visibility, ABE).

## 5. Virtualization Strategy (Workloads)

- 5.1 VM Inventory: Lista delle VM pianificate (DC, Linux/Docker, SQL).
- 5.2 Resource Allocation: vCPU, RAM (Dynamic vs Static), VHDX locations.
- 5.3 Services Catalog:
  - Plex (Configurazione transcodifica).
  - Immich (o Backup Manuale iOS).
  - SQL Server (Standard vs Developer instances).

## 6. Network & Connectivity

- 6.1 IP Plan: Tabella degli indirizzi IP statici (Host, VMs, iLO/AMT).
- 6.2 Remote Access: Tailscale (Subnet Routers, ACLs).
- 6.3 Public Exposure: Cloudflare Tunnels (se esponi il portfolio).
- 6.4 DNS & DHCP: Ruolo del Domain Controller vs Router ISP.

## 7. Backup & Disaster Recovery (DR)

- 7.1 Backup Strategy (3-2-1): Cosa, Dove, Quando.
- 7.2 Veeam Configuration: Job settings.
- 7.3 Runbooks (Procedure di Emergenza):
  - *Scenario A*: Rottura di un disco HDD (Procedura di sostituzione e rebuild).
  - *Scenario B*: Corruzione OS Host (Reinstallazione senza perdere i dati).
  - *Scenario C*: Ransomware (Recovery da Shadow Copies/Veeam).

## 8. Conclusions & Critical Takeaways

- 8.1 Executive Summary.
- 8.2 The "Golden Rules" (Fattori Critici di Successo).
- 8.3 Maintenance Schedule (Routine Operativa) .
- 8.4 Future Roadmap (Possibili Espansioni).

# 1. Project Overview

## 1.1 Scopo del Progetto

Il progetto "HP Fortress" nasce con l'obiettivo di progettare e implementare un'infrastruttura server on-premise ibrida, destinata a servire due scopi distinti e paralleli:

1. Educational & Engineering Lab: Una piattaforma di virtualizzazione Enterprise per lo studio pratico di tecnologie Microsoft (Windows Server 2025, Active Directory, Hyper-V, SQL Server) e Linux/Docker, simulando scenari di deployment reali per lo sviluppo software e l'amministrazione di sistema.
2. Home Production Environment: Un sistema centralizzato di archiviazione dati (NAS) ad alta affidabilità per la gestione dei backup familiari (dispositivi mobili e PC) e la distribuzione di contenuti multimediali (Media Server), garantendo la sovranità dei dati e l'indipendenza dai servizi cloud pubblici.

L'infrastruttura è progettata per operare 24/7, garantendo la segregazione logica tra l'ambiente di "Sviluppo" e l'ambiente di "Produzione Domestica" tramite permessi e virtualizzazione.

## 1.2 Requisiti Funzionali

Il sistema deve soddisfare i seguenti requisiti mandatori:

- Storage Resiliente: Implementazione di un RAID 1 (Mirroring) software-defined per la protezione contro il guasto di un singolo disco fisico, utilizzando file system con integrità dei dati (ReFS).
- Virtualizzazione: Capacità di ospitare ed eseguire simultaneamente molteplici Macchine Virtuali (Windows Server e Linux) per servizi di rete (DC, DNS) e applicativi (Docker, SQL).
- Centralized Backup Hub: Supporto nativo per il backup via protocollo SMB per dispositivi iOS (iPhone/iPad) e Windows, con gestione granulare dei permessi (ACL) per garantire la privacy tra i diversi membri della famiglia.
- Media Streaming: Transcodifica e streaming di contenuti video (Plex) sfruttando l'accelerazione hardware (Intel QuickSync) ove possibile.
- Development Environment: Hosting di istanze SQL Server (Developer/Standard) e Web Server per il portfolio personale e progetti universitari.
- Accesso Remoto Sicuro: Accessibilità ai servizi dall'esterno della rete locale senza esposizione diretta di porte critiche (tramite VPN/Tunneling).

