Problèmes rencontrés + troubleshooting

Problèmes Rencontrés et Solutions

1. Permissions SELinux avec bind mounts

Problème :

```
Error: lsetxattr(label=system_u:object_r:container_file_t:s0) /var/lib/vault: operation not permitted
```

Cause : En Podman rootless, impossible de relabeler des dossiers dans `/var/lib/` (appartiennent à root).

Solutions :

Option A - Volumes nommés (recommandé) :

```
podman volume create vault_data
podman run -v vault_data:/vault/file ...
# SELinux géré automatiquement
```

Option B - Bind mount avec relabeling manuel :

```
sudo chown -R $(id -u):$(id -g) /var/lib/vault
sudo chcon -R -t container_file_t /var/lib/vault
sudo semanage fcontext -a -t container_file_t "/var/lib/vault(/.*)?"
podman run -v /var/lib/vault:/vault/file ...  # Sans :Z
```

---

2. User namespace et UID mapping

Problème : Fichiers créés avec des UIDs étranges (524287, 525287).

Cause : Podman rootless mappe les UIDs du conteneur vers un range d'UIDs sur l'hôte.

Explication :

```
# Vérifier le mapping
cat /etc/subuid | grep username
# username:524288:65536

# UID conteneur 999 → UID hôte 524288 + 999 = 525287
```

Solution : Normal et voulu pour l'isolation.

---

4. Vault nécessite `cluster_addr` avec Raft

Problème :

```
Error: Cluster address must be set when using raft storage
```

Solution : Configuration Raft complète obligatoire :

```
storage "raft" {
  path    = "/vault/file"
  node_id = "vault-1"
}

api_addr = "http://127.0.0.1:8200"
cluster_addr = "https://127.0.0.1:8201"  # Port 8201 pour le cluster
```

Note :

- Port 8200 = API/UI
- Port 8201 = Communication inter-nœuds (même en single-node)

---

5. HTTPS vs HTTP - Erreur de connexion

Problème :

```
Error: http: server gave HTTP response to HTTPS client
```

Cause : `VAULT_ADDR` par défaut en HTTPS mais Vault configuré en HTTP (`tls_disable = true`).

Solution :

```
# Le temps de set up
export VAULT_ADDR='http://127.0.0.1:8200'
```

---

6. Permission denied - Authentification manquante

Problème :

```
Error reading auth/approle/role/admin/role-id: permission denied
```

Cause : Tentative de lecture sans être authentifié.

Solution :

```
# Se connecter d'abord
vault login <ROOT_TOKEN>

# Puis exécuter la commande
vault read auth/approle/role/admin/role-id
```

---

7. Confusion entre auth method path et role path

Problème : Création d'une auth method sur `auth/admin/` au lieu d'utiliser `auth/approle/`.

Solution :

```
# □ Incorrect - Création d'une nouvelle auth method
vault auth enable -path=admin approle

# □ Correct - Utiliser l'auth method standard
vault auth enable approle
vault write auth/approle/role/admin ...
```

Path correct : `auth/approle/role/<role_name>`

---

8. UI Web - Scroll bloqué

Problème : Impossible de scroller dans l'interface web Vault.

Solutions :

```
// DevTools Console (F12)
document.body.style.overflow = 'auto';
```

Ou :

- Utiliser le CLI (plus efficace de toute façon) Vault WebUI sert à rien en vrai ... il faudrait que vault améliore sa WebUI c'est vraiment naze.

---

9. AppRole non visible dans l'UI de login

Problème : Seule l'option "Token" apparaît dans l'UI de connexion.

Solution : Activer la visibilité de l'auth method :

```
vault write sys/auth/approle/tune listing_visibility="unauth"
```

Alternative : Utiliser le token généré par AppRole via CLI :

```
TOKEN=$(vault write -field=token auth/approle/login role_id="..." secret_id="...")
# Login UI avec ce token
```

---

10. Certificats Let's Encrypt et SELinux

Problème :

```
cannot load certificate: Permission denied
```

Cause : Après renouvellement Certbot, les nouveaux fichiers ont le mauvais contexte SELinux.

Solution :

```
# Quick fix
sudo restorecon -Rv /etc/letsencrypt
```

```
# Permanent fix
sudo semanage fcontext -a -t httpd_sys_content_t "/etc/letsencrypt(/.*)?"
sudo restorecon -Rv /etc/letsencrypt

# Tester Nginx
sudo nginx -t
```

Commandes de Maintenance

Unseal après redémarrage

```
export VAULT_ADDR='http://127.0.0.1:8200'
vault operator unseal <UNSEAL_KEY>
```

Vérifier le statut

```
vault status
podman logs vault
podman ps -a
```

Backup des données Vault

```
# Backup du volume
podman volume export vault_data > vault_data_backup.tar

# Ou copie directe
cp -r ~/.local/share/containers/storage/volumes/vault_data/_data /backup/vault/
```

Rotation du SecretID AppRole

```
# Générer un nouveau SecretID
vault write -f -field=secret_id auth/approle/role/admin/secret-id
```

Gestion des logs

```
# Voir les logs
podman logs vault

# Suivre les logs en temps réel
podman logs -f vault

# Dernières 100 lignes
podman logs --tail 100 vault
```

Concepts Clés

Raft Storage

- **Backend de stockage HA intégré**
- Algorithme de consensus distribué
- Permet plusieurs nœuds Vault synchronisés
- Pas besoin de base externe (Consul, MySQL, etc.)
- Recommandé par HashiCorp

AppRole Authentication

- **Méthode d'auth pour machines/applications**
- RoleID : identifiant permanent du rôle
- SecretID : credential temporaire/éphémère
- Idéal pour automation, CI/CD, scripts
- Plus secure que userpass pour l'automation

Unseal/Seal

- **Vault démarre "sealed" (verrouillé)**
- Données chiffrées, inaccessibles
- Unseal = déverrouiller avec la clé
- Nécessaire après chaque redémarrage
- Protège contre le vol de disque

Podman Rootless

- Conteneurs sans privilèges root
- User namespaces pour isolation
- Meilleure sécurité que Docker classique

- Compatible avec SELinux

Revision #3
Created 2025-11-28 01:13:44 UTC by Admin
Updated 2025-11-29 00:54:18 UTC by Admin