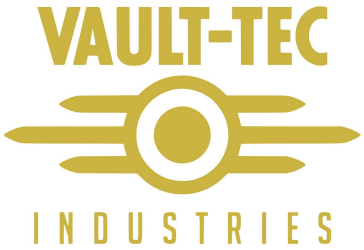


Systems Division – Internal Memorandum Vault 612

Classificazione: RISERVATO – USO INTERNO VAULT-TEC
Ref: VT-SD/AD/612-01
Subject: Identity & Access Control Deployment – vault612.local
Platform: Windows Server 2022 – AD DS / DNS
Date: 13/02/2026
Prepared by: Leonardo Chiaverini

Executive Note

In accordo ai protocolli Vault-Tec per la continuità operativa e la disciplina interna, è stata implementata un'infrastruttura di **Identity & Access Control** basata su **Active Directory** per il **Vault 612**, nell'ambito di un **primo test di laboratorio** finalizzato a validare l'impianto iniziale.
Lo scopo è garantire che **ogni abitante** operi esclusivamente entro il proprio perimetro autorizzato, con accesso alle risorse del Vault definito da **ruolo e reparto**, riducendo al minimo la propagazione di privilegi e la contaminazione tra aree critiche.

1. Mission Objective

Istituire il dominio **vault612.local** come autorità centrale per:

- organizzazione del personale tramite **Organizational Unit (OU)**;
- creazione e gestione delle utenze;
- definizione di **gruppi di reparto** (Global Security Groups);
- compartimentazione delle risorse tramite permessi **SMB Share + NTFS**;
- implementazione di un modello Security "SOC-like" con visibilità cross-reparto controllata.

2. Operational Environment

È stato predisposto un server Windows Server 2022 con i seguenti componenti:

- Active Directory Domain Services (AD DS)
- Domain Name System (DNS)

Dominio operativo: v*ault612.local*

Questa configurazione introduce un punto di controllo unico, indispensabile per:

- tracciabilità degli accessi e accountability;
- standardizzazione delle identità;
- applicazione futura di policy di sicurezza (GPO).

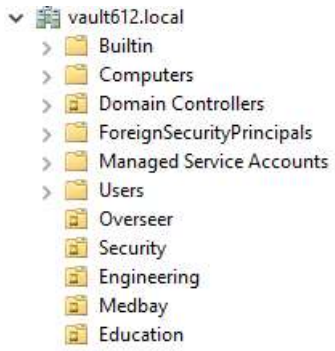


Figura 01 – Dominio "Vault612.local" operativo su Windows Server 2022 con ruoli AD DS/DNS.

3. Vault Directory Blueprint (OU Design)

Per garantire ordine strutturale e scalabilità amministrativa, le entità del Vault sono state modellate tramite OU dipartimentali.

Struttura OU implementata

- *OU Overseer*
- *OU Security*
- *OU Engineering*

- *OU Medbay*
- *OU Education*

Figura 02 – Struttura OU dipartimentale implementata in ADUC (Overseer, Security, Engineering, Medbay, Education).

4. Dweller Enrollment (Utenze)

Sono state create utenze in conformità ad una nomenclatura chiara e “operabile” in contesto Vault.
Le utenze sono state allocate nelle OU di reparto per riflettere la catena di comando e la separazione delle funzioni.

Reparto OU	Utenze	Funzione operativa
OVERSEER_OFFICE	sovrintendente@vault612.local	Direzione / Coordinamento
SECURITY	sec.chief@vault612.local sec.guard1@vault612.local	Controllo accessi / presidio
ENGINEERING	eng.chief@vault612.local eng.tech1@vault612.local	Manutenzione / infrastruttura
MEDBAY	med.doc@vault612.local med.nurse1@vault612.local	Assistenza Medica
EDUCATION	edu.teacher1@vault612.local edu.teacher2@vault612.local	Formazione / Istruzione Vault

Nota operativa: la collocazione per reparto consente l'applicazione di regole e policy mirate, senza impattare l'intero Vault.

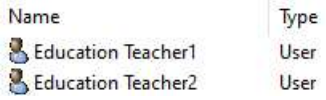


Figura 03 – Utenze Education create e collocate nella OU dedicata (edu.teacher1, edu.teacher2).

5. Teams & Clearance Model (Gruppi e ruoli)

Per assegnare accessi in modo controllato è stata adottata la logica Vault-Tec "role-based", evitando assegnazioni dirette ai singoli individui.

