Mode Opératoire

Investigation et résolution des items Vaultwarden bloqués ou divergents

Code :	MO-SEC-003
Version :	1.0
Date :	15 avril 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	15/04/2026	Création initiale — formalisation du traitement appliqué aux 4 items Colombo66 résiduels du Sprint 2 (Ferme HyperV, OPNsense 2, SuluCisco Wifi, Zabbix root)

1 Objet

Ce mode opératoire décrit la procédure d'investigation et de résolution des items du gestionnaire de mots de passe **Vaultwarden** qui ne peuvent pas être rotatés lors d'une opération de rotation périodique (cf. MO-AD-008) ou d'une rotation `krbtgt` (cf. MO-AD-002). Deux situations sont distinguées :

— **Cas A — BLOQUÉ** : l'hôte cible est injoignable (machine éteinte, segment réseau non routé, panne matérielle).

— **Cas B — DIVERGENCE** : l'hôte répond mais le mot de passe stocké en *vault* est refusé (`PermitRootLogin no`, mot de passe changé hors-trace, compte verrouillé).

L'enjeu n'est pas anodin : sans procédure formalisée, ces résidus s'accumulent silencieusement et l'on aboutit à une situation « rotaté en *vault* mais inopérant en réel », qui est strictement pire que pas de rotation du tout.

⚠ Contexte initial

À l'issue du Sprint 2 (rotation des mots de passe critiques, 14–15 avril 2026), **quatre items Colombo66 résiduels** ont été identifiés : Ferme HyperV (`10.0.112.4`, injoignable), OPNsense 2 (`10.0.112.101`, injoignable), SuluCisco-Wifi (`10.0.112.6`, injoignable) et Zabbix root (`10.0.112.190`, divergence SSH). Cette procédure est issue du traitement appliqué à ces quatre items.

2 Champ d'application

Public concerné	Administrateurs de l'infrastructure BTS SIO
Vault	Vaultwarden auto-hébergé `https://10.0.112.10` (CT 127 ProxMox)
Outils	`bw` CLI (Bitwarden CLI), `ping`/`nc`/`ssh`, navigateur web, `jq`
Authentification	Vault Vaultwarden déverrouillé (`admin@bts.sio`) ; accès LAN/console pour les pivots
Durée	15–30 min par item, ∼2 h pour un lot complet de quatre items
Présentiel requis	Dépend du cas : Cas A (souvent oui), Cas B (souvent non)

Ce MO est **complémentaire**, et non substitutif, des MO-AD-002 et MO-AD-008. Il couvre exclusivement la phase « résidu post-rotation ».

3 Prérequis

Prérequis

— Une rotation MO-AD-008 ou MO-AD-002 a été exécutée et a remonté au moins un item résiduel
— Vault Vaultwarden déverrouillé : `export BW_SESSION=$(bw unlock -raw)` (cf. MO-PLT-009)
— VPN WireGuard `wg-bts` actif (`bts vpn status`)
— Accès console physique disponible si pivot nécessaire (Cas A irrémédiable à distance)
— Compte Domain Admin si l'item concerne un objet AD (Cas B avec reset nécessitant DSRM)

Certificat self-signed

Vaultwarden héberge un certificat auto-signé. Préfixer toute commande `bw` par `NODE_TLS_REJECT_UNAUTHORIZED=0` ou exporter cette variable une fois pour la session. Pas de fallback gracieux dans `bw` en cas d'erreur TLS.

4 Diagnostic initial — triage commun

Étape 1 — Récupérer la liste des items résiduels

Après une rotation, identifier les items qui contiennent encore l'ancien mot de passe (ex. recherche `Colombo66`) :

```
export NODE_TLS_REJECT_UNAUTHORIZED=0
export BW_SESSION=$(bw unlock --raw)

bw list items 2>/dev/null \
  | jq -r '.[] |
   select(.login.password|ascii_downcase|startswith("colombo")) |
   "\(.id) | \(.name) | \(.login.username // "-")"'
```

La sortie liste les items à traiter avec leur identifiant Vaultwarden, leur nom et le compte concerné.