## 1.3 Vincoli e Presupposti

Il progetto deve rispettare i seguenti vincoli tecnici ed economici:

- Budget Cap: Costo totale dell'hardware (Server + Storage + Memory) rigorosamente inferiore a € 600,00.
- Hardware Form Factor: Utilizzo di workstation Enterprise ricondizionate (HP EliteDesk Tower) per bilanciare costi, espandibilità e consumi energetici, accettando l'assenza di funzionalità server-grade native (IPMI/iLO, ECC RAM, Redundant PSU).
- Licensing: Utilizzo esclusivo di licenze Microsoft Education (Azure Dev Tools for Teaching) per il layer software, vincolando l'uso a scopi non commerciali diretti.
- Ambiente Fisico: Il server opererà in ambiente domestico residenziale; pertanto, le emissioni acustiche e termiche devono essere contenute.

## 2. Hardware Architecture

### 2.1 Bill of Materials (BOM)

Elenco della componentistica hardware acquisita per la realizzazione del nodo server.

Componente	Modello / Specifica	Ruolo	Stato
Compute Node	HP EliteDesk 800 G4 Tower	Chassis & Motherboard (Q370 Chipset)	Refurbished
CPU	Intel Core i5-8500 (6 Cores, 3.0/4.1 GHz, 9MB Cache)	Processing Unit	OEM Included
RAM (Bank A)	16 GB DDR4 2666 MHz UDIMM (Samsung/OEM)	Memory	OEM Included
RAM (Bank B)	16 GB DDR4 2666 MHz UDIMM (Kingston/Crucial)	Memory Expansion	New
Boot Storage	512 GB M.2 NVMe SSD	Host OS & VMs vDisk	OEM Included

Data Storage 1	WD Red Plus 4TB (WD40EFPX) - CMR	NAS Storage (Mirror A)	New
Data Storage 2	WD Red Plus 4TB (WD40EFPX) - CMR	NAS Storage (Mirror B)	New
Accessori	Cavi SATA III, Viti HP Grommet, Pasta Termica	Assembly	New

## 2.2 Specifiche Tecniche del Nodo

- Total Memory: 32 GB DDR4 (Dual Channel Config).
- Total Storage Raw: ~8.5 TB (0.5 TB NVMe + 8 TB HDD).
- Network Interface: 1x Intel I219-LM Gigabit Ethernet (Onboard).
- Expansion Slots:
  - 2x PCIe x16 (wired x16/x4) - *Disponibili per future espansioni (10GbE NIC / NVMe Adapter).*
  - 2x PCIe x1 - *Disponibili.*
  - 2x M.2 2280 PCIe (1 occupato da Boot Drive).

## 2.3 BIOS & Firmware Configuration (UEFI Settings)

Configurazione obbligatoria del BIOS HP per abilitare le funzionalità Server/Virtualization.

- Security > Secure Boot Configuration:
  - Legacy Support: Disabled (Obbligatorio per Server 2025).
  - Secure Boot: Enabled.
- Advanced > System Options:
  - Virtualization Technology (VTx): Enabled (Critico per Hyper-V).
  - Virtualization Technology for Directed I/O (VTd): Enabled.
- Advanced > Built-in Device Options:
  - Video memory size: 64MB/Minimo (Risparmia RAM di sistema, il server è headless).
- Advanced > Power Management Options:
  - Runtime Power Management: Disabled (Massime prestazioni).
  - Extended Idle Power States (C-States): Disabled (Riduce la latenza).
- Advanced > Boot Options:
  - After Power Loss: Power On (Il server deve riaccendersi da solo dopo un blackout).

## 2.4 Port Map & Storage Topology

Mappatura fisica delle connessioni SATA per facilitare la manutenzione.

- SATA 0 (Blue): *Vuoto* (o DVD Drive se presente).
- SATA 1 (Dark Blue): WD Red Plus 4TB (Disk 1) -> Bay 3.5" Primario.
- SATA 2 (Light Blue): WD Red Plus 4TB (Disk 2) -> Bay 3.5" Secondario.
- M.2 Slot 1: NVMe SSD 512GB (Boot).

## 3. Host System Configuration (Hypervisor Layer)

### 3.1 Operating System

Configurazione del sistema operativo "Bare Metal". L'Host deve rimanere il più pulito possibile, delegando i servizi applicativi alle macchine virtuali.

- OS Version: Windows Server 2025 Datacenter (Desktop Experience).
- Build Channel: Long-Term Servicing Channel (LTSC).
- Licensing: Academic / Volume License (Azure Dev Tools for Teaching).
- Hostname: **HV-NODE-01** (Hyper-V Node 01).
- Role: Hyper-V Host & Storage Server (File Services).
- Local Administrator: **.\Administrator** (Da utilizzare solo per manutenzione d'emergenza o configurazione iniziale).