Gruppi di reparto (Global Security Groups)

- *GG_V612_Overseer*
- *GG_V612_Security*
- *GG_V612_Engineering*
- *GG_V612_Medbay*
- *GG_V612_Education*

Figura 04 – Elenco gruppi Global Security (GG_V612_*) utilizzati come "security principals" per l'assegnazione dei permessi.

Membership

Ciascuna utenza è membro del proprio gruppo di reparto; autorizzazioni aggiuntive sono gestite tramite ACL in base alle esigenze operative.

6. Resource Compartmentalization (Cartelle, shares e permessi)

Per prevenire circolazione non autorizzata di informazioni e materiali, le risorse del Vault sono state compartimentate per reparto.

6.1 Directory radice risorse

Per migliorare governance e manutenzione, le directory operative sono state consolidate sotto una root dedicata:

- *C:\Vault612_Shares*

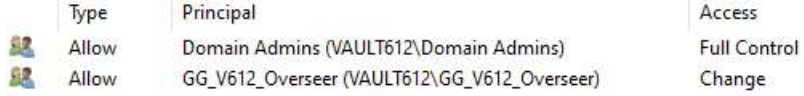
6.2 Compartimenti (sottocartelle)

- *C:\Vault612_Shares\10_Public-Notice*
- *C:\Vault612_Shares\20_OverseerOffice*
- *C:\Vault612_Shares\30_Security*
- *C:\Vault612_Shares\40_Engineering*
- *C:\Vault612_Shares\50_Medbay*
- *C:\Vault612_Shares\60_Education*

7. Share Permissions (SMB)

Per ogni cartella condivisa è stata adottata la seguente logica standard:

- Domain Admins: **Full Control** (governance e gestione)
- Gruppo reparto: **Change** + **Read** (operatività senza privilegi eccessivi)
- Dove previsto: accessi aggiuntivi in **sola lettura** per funzioni di controllo (Security/SOC)



Type	Principal	Access
Allow	Domain Admins (VAULT612\Domain Admins)	Full Control
Allow	GG_V612_Overseer (VAULT612\GG_V612_Overseer)	Change

Figura 05 – Share Permissions su 20_OverseerOffice: accesso operativo limitato al reparto OverseerOffice, governance Domain Admins.

Type	Principal	Access
Allow	GG_V612_Education (VAULT612\GG_V612_Education)	Read
Allow	GG_V612_Overseer (VAULT612\GG_V612_Overseer)	Change
Allow	GG_V612_Security (VAULT612\GG_V612_Security)	Read
Allow	GG_V612_Engineering (VAULT612\GG_V612_Engineering)	Read
Allow	GG_V612_Medbay (VAULT612\GG_V612_Medbay)	Read
Allow	Domain Admins (VAULT612\Domain Admins)	Full Control

Figura 06 – Share Permissions su 10_Public-Notice: pubblicazione riservata a OverseerOffice e consultazione in lettura per i reparti autorizzati.

8. NTFS Permissions (Security)

È stata implementata compartimentazione tramite permessi espliciti sulle cartelle di reparto (inheritance disabilitata a livello compartimento), mantenendo:

- **SYSTEM**: Full Control
- **Administrators / Domain Admins**: Full Control
- Gruppo reparto: Modify / Read in base al ruolo
- Accessi cross-reparto definiti esplicitamente e documentati (SOC model / Public Notice).

Type	Principal	Access
Allow	SYSTEM	Full control
Allow	Administrators (VAULT612\Administrators)	Full control
Allow	CREATOR OWNER	Full control
Allow	GG_V612_Engineering (VAULT612\GG_V612_Engineering)	Modify
Allow	GG_V612_Security (VAULT612\GG_V612_Security)	Read & execute

Figura 07 – NTFS su 40_Engineering: GG_V612_Engineering con Modify e GG_V612_Security in sola lettura (audit SOC).

9. Security “SOC Model” (Cross-Access Controlled)

Per simulare una funzione Security assimilabile ad un **SOC**:

- **Security** può accedere **in sola lettura** ai compartimenti di **Engineering, Medbay e Education** (audit/monitoring).
- **Security** è esclusa dal compartimento **OverseerOffice**.

