



# PROGETTO "HP FORTRESS" - TECHNICAL DOCUMENTATION

Author: Alessandro Mainardi | Status: Final | Version: 2.0 | Data: 28 gen 2026

---

## 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 (temporaneamente disattivato), 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(deactivated)).
- 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 - al momento non attivo).

## 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 (all'occorrenza) 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.

CRITICAL RISK ACCEPTANCE (POWER): L'infrastruttura non dispone di un gruppo di continuità (UPS).

- Rischio: In caso di interruzione improvvisa dell'alimentazione, il volume ReFS e i database SQL in memoria (Write-Back caching) sono esposti a rischio di corruzione.
- Mitigazione: Il sistema è configurato per *non* riavviarsi automaticamente in caso di alimentazione instabile ("Stay Off" dopo Power Loss nel BIOS) per evitare danni da sbalzi ripetuti (brownouts), a meno che non sia strettamente necessario per l'accesso remoto. Backup frequenti sono l'unica garanzia.

## 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 i7-8700k       | Processing Unit                      | OEM Included |



|                |  |                        |                     |
|----------------|--|------------------------|---------------------|
| RAM (Bank A)   | 2x8 GB DDR4 2666 MHz<br>UDIMM (Samsung/OEM)      | Memory                 | OEM Included        |
| RAM (Bank B)   | 2x8 GB DDR4 2666 MHz<br>UDIMM (Kingston/Crucial) | Memory Expansion       | New (se necessario) |
| Boot Storage   | 2x512 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: 16 GB DDR4 (Dual Channel Config). (+16gb se necessari)
- Total Storage Raw: ~9 TB (2x512 GB NVMe + 2x4 TB HDD).
- Network Interface: 1x Intel I219-LM Gigabit Ethernet (Onboard).  
+ 2x10 Gbit/s ports board OEM included
- Expansion Slots:
  - 2x PCIe x16 (wired x16/x4) - *Disponibili per future espansioni (1 occupato da scheda 10G)*
  - 2x PCIe x1 - *Disponibili.*
  - 2x M.2 2280 PCIe (2 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
- 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).
- M.2 Slot 2: 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).

DNS Configuration Strategy (Host Physics): Per evitare dipendenze circolari (dove l'Host attende la VM per risolvere i nomi), la configurazione DNS dell'interfaccia fisica dell'Host segue questa priorità:

1. Primary DNS: `127.0.0.1` (o IP statico di VM-DC-01) - *Necessario per l'integrazione in Dominio.*
2. Secondary DNS: `1.1.1.1` (Cloudflare Public) - *Necessario per permettere all'Host di contattare servizi critici (Tailscale, NTP, Windows Update) anche se la VM Domain Controller è offline o in boot.*

### 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).

Encryption & Physical Security:

- BitLocker Drive Encryption: Attivo su volume di avvio (C:) e volumi dati (D:).
- Algoritmo: XTS-AES 256-bit (Massima protezione, impatto CPU trascurabile con i5-8500).
- Key Management:
  - o TPM 2.0: Sblocco automatico all'avvio (protezione contro furto disco).
  - o Recovery Keys: Salvate su supporto esterno crittografato (USB FIDO2 token) e stampate in copia cartacea (Safe Box). MAI salvare le chiavi sul server stesso.

# 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:

```
D:\|
 └── MEDIA          # Repository per contenuti multimediali (Plex)
     ├── Movies       # Film (Nominati secondo convenzione Plex)
     ├── TV_Shows     # Serie TV
     └── Music         # Libreria Musicale x navidrome

 └── FAMILY_BACKUP  # Target SMB per backup manuale dispositivi iOS/PC
     ├── Mamma        # Private folder (RW: Mamma)
     ├── Papa          # Private folder (RW: Papa)
     ├── Sorella       # Private folder (RW: Sorella)
     └── Alex_Personal # Private folder (RW: Alex)

 └── DEV            # Workspace Sviluppo & Lab
     ├── ISO           # Immagini .iso per installazione OS
     ├── VMs           # Dischi virtuali Hyper-V (.vhdx)
     └── Repos          # Repository Git locali / Codice

 └── PUBLIC          # Cartella di scambio temporaneo (RW: Everyone)

 └── APP_DATA        # NUOVA CARTELLA: Dati persistenti dei Container
     ├── Navidrome    # Database e Cache di Navidrome
     ├── Immich_DB     # (Spostiamo qui il dump di Immich per ordine)
     └── Plex_Config   # (Opzionale: Metadata di Plex)
```

## 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).
  - 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)                | Low      | Lab Sviluppo & DB.<br>(all'occorrenza, non attivo sempre) |

### 5.2 Resource Allocation Plan

Strategia di assegnazione risorse CPU/RAM (Host Total: 6 Core / 16 GB RAM).

| VM Name                   | vCPU         | RAM (Startup) | RAM (Min/Max)         | Disk (VHDX)  | Network          |
|---------------------------|--------------|---------------|-----------------------|--------------|------------------|
| VM-DC-01                  | 2 vCPU       | 2 GB          | Dynamic (2 GB – 4 GB) | 60 GB (OS)   | vSwitch_External |
| VM-LINUX-01               | 4 vCPU       | 4 GB          | Dynamic (4 GB – 8 GB) | 50 GB (OS)   | vSwitch_External |
| VM-SQL-01<br>(NON ATTIVO) | (non attivo) | (NON ATTIVO)  | (NON ATTIVO)          | (NON ATTIVO) | 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).