### 3.2 Network Configuration (Physical Host)

Configurazione della connettività fisica e logica dell'Host.

- Physical Interface (NIC): Intel Ethernet Connection I219-LM.
  - o *Driver Note*: Installazione forzata manuale dei driver Intel (versione Windows 10/11 64-bit) tramite **devmgmt.msc** per bypassare il check di compatibilità Server OS.
- IP Addressing Strategy: Statico.
  - o IP Address: **192.168.1.10** (Esempio - Da confermare in base alla subnet).
  - o Subnet Mask: **255.255.255.0**
  - o Gateway: **192.168.1.1** (Router ISP).

- o DNS Primario: 127.0.0.1 (Dopo la promozione a DC della VM) o 1.1.1.1 (Iniziale).
- Virtual Switch Topology:
  - o Name: vSwitch\_External
  - o Type: External Network.
  - o Configuration: "Allow management operating system to share this network adapter" = Enabled. (L'Host condivide la porta fisica con le VM).

### 3.3 Storage Strategy (Software Defined Storage)

Implementazione dello storage resiliente tramite tecnologia Microsoft Storage Spaces. Il controller RAID hardware del BIOS è disabilitato/non utilizzato (AHCI Mode).

- Storage Pool:
  - o Name: SP\_DATA\_01
  - o Physical Disks: 2x WD Red Plus 4TB.
  - o Type: Primordial Pool.
- Virtual Disk (LUN):
  - o Name: vDisk\_Data
  - o Layout: Mirror (2-Way Mirroring - Equivalente RAID 1).
  - o Provisioning: Thin (Allocazione dinamica).
- Volume & File System:
  - o Drive Letter: D:
  - o Label: DATA
  - o File System: ReFS (Resilient File System).
  - o Features Abilitate: Integrity Streams (Protezione Bit-rot), Data Deduplication (Opzionale, per cartelle ISO/Backup).

### 3.4 Security Hardening (Host Level)

Misure di sicurezza di base applicate all'Host fisico.

- Remote Access: Remote Desktop (RDP) abilitato solo per amministratori.

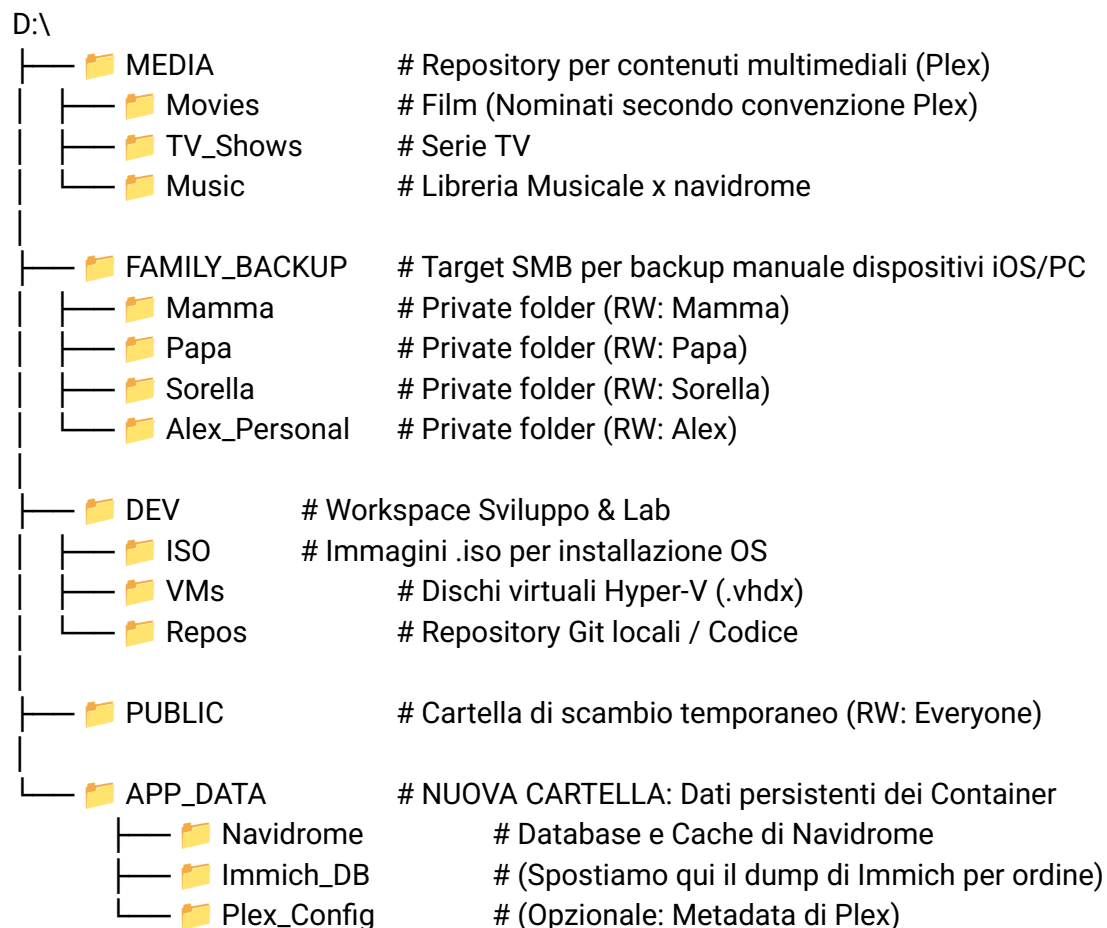
- Firewall: Windows Defender Firewall attivo. Regole inbound limitate a RDP, SMB (File Sharing) e gestione Hyper-V.
- Updates: Windows Update configurato per download automatico ma installazione/riavvio manuale (per evitare riavvii imprevisti durante lo streaming Plex).