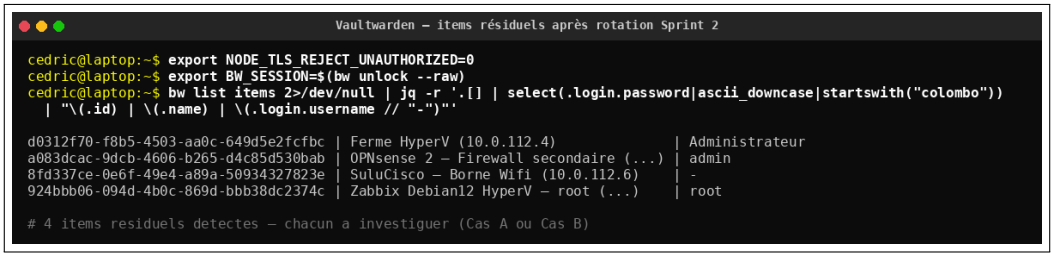

Figure 1 – Liste des items Vaultwarden résiduels après rotation Sprint 2

Étape 2 — Triage en quatre passes ordonnées

Pour chaque item identifié, exécuter les quatre tests dans cet ordre. Le premier qui échoue déclenche le cas correspondant :

```
HOST=10.0.112.4

ping -c 3 -W 2 $HOST            # 1. Joignabilité réseau
nc -vz $HOST 22                 # 2. Port SSH ouvert ?
nc -vz $HOST 443                # 3. Port HTTPS ouvert ?
ssh -o BatchMode=yes \
    -o ConnectTimeout=5 \
    -o StrictHostKeyChecking=no \
    root@$HOST exit             # 4. Auth réelle
```

Arbre de décision :

— Test 1 échoue → **Cas A — BLOQUÉ** (§ 5)

— Tests 1–3 OK, test 4 répond `Permission denied (password)` → **Cas B — DIVERGENCE** (§ 6)

— Tests 1–3 OK, test 4 répond `Permission denied (publickey)` sans `password` → SSH par clé uniquement, voir § 6 (sshd_config)

Tracer le diagnostic

Garder un horodatage et la sortie brute des tests : cela alimentera les notes Vaultwarden (§ 7) et permettra de comparer dans le temps si le même item revient régulièrement.

5 Cas A — Hôte injoignable

Étape 3 — Confirmer l'injoignabilité

Vérifier l'injoignabilité depuis plusieurs points pour exclure un problème local de routage VPN :

```
# Depuis le poste admin (via VPN)
ping -c 3 10.0.112.4

# Depuis OPNsense (autre point de vue)
ssh root@10.0.112.1 "ping -c 3 10.0.112.4"

# Verifier la couverture VPN
wg show wg-bts allowed-ips
```

Si tous les points retournent un échec, l'hôte est confirmé hors réseau.

Étape 4 — Identifier la cause probable

Symptôme	Hypothèse la plus probable
`ping` timeout depuis tous les vantage points	Machine éteinte ou débranchée
`ping` OK depuis OPNsense, KO depuis VPN	Plage non couverte par `allowed-ips` sur `wg-bts`
`ping` KO partout sauf SuluCisco voisin	Interface réseau de l'hôte tombée
Plage entière injoignable (`10.0.X.0/24`)	VLAN entier coupé ou switch éteint

Étape 5 — Pivot d'escalade

Dans l'ordre, jusqu'à obtenir un accès :

1. Demander aux collègues si l'équipement est censé être actif
2. Vérifier sur site (présentiel) l'état physique : led, câble, alimentation
3. Accès console hors-bande : IPMI/iDRAC/iLO si la machine en dispose
4. Déclarer l'item BLOQUÉ et reporter au prochain présentiel

Étape 6 — Marquer l'item dans Vaultwarden

Tant que la rotation n'a pas pu se faire, l'item doit être annoté pour éviter qu'il soit oublié :

```
ITEM_ID=$(bw list items --search "Ferme HyperV" 2>/dev/null \
            | jq -r '.[0].id')

bw get item $ITEM_ID \
  | jq '.notes = "[BLOQUE 2026-04-15] Host 10.0.112.4 injoignable depuis
   VPN wg-bts. Rotation reportee. Action : ping check au prochain
   presentiel."' \
  | bw encode \
  | bw edit item $ITEM_ID

bw sync
```

Le préfixe `[BLOQUE YYYY-MM-DD]` est volontairement sans accent pour faciliter le `grep` ultérieur sur le *vault*.

6 Cas B — Divergence vault / réel

Étape 7 — Confirmer la divergence

L'auth réelle (SSH, web, WinRM) refuse le mot de passe du *vault* alors que le port répond. Avant d'investiguer côté serveur, exclure une coquille de saisie en testant depuis deux clients différents (`ssh` ligne de commande **et** navigateur ou client GUI).