Altri container che saranno presenti:

| Service  | Port | Access       | Purpose  |
|----------|------|--------------|--|
| Homepage | 3000 | Internal/VPN | Dashboard centralizzata per stato servizi e link rapidi. |

### B. VM-SQL-01 (Development Lab) (ATTIVO SOLO SE NECESSARIO)

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).

## 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)                                    |

## 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://music.alexmaina.dev> -> Tunnel -> <http://192.168.1.12:4533> (Opzionale, protetto da Cloudflare Access).
  - 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/sovrascriviti.

USB Local Backup Hardening: Poiché il drive USB è fisicamente connesso, non costituisce un vero "Air-Gap". Per mitigare il rischio Ransomware:

1. File System Permissions: Il drive USB ha permessi NTFS impostati su "Deny Write" per l'utente standard e l'utente Admin quotidiano.
2. Service Isolation: Solo l'account di servizio SVC\_VEEAM (o System) ha permessi di scrittura esplicativi sulla root del drive USB.



3. Veeam Hardening: I file di backup creati sono impostati come *Read-Only* dopo la scrittura ove possibile, o gestiti tramite Veeam Agent con opzione di espulsione logica del media post-job (se supportata) per ridurre la finestra di attacco.

## 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.

## Procedure 7.3.X: "Bare Metal" Recovery (Total Loss)

In caso di fallimento catastrofico del disco OS (C):

1. Hardware Prep: Sostituire SSD NVMe.
2. OS Install: Installare Windows Server 2025 (stessa edizione). Nome Host *identico* al precedente.
3. Storage Spaces Import:
  - o I dischi dati (HDD) verranno rilevati come "Foreign".



- Powershell: `Get-StoragePool | Set-StoragePool -IsReadOnly $false`
  - Se BitLocker era attivo: `Unlock-BitLocker -MountPoint "D:" -RecoveryPassword [INSERIRE_CHIAVE_RECUPERO]`
4. Hyper-V Import:
    - Ricreare il Virtual Switch "vSwitch-External" mappato sulla NIC fisica corretta.
    - Importare le VM dalla cartella su D: (Select Folder -> "Import Virtual Machine" -> "Register the virtual machine in-place").
  5. Restore: Ripristino Veeam per file mancanti o configurazioni specifiche.

## 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.



# 9. Secure Remote Access & Zero Trust Architecture

## 9.1 Philosophy: The "Invisible Fortress"

L'obiettivo primario della sicurezza perimetrale di HP FORTRESS è l'invisibilità. In un'era di scansioni massive automatizzate (Shodan, botnet), esporre porte sul router ISP (Port Forwarding) è una vulnerabilità inaccettabile.

La strategia adottata è Zero Open Ports: nessun traffico in ingresso è permesso direttamente dal router. Tutto il traffico in entrata deve passare attraverso tunnel crittografati pre-autenticati, suddivisi per vettore di utilizzo.

## 9.2 Architecture Topology

La connettività esterna è segregata in due canali logici distinti ("Split-Tunnel Architecture"):

1. Management Plane (Backend): Gestito via Tailscale. Accesso completo alla rete (Layer 3), riservato all'amministratore.
2. Application Plane (Frontend): Gestito via Cloudflare Tunnel. Accesso puntuale ai servizi Web (Layer 7), protetto da Cloudflare Access (Identity Aware Proxy).

### Diagramma Logico dei Flussi

```
[ INTERNET ]  
|  
+-- [ ROUTE A: TAILSCALE ] (Admin & Backup)  
| |  
| +-- Protocol: WireGuard (UDP)  
| +-- Auth: Node Authentication  
| +-- Entry Point: VM-LINUX-01 (Subnet Router)  
| +-- Target: INTERA LAN 192.168.1.0/24 (RDP, SMB, SQL, SSH)  
|  
+-- [ ROUTE B: CLOUDFLARE ] (Web Services & Sharing)  
| |  
| +-- Protocol: HTTPS/WSS (TCP)  
| +-- Auth: Cloudflare Access (Email OTP / OIDC)  
| +-- Entry Point: VM-LINUX-01 (cloudflared container)  
| +-- Target: SINGOLI SOCKET (HTTP Only)
```

## 9.3 Channel A: The Management Plane (Tailscale)

Tailscale funge da estensione virtuale della LAN fisica. Non è concepito per l'accesso pubblico, ma per l'operatività tecnica e il trasferimento dati "raw".

- Ruolo del Nodo: VM-LINUX-01 (192.168.1.12) agisce come Subnet Router.
- Comando di attivazione: tailscale up --advertise-routes=192.168.1.0/24  
–accept-routes
- Funzionalità Abilitate:
  - MagicDNS: Risoluzione dei nomi host interni.
  - ACLs (Access Control Lists): (Opzionale) Restrizione per impedire a device



meno sicuri (es. telefono sorella) di accedere all'Admin VLAN.