## 4. File System & Data Governance

### 4.1 Directory Structure (Volume D:)

Organizzazione logica del volume dati RAID 1 (D: [DATA]). La struttura è progettata per segregare i carichi di lavoro (Media, Backup, Dev) e facilitare la gestione dei permessi.

#### SCHEMA LOGICO:



### 4.2 Identity & Access Management (IAM)

Strategia di gestione delle identità. Gli utenti "Consumer" (Famiglia) sono definiti come Utenti Locali sull'Host per garantire accesso anche senza Domain Controller.



## User Inventory:

| Username | Tipo | Ruolo | Note |

| :-- | :-- | :-- | :-- |

| u\_alex | Local Admin | System Owner | Accesso completo a tutto (Full Control). |

| u\_mamma | Local User | Consumer | Accesso RW alla propria cartella, RO ai Media. |

| u\_papa | Local User | Consumer | Accesso RW alla propria cartella, RO ai Media. |

| u\_sorella | Local User | Consumer | Accesso RW alla propria cartella, RO ai Media. |

| svc\_plex | Service Account | Daemon | Utente dedicato per il servizio Plex. |

| svc\_immich | Service Account | Daemon | Utente dedicato per il mount SMB della VM Linux.

|

## Permission Matrix (ACLs):

Configurazione dei permessi NTFS. L'ereditarietà (Inheritance) viene disabilitata nelle sottocartelle di FAMILY\_BACKUP per garantire privacy rigorosa.

Path	Principal	Access Level	Scopo
D:\MEDIA	Everyone	Read & Execute	Streaming / Visione.
D:\MEDIA	u_alex	Modify	Gestione libreria.
D:\FAMILY_BACKUP\Mamma	u_mamma	Modify	Backup foto personale.
D:\FAMILY_BACKUP\Papa	u_papa	Modify	Backup foto personale.
D:\FAMILY_BACKUP\Sorella	u_sorella	Modify	Backup foto personale.
D:\FAMILY_BACKUP\Alex_Pers	u_alex	Full Control	Backup personale.
D:\DEV	u_alex	Full Control	Sviluppo esclusivo.

D:\IMMICH_DATA	svc_immich	Modify	Scrittura dati da container Docker.
----------------	------------	--------	-------------------------------------

### 4.3 Sharing Protocols & Configuration

Configurazione del protocollo SMB per l’esposizione in rete.

- Share Name: FAMILY\_BACKUP (Mappa a D:\FAMILY\_BACKUP)
- Share Name: MEDIA (Mappa a D:\MEDIA)
- Feature Abilitata: Access-Based Enumeration (ABE).
  - o Funzione: Gli utenti vedono nell’elenco file *solo* le cartelle per cui hanno permessi di lettura. Le cartelle degli altri membri della famiglia risultano invisibili.
- Network Discovery: Abilitato su profilo “Private Network”.