Étape 8 — Diagnostiquer côté serveur

Pour SSH (Linux) : pivoter via un compte non-root encore valide, vérifier la configuration `sshd` :

```
ssh admin@10.0.112.190
sudo grep -E '^(PermitRootLogin|PasswordAuthentication)'
    /etc/ssh/sshd_config
sudo last -n 5 root          # date de la derniere connexion root reussie
```

Pour AD (Windows) : vérifier le statut du compte :

```
Get-ADUser -Identity <user> -Properties LockedOut, AccountExpired,
    PasswordExpired, PasswordLastSet
```

Pour une appliance web (OPNsense, NAS QNAP) : tester via l'UI web et regarder les journaux d'audit `System→Log Files` ou équivalent.

Étape 9 — Tester via canal alternatif

L'objectif est de prouver que le compte **fonctionne réellement avec un autre mot de passe** (cas du MDP changé hors-trace) ou qu'il est réellement cassé (cas où aucune méthode ne passe). Canaux : web UI, console physique (ESXi/HyperV), Recovery Mode, WinRM si compte AD, console série pour les firewalls.
Pour Zabbix sur HyperV (constaté le 15/04/2026) : la divergence vault/SSH est réellement résolue par la **console HyperV**, qui demande l'accès à la Ferme HyperV (`10.0.112.4`). Si cette dernière est elle-même injoignable (Cas A), l'item passe en *Cas B bloqué par Cas A* à signaler explicitement.

Étape 10 — Reset si possible et autorisé

Plate-forme	Méthode de reset
Linux (général)	Console single-user (`init=/bin/bash`), `passwd`, reboot
Active Directory	Mode DSRM (*Directory Services Restore Mode*) ou `Set-ADAccountPassword` via un autre DA
NAS QNAP	Bouton reset physique (3 s = reset administrateur)
OPNsense	Boot menu, option 3 (« Reset root password »)
Cisco IOS	Mode *rommon*, contournement par changement de `config-register`

Étape 11 — Marquer l'item

Convention symétrique au Cas A :

```
ITEM_ID=$(bw list items --search "Zabbix" 2>/dev/null | jq -r '.[0].id')

bw get item $ITEM_ID \
  | jq '.notes = "[DIVERGENCE 2026-04-15] Vault dit Colombo66 mais SSH
   refuse (Permission denied). Hypotheses : (a) PermitRootLogin no, (b)
   MDP change hors-trace 2025-Q4. Procedure : reset console HyperV
   (depend de la Ferme HyperV 10.0.112.4 elle-meme injoignable)."' \
  | bw encode \
  | bw edit item $ITEM_ID

bw sync
```

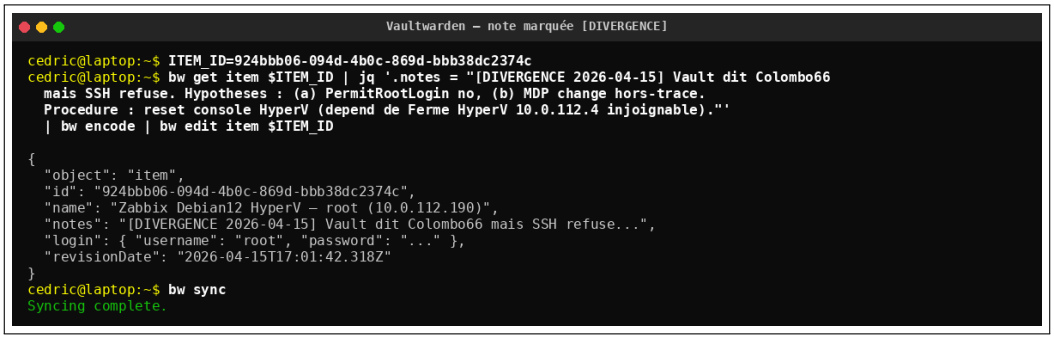

Figure 2 – Note Vaultwarden mise à jour avec le préfixe `[DIVERGENCE]` et la procédure programmée

⚠ Risque d'auto-lockout

La plupart des appliances appliquent un verrouillage après 3–5 échecs d'authentification. Limiter les tests à **deux tentatives par canal** et attendre le délai de déverrouillage avant de retenter, sous peine de se retrouver bloqué même lorsque le bon mot de passe sera retrouvé.

7 Convention Vaultwarden — format des notes

Préfixe	Cas	Modèle
`[BLOQUE YYYY-MM-DD]`	A	Host injoignable depuis <contexte>. Rotation reportée. Action : <prochaine étape>.
`[DIVERGENCE YYYY-MM-DD]`	B	Vault dit X mais auth refuse. Hypothèses : (a)…, (b)…. Procédure : <canal>.
`[RESOLU YYYY-MM-DD]`	post-traitement	Re-rotation OK. Préfixe antérieur purgé ; à effacer complètement à la rotation suivante.

