

# 📖 Guide — Mettre à jour les IP de SAP quand l'accès ne fonctionne plus

À qui s'adresse ce guide ? À toute personne de l'équipe infra qui doit rétablir l'accès à SAP Private lorsqu'il cesse de fonctionner. Aucune connaissance préalable du montage n'est nécessaire : suivre les étapes dans l'ordre.

## 1. Pourquoi ce problème arrive

L'accès à SAP Private passe par le serveur Scaleway ( `151.115.148.243` ), dont l'IP est autorisée (« whitelisted ») côté SAP. Pour que ça marche, le serveur doit savoir vers quelles **adresses IP** envoyer le trafic SAP.

Or le SAP de Seize est hébergé derrière un **load balancer Amazon (AWS)**. Ce load balancer **change ses adresses IP de temps en temps, sans prévenir**. Le jour où AWS change ces IP, le serveur continue d'envoyer le trafic vers les **anciennes IP**, qui ne répondent plus → **l'accès SAP tombe en panne**.

La solution : retrouver les **nouvelles** IP et les enregistrer dans le système. C'est ce que décrit ce guide. L'opération prend ~5 minutes.

**Informations de référence** : - Nom d'hôte SAP : `sandbox-z38bb8twno7.rise.cloud.sap` - Serveur Scaleway : `151.115.148.243` (connexion SSH avec son compte : `ssh sonnom@151.115.148.243`) - Le VPN/routage est géré par **Headscale** (conteneur Docker `headscale`) et un client **Tailscale** installé sur le serveur lui-même.

## 2. Confirmer que c'est bien CE problème

Avant de modifier quoi que ce soit, vérifier que la panne vient bien des IP SAP.

**a) Se connecter au serveur en SSH, puis tester si le serveur joint SAP :**

```
curl -I -m 10 "https://sandbox-z38bb8twno7.rise.cloud.sap:44301/sap/bc/ui5_ui5/ui2/ushell/shells/abap/FioriLaunchpad.html?sa
```

- ✓ Si ça répond `HTTP/2 200` → le serveur joint SAP, le problème est **ailleurs** (ce guide ne s'applique pas ; vérifier plutôt Traefik ou le DNS `sap-fiori`).
- ✗ Si ça affiche `Connection timed out` (au bout de 10 s) → **c'est probablement ce problème d'IP**. Continuer.

**b) Voir quelles IP sont actuellement enregistrées dans le système :**

```
docker exec headscale headscale routes list
```

Noter les IP affichées dans la colonne `Prefix` (ex. `13.49.123.44/32`, `13.51.212.60/32`) et leur `ID`. Ce sont les IP **actuellement** utilisées — on va les comparer aux vraies.

## 3. Trouver les nouvelles IP de SAP

Sur le serveur, demander au DNS les IP actuelles du nom d'hôte SAP :

```
dig +short sandbox-z38bb8twno7.rise.cloud.sap
```

Résultat typique :

```
1b-329119128-caltdc-262348694.eu-north-1.elb.amazonaws.com.  
13.49.200.11  
13.51.45.230
```

- Ignorer la ligne qui finit par `.amazonaws.com.` (c'est un nom, pas une IP).
  - Les vraies IP sont les lignes qui ressemblent à des chiffres** (ex. `13.49.200.11`, `13.51.45.230`). Il peut y en avoir 1, 2 ou plus.
- ☞ **Comparer avec les IP de l'étape 2b**. Si elles sont **différentes**, c'est confirmé : les IP ont changé. Noter les **nouvelles** IP, on va les enregistrer.

! Si `dig` n'est pas trouvé, utiliser : `getent hosts sandbox-z38bb8twno7.rise.cloud.sap`

## 4. Enregistrer les nouvelles IP

Deux sous-étapes : (A) annoncer les nouvelles routes sur le serveur, (B) les autoriser dans Headscale.

### A. Annoncer les nouvelles routes (sur le serveur)

Remplacer les IP ci-dessous par les **nouvelles** IP trouvées à l'étape 3. Mettre chaque IP suivie de `/32`, séparées par une virgule **sans espace** :

```
sudo tailscale set --advertise-routes=13.49.200.11/32,13.51.45.230/32
```

(Exemple avec 2 IP. S'il y en a 3, en mettre 3 : `IP1/32,IP2/32,IP3/32`.)