## 5. Virtualization Strategy (Workloads)

### 5.1 VM Inventory

Elenco delle Macchine Virtuali (Guest OS) pianificate per il deployment iniziale.

VM Name	OS Family	Ruolo	Priority	Note
VM-DC-01	Windows Server 2025	Domain Controller, DNS, DHCP	High	Infrastruttura Core.
VM-LINUX-01	Ubuntu Server 24.04 LTS	Docker Host (Media, Backup, Tunnel)	Medium	Gestione servizi Casa.
VM-SQL-01	Windows Server 2025	SQL Server (Dev/Std), IIS (Portfolio)	Low	Lab Sviluppo & DB.

### 5.2 Resource Allocation Plan

Strategia di assegnazione risorse CPU/RAM (Host Total: 6 Core / 32 GB RAM).

VM Name	vCPU	RAM (Startup)	RAM (Min/Max)	Disk (VHDX)	Network
VM-DC-01	2 vCPU	4 GB	Dynamic (2GB – 6GB)	60 GB (OS)	vSwitch_External
VM-LINUX-01	4 vCPU	8 GB	Dynamic (4GB – 12GB)	50 GB (OS)	vSwitch_External
VM-SQL-01	4 vCPU	8 GB	Static 8 GB	100 GB (OS+DB)	vSwitch_External

## 5.3 Services Catalog (Application Layer)

Dettaglio dei servizi applicativi eseguiti all'interno delle VM.

### A. VM-LINUX-01 (Docker Environment)

Questa VM funge da motore per i container e monta via SMB le cartelle dati dall'Host fisico.

- Plex Media Server:
  - *Scopo:* Streaming Video (Film/Serie TV) con transcodifica.
  - *Mount SMB:* `/mnt/media $to$ \\HOST\MEDIA`
  - *Porta:* 32400 (TCP)
- Navidrome:
  - *Scopo:* Streaming Audio/Music Server (Spotify self-hosted).
  - *Mount SMB:* `/mnt/media/Music $to$ \\HOST\MEDIA\Music`
  - *Data Persistence:* `/data $to$ \\HOST\APP_DATA\Navidrome` (Database/Cache)
  - *Porta:* 4533 (TCP)
- Immich (Photo Backup):
  - *Scopo:* Backup automatico foto/video da iOS/Android con Machine Learning.
  - *Mount SMB:* `/mnt/immich $to$ \\HOST\IMMICH_DATA`
  - *Data Persistence:* `/postgres_dump $to$ \\HOST\APP_DATA\Immich_DB`
  - *Porta:* 2283 (TCP)
- Cloudflare Tunnel (cloudflared):
  - *Scopo:* Esposizione sicura dei servizi web (es. Portfolio) su internet senza Port Forwarding sul router (Zero Trust Network Access).

### B. VM-SQL-01 (Development Lab)

Ambiente Windows Server dedicato allo sviluppo .NET e Database.

- SQL Server Instance:
  - *Edizione*: Developer (per test feature Enterprise) o Standard (per test limiti produzione).
  - *Instance Name*: **MSSQLSERVER** (Default Instance).
  - *Auth Mode*: Mixed (Windows Authentication + SQL Server Authentication).
  - *Porta*: 1433 (TCP).
- Web Server (IIS):
  - *Scopo*: Hosting del portfolio personale e progetti web.
  - *Binding*: HTTP (80), HTTPS (443 - gestito internamente o via Tunnel).

## 5.4 Automatic Virtual Machine Activation (AVMA)

Le VM Windows Server (**VM-DC-01**, **VM-SQL-01**) verranno attivate automaticamente tramite la licenza Datacenter dell'Host fisico.

# 6. Network & Connectivity

## 6.1 IP Addressing Plan (IPv4)

Schema di indirizzamento statico per l'infrastruttura server. Il DHCP del router ISP viene limitato al range **.100 - .254** per lasciare liberi gli indirizzi bassi per i server.

Subnet: 192.168.1.0/24 (Esempio standard, adattare alla rete reale).

Gateway: 192.168.1.1 (Router ISP).

Device / VM	Hostname	Static IP	Ruolo	Porta Servizi Principali
Physical Host	<b>HV-NODE-01</b>	.10	Hypervisor / Storage	RDP (3389), SMB (445)
VM-DC-01	<b>DC-01</b>	.11	Domain Controller / DNS	DNS (53), LDAP (389)
VM-LINUX-01	<b>LINUX-01</b>	.12	Docker Host	Plex (32400), Immich (2283), Navidrome (4533)
VM-SQL-01	<b>SQL-01</b>	.13	Database / Web	SQL (1433), HTTP (80)

## 6.2 DNS Strategy (Internal & External)

Gestione della risoluzione nomi per garantire il funzionamento di Active Directory e l'accesso ai servizi.