## Use Cases Critici (Solo via Tailscale)

1. RDP (Remote Desktop): Connessione verso l'Host Fisico 192.168.1.10 o la VM SQL 192.168.1.13. MAI esporre la porta 3389 via web.
2. SMB (File Sharing): Accesso ai volumi \\HV-NODE-01\\MEDIA o \\DEV per il trasferimento massivo di file. Il protocollo SMB è insicuro su internet pubblico; encapsulato in WireGuard (Tailscale) è sicuro.
3. Database Management: Accesso diretto alla porta 1433 di SQL Server tramite SSMS dal laptop remoto.

## 9.4 Channel B: The Application Plane (Cloudflare Tunnel)

Cloudflare Tunnel espone servizi specifici al mondo, ma con un livello intermedio di autenticazione ("Zero Trust") che agisce *prima* che la richiesta tocchi il server.

- Agente: Container Docker cloudflared su VM-LINUX-01.
- Sicurezza: Il tunnel crea una connessione *outbound* verso l'edge di Cloudflare. Nessuna necessità di IP Pubblico statico o DDNS.

### Configurazione dei Public Hostnames e Policy

La configurazione delle policy di accesso è il cuore della sicurezza "consapevole". Non trattiamo tutti i sottodomini allo stesso modo.

#### 1. Public Tier (Accesso Libero)

Servizi destinati a essere visti da chiunque (Recruiter, Internet).

- Dominio: alexmaina.dev / www.alexmaina.dev
- Target Interno: http://192.168.1.13:80 (IIS Web Server su VM-SQL).
- Cloudflare Policy: Bypass (Nessuna autenticazione richiesta).
- Security Features: WAF (Web Application Firewall) attivo, Bot Fight Mode attivo, HTTPS forzato all'edge.

#### 2. Private Tier (Accesso Protetto - "Previo Accesso")

Servizi potenti o contenenti dati personali che necessitano di una GUI Web.

- Domini:
  - pdf.alexmaina.dev (Stirling-PDF)
  - immich.alexmaina.dev (Immich Photos)
  - portainer.alexmaina.dev (Gestione Docker)
- Cloudflare Policy: Allow solo se:
  - Selector: Email
  - Value: tua.email@gmail.com (ed eventuali email familiari autorizzate).
- Experience: L'utente visita il sito -> Viene reindirizzato su una pagina di login Cloudflare -> Inserisce email -> Riceve codice OTP -> Se corretto, accede al servizio.
- Vantaggio Critico: Anche se Stirling-PDF ha una vulnerabilità 0-day, l'attaccante non può sfruttarla perché non può nemmeno raggiungere la pagina di login dell'applicazione senza prima autenticarsi su Cloudflare.

#### 3. Hybrid Tier (Plex)



Il caso specifico dello streaming media.

- Dominio: plex.alexmaina.dev
- Configurazione: Plex mal sopporta il caching di Cloudflare.
  - *Opzione A (Consigliata)*: Usare l'app nativa Plex che negozia la connessione automaticamente (Relay).
  - *Opzione B (Tunnel)*: Disabilitare il Caching (Cache Level: Bypass) nelle regole di pagina di Cloudflare per questo sottodomini. Policy: Service Auth (complesso) o Bypass (affidandosi all'auth di Plex).

## 9.5 Security Hardening Checklist (Da eseguire SUBITO)

1. Geofencing (Cloudflare WAF): Crea una regola WAF personalizzata.
  - *Block* traffico proveniente da paesi "ad alto rischio" (Russia, Cina, Corea del Nord, ecc.) se non prevedi di viaggiare lì.
2. HTTPS Strict Transport Security (HSTS): Abilita HSTS su Cloudflare per forzare i browser a usare sempre la crittografia.
3. Tailscale Key Expiry: Disabilita la scadenza delle chiavi ("Key Expiry") per il nodo Server VM-LINUX-01 per evitare che l'accesso remoto si interrompa ogni 90 giorni.
4. Local Firewall Fallback:
  - Su VM-LINUX-01 (UFW), permetti il traffico sulla porta 8080 (Stirling) e 2283 (Immich) SOLO da 127.0.0.1 (il tunnel Docker) e dalla subnet LAN 192.168.1.0/24.
  - Questo impedisce che, se per errore configuri un port forwarding sul router in futuro, i servizi siano esposti "nudi".

## 9.6 Disaster Recovery per l'Accesso

In caso di fallimento di VM-LINUX-01 (il gateway di accesso):

1. Tailscale smette di funzionare.
2. Cloudflare Tunnel cade.
3. Piano B (Emergenza): Devi essere fisicamente presente o avere AnyDesk installato sull'Host Windows (192.168.1.10) come backup estremo "dormiente" (servizio stoppato, da avviare solo in locale o via WoL se supportato). Tuttavia, la vera ridondanza è l'accesso fisico.