Pourquoi cette convention ?

— **grep facile** sur le *vault* : `bw list items | jq '.[] | select(.notes | test("BLOQUE|DIVERGEN`

— **Audit semestriel automatisable** : extraire la liste des items toujours marqués BLOQUÉ depuis plus de 60 jours

— **Traçabilité incident** : la note se substitue à un ticket simple pour les anomalies basse-priorité

— **Datation systematique** : sans date, la note se périme silencieusement et perd toute valeur

Préfixes sans accent

Les préfixes `[BLOQUE]`, `[DIVERGENCE]` et `[RESOLU]` sont écrits sans accent pour éviter les problèmes d'encodage lors des `grep` cross-platform et lors des recherches dans l'UI Vaultwarden.

8 Reprise après déblocage

Étape 12 — Détection

L'item redevient joignable (présentiel, fix réseau, retour de la machine). Confirmer avec un `ping` + un test d'auth réel, puis vérifier que la note `[BLOQUE]` ou `[DIVERGENCE]` est bien encore présente sur l'item :

```
bw get item $ITEM_ID | jq -r '.notes'
```

Étape 13 — Re-rotation

Ré-exécuter la portion concernée du MO d'origine :

— Item `krbtgt` → MO-AD-002 (double rotation)

— Compte AD ou compte système classique → MO-AD-008 § 5.x correspondant

Une re-rotation immédiate ne demande pas d'attendre la prochaine échéance : le but est de combler la fenêtre où l'ancien mot de passe a continué à être valide.

Étape 14 — Nettoyage de note

Remplacer le préfixe par `[RESOLU YYYY-MM-DD]` avec un résumé court :

```
bw get item $ITEM_ID \
  | jq '.notes = "[RESOLU 2026-04-22] Re-rotation OK lors du presentiel
   S16."' \
  | bw encode \
  | bw edit item $ITEM_ID
bw sync
```

Le préfixe `[RESOLU]` sera lui-même purgé à la rotation programmée suivante (semestrielle), une fois confirmé qu'aucune régression n'est apparue.

Vérification

Avant de fermer le traitement d'un item :

- ☐ Note datée du jour avec préfixe `[RESOLU]`
- ☐ Mot de passe re-rotaté (24–32 caractères aléatoires)
- ☐ Test d'authentification réussi sur le canal réel (SSH, web, WinRM)
- ☐ `bw sync` exécuté (la modification est poussée côté serveur)
- ☐ L'item ne remonte plus dans la commande `grep` de l'§ 4

9 Dépannage

Symptôme	Solution
`bw edit` retourne 400 *Bad Request*	JSON malformé : vérifier l'échappement des guillemets dans la note (utiliser `jq` pour la construction plutôt qu'une concaténation *string* en bash).
Note tronquée après `bw edit`	Limite serveur Vaultwarden ∼10 000 caractères. Raccourcir la note ou la préfixer d'un identifiant d'incident externe (Vikunja, ticket).
VPN remonte mais hôte toujours injoignable	Vérifier la route 10.0.112.0/24 dans `wg show wg-bts allowed-ips` ; certaines plages internes ne sont pas couvertes par défaut (cas OPNsense 2 sur `10.0.112.101`).
SSH refuse même avec MDP correct	Tester avec `ssh -v` pour distinguer `Permission denied (publickey)` de `(password)`. Si `(publickey)` seul, `PasswordAuthentication no` dans `sshd_config`.
NAS QNAP dont le bouton reset physique est inaccessible	Reporter au prochain présentiel ; en attendant, marquer `[BLOQUE]` avec une date butoir et bloquer toute tâche planifiée qui dépend du compte concerné.
`NODE_TLS_REJECT_UNAUTHORIZED=0` oublié	`bw` refuse avec `self-signed certificate`. Toujours exporter la variable en début de session ou préfixer chaque commande.

10 Voir aussi

— **MO-AD-002** — Rotation du compte krbtgt (cas particulier d'item dont la rotation peut générer un résidu si DC2 indisponible)
— **MO-AD-006** — Backup System State (rollback en cas de cassure complète d'un compte AD)
— **MO-AD-007** — Audit périodique AD (le check `krbtgt` permet de détecter les rotations manquantes)
— **MO-AD-008** — Rotation périodique des mots de passe critiques (procédure mère ; ce MO en couvre les résidus)
— **MO-PLT-009** — Connexion à Vaultwarden (prérequis pour `bw unlock`)