9.1 Access Matrix (Target Model)

Risorsa	Gruppo reparto	GG_V612_Security
20_OverseerOffice	GG_V612_Overseer = Modify	Deny (Read & execute)
30_Security	GG_V612_Security = Modify	—
40_Engineering	GG_V612_Engineering = Modify	Read & execute
50_Medbay	GG_V612_Medbay = Modify	Read & execute
60_Education	GG_V612_Education = Modify	Read & execute

Nota operativa: il Deny su OverseerOffice mantiene separazione gerarchica e riduce rischi di accesso non autorizzato ad attività direzionali.

10. Public Notice (Bacheca Operativa)

La cartella Public-Notice è stata configurata come canale informativo interno ufficiale da parte della Sovrintendenza:

- OverseerOffice: pubblicazione/gestione comunicazioni (Modify)
- altri reparti: consultazione (Read)

Risorsa	10_Public-Notice
GG_V612_Overseer	Modify
GG_V612_Security	Read
GG_V612_Engineering	Read

GG_V612_Medbay	Read
GG_V612_Education	Read

11. Verification & Evidence (Client-side)

Sono stati eseguiti test funzionali da client per validare il modello di autorizzazione:

- sec.guard1: accesso operativo completo alla share Security; accesso in sola lettura a Engineering/Medbay/Education; accesso negato a OverseerOffice.
- Utenze di reparto (es. eng.tech1, med.nurse1, edu.teacher1) con accesso in scrittura esclusivamente al proprio compartimento e lettura su Public-Notice.

Le evidenze sono documentabili tramite screenshot (creazione file in compartimento autorizzato e messaggi “Access Denied” in compartimenti non autorizzati).

Figura 08 – Test da client (sec.guard1): Access Denied su 20_OverseerOffice.

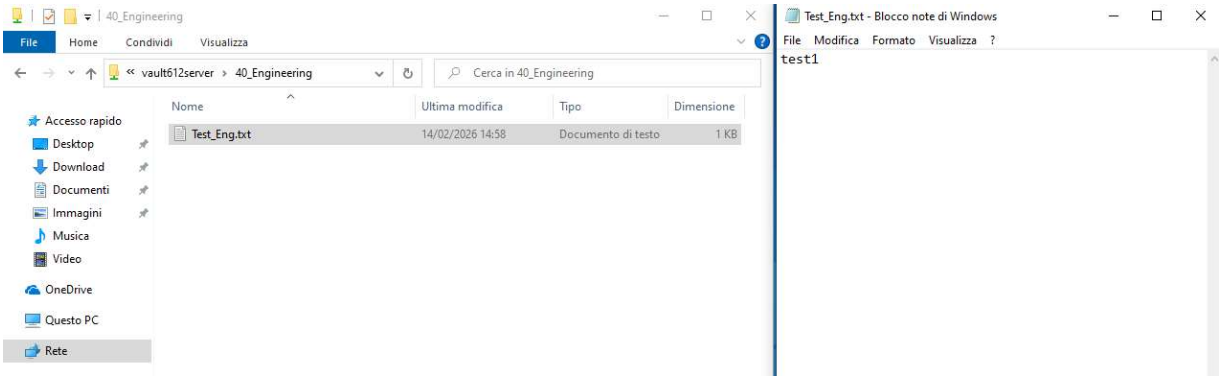


Figura 11 – Test da client (sec.guard1): accesso in sola lettura su 40_Engineering per finalità di audit.

13. Conclusion & Next Steps

L'implementazione descritta costituisce un **test di laboratorio iniziale** finalizzato a validare i meccanismi base di **Identity & Access Control** del dominio ***vault612.local*** (OU, utenze, gruppi, condivisioni e ACL), nonché il modello di segregazione e controllo incrociato per il reparto Security in modalità "SOC-like".

In vista della costruzione operativa del Vault, questa prima baseline verrà evoluta verso un'architettura **più granulare e scalabile**, includendo in particolare: maggiore segmentazione per ruoli e funzioni (gruppi aggiuntivi e policy dedicate), standardizzazione completa della struttura (separazione di oggetti e gruppi in contenitori dedicati), introduzione di **GPO** per hardening e governance, e definizione di un modello di accesso per processi (audit, incident response, formazione) con evidenze e controlli periodici.

L'obiettivo dei prossimi step è passare da un impianto validato in laboratorio a una configurazione **Vault-ready**, con controllo più fine dei privilegi, tracciabilità e riduzione sistematica della superficie di rischio.