- Internal DNS Authority: **VM-DC-01** (192.168.1.11).
  - o *Configurazione*: Tutti i server (Host e altre VM) devono avere **.11** come DNS Primario per risolvere il dominio **home.alexmaina.dev**.
  - o *Forwarders*: Il DC inoltra le richieste esterne a **1.1.1.1** (Cloudflare) o **8.8.8.8** (Google).
- Split-DNS:
  - o Internamente: **plex.home.alexmaina.dev** risolve sull'IP locale **.12**.
  - o Esternamente: Gestito da Cloudflare (vedi 6.4).

## 6.3 Remote Access (Private - Admin & Family)

Accesso sicuro alla rete domestica per amministrazione e backup (iPhone) senza esporre porte sul router.

- Tecnologia: Tailscale (Mesh VPN).
- Deployment Point: Installato su **VM-LINUX-01** configurato come Subnet Router.
  - o *Command*: **tailscale up --advertise-routes=192.168.1.0/24**
  - o *Funzione*: Permette ai dispositivi autorizzati (il tuo Laptop, iPhone di Mamma) di accedere agli IP locali (**192.168.1.x**) ovunque si trovino, come se fossero a casa.
- Use Case:
  - o Backup Foto Immich/SMB da remoto.
  - o Streaming Navidrome/Plex sicuro fuori casa.
  - o RDP verso i server per manutenzione.

## 6.4 Public Exposure (Ingress - Portfolio)

Esposizione selettiva dei servizi web pubblici (Portfolio) al mondo internet.

- Tecnologia: Cloudflare Tunnel (**cloudflared**).
- Deployment Point: Container Docker su **VM-LINUX-01** o servizio su **VM-SQL-01**.
- Configurazione Tunnel (Zero Trust):
  - o Nessun Port Forwarding sul Router ISP.
  - o Il tunnel instaura una connessione in uscita verso l'edge di Cloudflare.
- Public Mapping:
  - o **https://alexmaina.dev** -> Tunnel -> **http://192.168.1.13:80** (Portfolio su IIS).

- o <https://immich.alexmaina.dev> -> Tunnel -> <http://192.168.1.12:2283> (Opzionale, protetto da Cloudflare Access).

## 6.5 Firewall Rules (Internal Traffic)

Regole da applicare sui Firewall dei Guest OS (Windows Defender / UFW) per permettere il traffico interno.

- VM-LINUX-01 (UFW/Docker):
  - o Allow TCP 32400 (Plex) from [192.168.1.0/24](#).
  - o Allow TCP 2283 (Immich) from [192.168.1.0/24](#).
  - o Allow TCP 4533 (Navidrome) from [192.168.1.0/24](#).
- VM-SQL-01 (Windows Firewall):
  - o Allow TCP 1433 (SQL Server) from [192.168.1.0/24](#).
  - o Allow TCP 80/443 (IIS) from [192.168.1.0/24](#) e dal IP del Tunnel.

## 7. Backup & Disaster Recovery (DR)

### 7.1 Backup Strategy (The 3-2-1 Rule)

Strategia di protezione dei dati per garantire la Business Continuity domestica e la sopravvivenza dei dati critici (Foto, Documenti, Codice).

- 3 Copie dei Dati:
  1. Produzione: Dati vivi su RAID 1 ReFS ([D:](#)).
  2. Backup Locale (On-Site): Copia su Disco USB Esterno (Offline/Air-gapped quando possibile).
  3. Backup Remoto (Off-Site): Copia dei soli dati critici (Documenti/Foto) su Cloud (es. OneDrive Education 1TB) o su un secondo disco tenuto in altra locazione fisica.
- Tooling:
  - o Veeam Backup & Replication (Community Edition): Software Enterprise (Gratuito fino a 10 Workload) installato sull'Host fisico. Gestisce backup di VM e File.
  - o Volume Shadow Copies (VSS): Snapshot orari del volume [D:](#) per recupero rapido file cancellati/sovrascritti.

### 7.2 Backup Jobs Configuration

Configurazione dei task automatici di salvataggio.