Cette commande **remplace** les anciennes routes par les nouvelles. Aucune confirmation n'est affichée si elle réussit — c'est normal.

### B. Autoriser les nouvelles routes dans Headscale (sur le serveur)

Lister à nouveau les routes pour voir les nouvelles apparaître :

```
docker exec headscale headscale routes list
```

Les **nouvelles** IP apparaissent maintenant dans la liste, avec un nouvel `ID` chacune, et la colonne `Enabled` à `false` (pas encore autorisées).

Les autoriser **une par une**, en remplaçant `<ID>` par le numéro de chaque nouvelle route :

```
docker exec headscale headscale routes enable -r <ID>
```

Exemple, si les nouvelles routes ont les ID 3 et 4 :

```
docker exec headscale headscale routes enable -r 3
docker exec headscale headscale routes enable -r 4
```

Les anciennes routes (qui ne sont plus annoncées) peuvent rester dans la liste sans gêner. Si on veut faire le ménage, on peut les supprimer :

```
docker exec headscale headscale routes delete -r <ancien_ID>
```

## 5. Vérifier que l'accès est rétabli

a) **Depuis le serveur**, refaire le test de l'étape 2a :

```
curl -I -m 10 "https://sandbox-z38bb8twno7.rise.cloud.sap:44301/sap/bc/ui5_ui5/ui2/ushell/shells/abap/FioriLaunchpad.html?sa
```

- ✓ `HTTP/2 200` → le serveur rejoint SAP. C'est réparé côté serveur.

b) **Depuis un navigateur** (n'importe quel poste), ouvrir :

```
https://sap-fiori.seizeconsulting.com/sap/bc/ui5_ui5/ui2/ushell/shells/abap/FioriLaunchpad.html?sap-client=100&sap-language=
```

La page de login SAP doit s'afficher → ✓ tout fonctionne pour les collaborateurs.

## 6. Si ça ne marche toujours pas

- Le `curl` (5a) répond toujours `timed out` : vérifier que les nouvelles routes sont bien `Enabled: true` dans `headscale routes list`. Si oui, il est possible que **SAP ait aussi changé de région** ou que l'IP du serveur ne soit **plus whiteliste** côté SAP → contacter l'admin SAP RISE pour reconfirmer la whitelist de `151.115.148.243`.
- Le `curl` répond 200 mais le navigateur non : le problème n'est pas les IP SAP mais le proxy `sap-fiori`. Vérifier le conteneur Traefik ( `docker logs --since 5m traefik | grep sap-fiori` ) et le DNS ( `dig +short sap-fiori.seizeconsulting.com` ).

- **Le conteneur Headscale ne répond pas** ( `docker exec headscale ...` échoue) : vérifier qu'il tourne ( `docker ps | grep headscale` ) et le redémarrer si besoin ( `cd ~/docker/headscale && docker compose up -d` ).

---

## 7. Pour éviter ce problème à l'avenir (recommandation)

---

Ce problème existe parce qu'on dépend des IP changeantes d'un load balancer AWS. La solution durable serait de **demander à SAP RISE un point d'accès à IP stable** (endpoint privé / IP fixe) pour le tenant. Si SAP le fournit, on enregistrerait cette IP fixe une fois pour toutes et ce guide ne serait plus nécessaire.

---

*Résumé express (pour les pressés) :*

```
# 1. Trouver les nouvelles IP
dig +short sandbox-z38bb8twno7.rise.cloud.sap
# 2. Les annoncer (remplacer par les vraies)
sudo tailscale set --advertise-routes=IP1/32,IP2/32
# 3. Voir les nouveaux ID
docker exec headscale headscale routes list
# 4. Les autoriser
docker exec headscale headscale routes enable -r <ID>
# 5. Vérifier
curl -I -m 10 "https://sandbox-z38bb8twno7.rise.cloud.sap:44301/sap/bc/ui5_ui5/ui2/ushell/shells/abap/FioriLaunchpad.html?sa
```