Job Name	Source	Destination	Schedule	Retention	Scopo
----------	--------	-------------	----------	-----------	-------

BKP-VMs-Daily	Tutte le VM (DC, LINUX, SQL)	USB Drive (Repository)	Daily @ 02:00	14 Giorni	Disaster Recovery intera macchina. Ripristino servizi in caso di crash OS.
BKP-Files-Crit	D:\FAMILY_BACKUP, D:\DEV, D:\APP_DATA	USB Drive + Cloud Sync	Daily @ 04:00	30 Giorni	Protezione dati insostituibili (Foto, Codice).
BKP-Media-Wkly	D:\MEDIA	USB Drive	Weekly (Sun)	2 Versioni	Protezione libreria Plex (bassa priorità, dati rimpiazzabili).
VSS-Snapshots	Volume D:	Local Shadow Storage	Ogni 6 ore	Max Space 10%	"Undo" rapido per errori utente (file cancellati per sbaglio).

*Nota:* I container Docker (Immich/Navidrome) salvano i loro dati in D:\APP\_DATA e D:\IMMICH\_DATA. Backupando quelle cartelle via "BKP-Files-Crit", stai automaticamente salvando lo stato delle applicazioni.

## 7.3 Runbooks (Procedure di Emergenza)

Manuale operativo per il ripristino dei servizi in caso di guasto critico.

### Scenario A: Guasto Disco Fisico (HDD Failure)

*Sintomo:* Windows segnala "Degraded" sul Virtual Disk, LED disco spento/ambra (se presente), rallentamenti.

1. Identificazione: Usare PowerShell `Get-PhysicalDisk` per identificare il seriale del disco guasto (`Lost Communication` o `HealthStatus: Unhealthy`).
2. Sostituzione: Spegnere il server (o hot-swap se supportato). Rimuovere disco guasto, inserire disco nuovo (stessa capacità o superiore).
3. Riparazione (PowerShell):
  - o Aggiungere il nuovo disco al pool: `Add-PhysicalDisk -StoragePoolFriendlyName "SP_DATA_01"`.
  - o Associare il nuovo disco al Virtual Disk.
  - o Rimuovere il vecchio disco logico ("Retired").
  - o Avviare riparazione: `Repair-VirtualDisk -FriendlyName "vDisk_Data"`.

- o Monitorare: [Get-StorageJob](#).

## Scenario B: Corruzione Totale OS Host (Blue Screen of Death)

*Sintomo:* Windows Server non parte più. I dati su **D:** sono intatti ma inaccessibili.

1. Reinstallazione: Installare Windows Server 2025 pulito su NVMe.
2. Importazione Storage: In *Server Manager* > *Storage Pools*, fare tasto destro sul Pool rilevato -> "Attach Virtual Disk". Il volume **D:** torna online con tutti i dati intatti (grazie ai metadati su disco).
3. Restore VM: Importare le VM in Hyper-V puntando alla cartella **D:\DEV\VMs**.
4. Restore Config: Riconfigurare IP statico e Share.

## Scenario C: Attacco Ransomware

*Sintomo:* File con estensioni strane, richiesta riscatto, file inaccessibili.

1. ISOLAMENTO: Staccare cavo di rete IMMEDIATAMENTE.
2. Verifica VSS: Controllare "Versioni Precedenti" su **D:**. Se intatte, ripristinare.
3. Veeam Restore: Se VSS è compromesso, usare la console Veeam per fare "File Level Restore" o "VM Restore" dal disco USB (che idealmente dovrebbe essere scollegato quando non in uso, o marcato come "Offline" se Veeam lo supporta).
4. Bonifica: Piallare l'OS infetto e reinstallare da zero prima di ripristinare i dati.

# 8. Conclusions & Critical Takeaways

## 8.1 Executive Summary

Il progetto "HP Fortress" ha trasformato con successo una workstation aziendale dismessa in un'infrastruttura di virtualizzazione di classe Enterprise. Con un investimento hardware inferiore ai € 600, è stato realizzato un sistema capace di erogare servizi che in ambito commerciale richiederebbero budget decuplicati. L'architettura ibrida (Windows Server Datacenter + Linux Docker) garantisce il perfetto equilibrio tra la necessità didattica di un laboratorio Microsoft e la flessibilità dei moderni servizi containerizzati per l'uso domestico.

## 8.2 The "Golden Rules" (Fattori Critici di Successo)

Per mantenere l'integrità e la disponibilità del sistema nel tempo, è imperativo rispettare le seguenti regole operative:

1. RAID non è Backup: La configurazione Mirror (RAID 1) protegge dalla rottura fisica di un disco, ma non protegge da cancellazioni accidentali, corruzione file system o ransomware. La strategia di backup 3-2-1 (Veeam + USB) è l'unica vera assicurazione sulla vita dei dati.



2. Sovranità delle Licenze: L'accesso al portale *Azure* è temporaneo , ma le Product Key sono perpetue. È mandatorio aver salvato tutte le chiavi in un Password Manager sicuro esterno al server stesso.
3. Segregazione dei Ruoli: L'Host fisico (**HV-NODE-01**) deve rimanere un'entità "pura", dedicata esclusivamente alla gestione di Hyper-V e Storage. Tutti i servizi applicativi (Plex, SQL, Web) devono risiedere all'interno delle VM.
4. Zero Trust Networking: L'accesso remoto deve avvenire esclusivamente tramite tunnel sicuri (Tailscale / Cloudflare Tunnel).

## 8.3 Maintenance Schedule (Routine Operativa)

Il server richiede una manutenzione programmata per garantire stabilità e sicurezza.

- Mensile:
  - o Installazione Patch di Sicurezza Windows Server (Host e VM Guest). *Nota: Riavviare prima le VM, poi l'Host.*
  - o Aggiornamento container Docker
  - o Verifica visiva dello stato dei dischi fisici (LED e SMART status).
- Trimestrale:
  - o Restore Test: Provare a ripristinare un file a caso dal backup Veeam per assicurarsi che i backup siano leggibili. Un backup non testato è un backup inesistente.
  - o Pulizia fisica: Rimozione polvere dalle ventole e dai filtri dell'HP EliteDesk (i server domestici soffrono la polvere più dei datacenter).
- Annuale:
  - o Review delle licenze e scadenze certificati.
  - o Aggiornamento della documentazione tecnica (questo documento) se sono state fatte modifiche all'architettura.

## 8.4 Future Roadmap (Possibili Espansioni)

Il sistema è progettato per essere scalabile. Upgrade futuri consigliati:

· Networking: Aggiunta scheda di rete 2.5GbE ·

Compute: Espansione RAM a 64GB (sostituendo i banchi attuali) per ospitare laboratori Kubernetes o EVE-NG complessi.

1. Project Overview
  - 1.1 Scopo del Progetto
  - 1.2 Requisiti Funzionali
  - 1.3 Vincoli e Presupposti
2. Hardware Architecture
  - 2.1 Bill of Materials (BOM)
  - 2.2 Specifiche Tecniche del Nodo
  - 2.3 BIOS & Firmware Configuration (UEFI Settings)
  - 2.4 Port Map & Storage Topology
3. Host System Configuration (Hypervisor Layer)
  - 3.1 Operating System
  - 3.2 Network Configuration (Physical Host)
  - 3.3 Storage Strategy (Software Defined Storage)
  - 3.4 Security Hardening (Host Level)
4. File System & Data Governance
  - 4.1 Directory Structure (Volume D:)
  - 4.2 Identity & Access Management (IAM)
  - 4.3 Sharing Protocols & Configuration
5. Virtualization Strategy (Workloads)
  - 5.1 VM Inventory
  - 5.2 Resource Allocation Plan
  - 5.3 Services Catalog (Application Layer)
  - 5.4 Automatic Virtual Machine Activation (AVMA)
6. Network & Connectivity
  - 6.1 IP Addressing Plan (IPv4)
  - 6.2 DNS Strategy (Internal & External)
  - 6.3 Remote Access (Private - Admin & Family)
  - 6.4 Public Exposure (Ingress - Portfolio)
  - 6.5 Firewall Rules (Internal Traffic)
7. Backup & Disaster Recovery (DR)
  - 7.1 Backup Strategy (The 3-2-1 Rule)
  - 7.2 Backup Jobs Configuration
  - 7.3 Runbooks (Procedure di Emergenza)
8. Conclusions & Critical Takeaways
  - 8.1 Executive Summary
  - 8.2 The "Golden Rules" (Fattori Critici di Successo)
  - 8.3 Maintenance Schedule (Routine Operativa)
  - 8.4 Future Roadmap (Possibili Espansioni)